BANK OF GHANA

CYBER & INFORMATION SECURITY DIRECTIVE

OCTOBER 2018

PREFACE

In recent years, cyber-related systems and networks have been playing an increasing role in the financial sector. The financial sector relies on these infrastructures for processing transactions and transferring funds which has made them attractive and susceptible targets for cyber-attacks. Being high-profile targets creates a distinct challenge for financial institutions, since they must strike an optimal balance between security and maintaining efficient and reliable operations for their customers.

Today, cybercrime poses a real and persistent threat to financial institutions of all sizes and the number of companies that fall victim to cybercrime and digital espionage continues to rise. In fact, the financial services sector and its customers are heavily targeted by all those actors. Furthermore, the threat environment has become more sophisticated and diverse.

In recent times, cyber criminals have managed to bypass security controls and to exploit breaches or vulnerabilities within the cyber and information security defences of financial systems.

This document provides a framework for establishing Cyber and Information Security protocols and procedures for; routine and emergency scenarios, delegation of responsibilities, inter- and intra-company communication and cooperation, coordination with government authorities, establishment of reporting mechanisms, physical security measures for IT Datacentres and Control Rooms, and assurance of data and network security.

CYBER & INFORMATION SECURITY DIRECTIVE

ARRANGEMENT OF SECTIONS

Section

PART I – PRELIMINARY MATTERS

1. Objective

The objective of this Directive is to:

(1) Create a secure environment within *'cyberspace'* for the financial services industry and generate adequate trust and confidence in ICT systems as well as transactions in the cyberspace;

(2) Create an assurance framework for design of security policies and for promotion of compliance to global security standards and best practices by way of *cyber and information security assessment*;

(3) Strengthen the Regulatory framework for ensuring a secure environment within cyberspace;

(4) Enhance the protection and resilience of the financial systems' operation and provide security practices related to the design, acquisition, development, and use of operation information resources;

(5) Improve the integrity of ICT products and services by establishing infrastructure for testing and validation of security of these products and services;

(6) Promote continuous cyber and information security risk assessment;

(7) Promote awareness creation and ensure human resource security.

2. Applicability

This Directive is issued under the powers conferred by Section 92(1) of the Banks & Specialised Deposit Taking Institutions Act, 2016 (Act 930)) and shall apply to regulated financial institutions licensed or registered under the Act 930 and any other entity regulated by the Bank of Ghana under any other enactment. The directive also applies to Ghanaian banks and their international affiliates and Ghanaian affiliates of international banks.

3. Obligations of Regulated Entities

BoG-regulated institutions shall perform the following obligations:

(1) Place special emphasis on cyber and information security and take all the necessary steps to protect and manage their systems and data effectively.

(2) Expand and enhance their cyber and information security capabilities.

(3) Improve the institution's resilience to operational disruptions due to the materialisation of cyber and information security risks; reduce their impact on the institution's business continuity; and to minimise damage to its ICT assets and information as well as those of its customers (see Part V for the definition of asset).

(4) Determine the extent of the implementation process by financial institutions while seeking to maintain, at the same time, a degree of flexibility as required by the unique nature of this Directive(s).

(5) An institution shall manage its cyber and information security risks with a systemic, organization-wide view, within the framework of Ghanaian law and subject to its Directive pertaining to risk, operational risk, business continuity, and ICT management.

(6) In managing its operational risks, the institution shall address and document the cyber and information risks relevant to its operations as well as the measures taken to mitigate them.

(7) Address cyber and information security scenarios that may affect its own activities and those of customers, suppliers and service providers.

(8) Understand the scope of cyber and information security threat and the required security capabilities for meeting this challenge.

(9) All institutions supervised by the BoG shall be ISO27001[1] certified and should adopt ISO27032.

(10) Institutions that handle, process, store, or transmit debit card, credit card, prepaid card, e-purse, ATM cards, and/or POS) and related information shall be PCI-DSS[2]-certified.

(11) The methodology for managing and handling cyber and information security events shall comply with international standards such as National Institute of Standards and Technology (NIST) and ISO 27001.

[1] https://www.iso.org/isoiec-27001-information-security.html
[2] https://www.pcisecuritystandards.org/pci_security/

PART II– GOVERNANCE

4. The Board

The Board of a regulated institution is responsible for the following:

(1) Determine the institution's cyber and information security risk management strategy.

(2) Approve institutional policies of cyber and information security, outsourcing, survivability, backup and recovery from cyber incidents and attacks, and disaster events.

(3) Appoint a Board Sub-Committee on Cyber and Information Security risks and countermeasures with a well-defined charter

(4) Approve the annual and other work plans for cyber and information security, business continuity and disaster recovery.

(5) Receive quarterly and/or immediate reports, as required, about significant cyber and information security incidents.

(6) Dedicate at least two meetings each year to cyber and information security risks and countermeasures.

(7) Hold an annual discussion about the adequacy of the institution's cyber and information security policies and strategies.

(8) State and extend its support for inter-institutional collaboration on cyber and information security defence.

(9) Ensure effective internal controls and risk management practices are implemented to achieve security, reliability, availability, resiliency, and recoverability.

5. The Senior Management

The Senior Management's responsibilities are the following:

(1) Create the institutional framework for cyber and information security risk management and oversee its implementation and maintenance.

(2) Formulate institutional policies about cyber and information security, outsourcing, survivability, backup and recovery from cyber incidents and disaster events.

(3) At least once a year, the Senior Management shall discuss whether the policies referred to in (2) above should be revised.

(4) Allocate the necessary resources for the institutional cyber and information security framework and policies.

(5) Hold a biannual meeting to monitor and control the implementation and effectiveness of the institution's cyber and information security activities and measures.

(6) Receive quarterly and ad-hoc reports, as required, about cyber and information security threats and countermeasures with reference to the risk estimate stipulated in this Directive.

(7) Receive and discuss monthly reports on significant cyber and information security incidents and analyse their corporate implications.

(8) Determine the types of cyber and information security incidents necessitating immediate notification of the Senior Management.

(9) Assign a Senior Management member to act as Director of Cyber and Information Security (DCIS).

(10) Appoint a Cyber and Information Security Steering Committee chaired by the DCIS.

(11) Appoint a Chief Information Security Officer (CISO) and determine his/her powers, responsibilities, and authority in the institution; and demand that he/she assume a proactive approach to cyber and information security defence.

(12) Report to the Board immediately any significant breach(es) of cyber and information security occur.

(13) Promote inter-institutional collaboration on cyber and information security defence.

(14) Report to the Bank of Ghana, all significant and suspected cyber and information security incidents.

(15) Senior Management should fully understand risks associated with ICT Outsourcing. Due diligence report should be prepared before a service provider is appointed.

(16) Report to the Bank of Ghana on major cyber and information security incidents.

6. Internal Audits

(1) The institution shall ensure that an internal independent unit is responsible for auditing Cyber and Information Security.

(2) The Senior Management shall allocate the necessary resources for implementing the auditing processes, and to ensure that adequate training is provided for the unit to boost its capabilities to perform its tasks.

(3) All aspects of cyber and information security management shall be audited at least once a year or in line with the risk-based audit approach of the institution.

(4) An audit shall review the institution's survivability, backup and recovery processes at least once a year.

(5) Audit findings on cyber and information security risks shall be reported to the Board and Senior Management.

(6) The Board and Senior Management shall discuss the Audit Reports.

(7) Whenever internal cyber and information security audits make use of outsourcing services, evaluation of audit findings shall remain the exclusive purview of the institution's internal auditing unit

(8) A follow-up process for tracking and monitoring cyber and information security audit issues and an escalation mechanism to notify the relevant Senior Management should be established.

PART III – THE CHIEF INFORMATION SECURITY OFFICER

7. Appointment

(1) The Senior Management shall appoint a Chief Information Security Officer (CISO) specifying responsibilities, duties and institutional authority.

(2) The CISO must be appropriately educated, skilled and experienced in the field of cyber and information security

(3) The CISO shall not hold any other position or bear any additional responsibility in the institution which can bring him/her into conflict in relation to his/her responsibilities as a CISO.

(4) The Senior Management shall provide the CISO with all the resources necessary to fulfil his/her duties.

8. Status in the Institutional Hierarchy

(1) The CISO shall be directly supervised by a member of the Senior Management, e.g., the DCIS.

(2) The CISO shall act autonomously in determining the work and reporting interfaces required between him and other officials in the institutions. Senior Management shall approve these interfaces.

9. Responsibilities

The CISO shall:

(1) Advise the Senior Management and Board on Cyber and Information Security Management.

(2) Formulate an institutional methodology for managing cyber and information security risks.

(3) Develop the institution's Cyber and Information Security policy and submit it to the Senior Management and Board for approval.

(4) Develop and update specific and general work procedures for realizing the institution's cyber and information security policy.

(5) Maintain an ongoing process of cyber and information security risk assessment with the relevant institutional units, in order to analyse and assess:

a) the risk levels integral to the institution's technological and business activities;

b) The controls required to ensure systems integrity.

c) The level of residual risk and exposure to cyber and information security threats the institution is willing to accept in implementing these activities.

(6) Integrate and coordinate all institutional cyber and information security efforts, including oversight and control of all institutional units participating in these efforts.

(7) Create a framework for receiving ongoing and ad-hoc reports from various institutional units.

(8) Initiate and conduct cyber and information security readiness exercises as follows:

a) at least quarterly, an exercise shall be staged to assess the ability of one or more institutional entities to deal with a cyber-attack; and

b) once a year, an exercise shall be undertaken to assess the preparedness of the entire institution to withstand cyber-attacks.

(9) Coordinate cyber and information security activities, including joint exercises with business partners and service providers.

(10) Promote cyber and information security awareness and train employees, suppliers, business partners and customers.

(11) Continuously learn and monitor cyber and information security issues by identifying trends, methods and advanced developments in the field while gathering information about emerging attack techniques and ways of dealing with them.

(12) Form a Cyber-Incident Response Team.

(13) Analyse cyber and information security incidents that have occurred in Ghana and worldwide, and assess their potential impact on the institution, as well as implement the relevant measures proposed.

(14) Develop metrics and indicators to assess the effectiveness of cyber and information security systems and procedures.

(15) Assess regular and ad-hoc institutional cyber and information security controls.

(16) Draw up annual and multiannual work plans, including budgeting, prioritisation and timetables for implementing the assessment processes.

(17) Prepare and submit annual reports to the Senior Management and Board, detailing the institutional cyber and information security defence level, weaknesses and vulnerabilities, available countermeasures, and the activities and budgets required to enhance its defences.

(18) Be responsible for collaborating with relevant institutions involved in cyber and information security issues.

(19) Ensure preparation of reports on major cyber and information security incidents to the Bank of Ghana.

PART IV – CYBER SECURITY RISK MANAGEMENT

Cyber and Information Security Policy and Procedures

10. Policy

(1) Policy, standard and procedures for managing cyber and information security risks shall be presented to, and approved by the Board. This document shall cover at least the following areas:

a) the cyber threat environment and its potential impact on the institution;

b) the institution's approach to managing cyber and information security risks and in determining and monitoring the level of exposure to cyber and information security threats;

c) The principles behind implementing cyber and information security measures.

The policy shall comply with relevant Ghanaian laws and regulations, as well as international cyber and information security standards such as ISO27000 family standards.

(2) The policy shall be reviewed at least once every two years regardless of and in addition to whatever updates are required during this time.

(3) The Senior Management is responsible for writing a framework document about managing the institution's cyber and information security risks. This document shall include but not be limited to:

a) the objectives that are to be achieved in managing cyber and information security risks;

b) structural mapping of institutional entities involved in cyber and information security risk management, including their responsibilities and authorities;

c) Description of the institution's risk assessment and management processes and methods and how they are to be utilized and reported.

(4) The Senior Management shall define the institution's cyber and information security policy in line with this Directive (see Part II). This policy document shall be consistent with the institution's cyber and information security strategy. It shall refer to all controls and methods for achieving the institution's cyber and information security targets and shall be reviewed on an annual basis and regularly updated.

(5) The cyber and information security policy document shall present and include, but not be limited to:

a) the purpose of cyber and information security;
b) the necessity for proactivity in cyber and information security and for implementing advanced protective capabilities;
c) the responsibilities of cyber and information security officers;
d) institutional structures that support cyber and information security;
e) the link between cyber and information security risk management and its countermeasures;
f) a detailed description of countermeasures and controls required and the framework for their implementation;
g) monitoring and response systems;
h) enhancing the information and cyber security awareness of employees, business partners, suppliers, service providers and customers;
i) gathering and sharing information among employees and with other institutions;
j) the use of implementation, maturity and effectiveness indicators to assess the institution’s cyber and information security controls; and
k) evaluation, control and reporting.

(6) Specific policies for implementation of security controls shall be formulated based on the overall cyber and information security policy and be updated regularly.

11. Procedures

(1) Based on the institutional cyber and information security policy, specific procedures shall be developed to cover all cyber and information security issues.

(2) Procedures shall be detailed and related to each stage, process and unit involved in managing operations, security, backup, survivability, recovery and control.

(3) The Senior Management shall implement compliant processes to verify that information and cyber security standards and procedures are enforced.

(4) The procedures shall be reviewed on an annual basis or as required following changes in the relevant business or technological environment.

12. The Cyber and Information Security Risk Management Steering Committee

The Senior Management shall appoint a Cyber and Information Security Risk Management Steering Committee (hereafter, Steering Committee). The composition and the responsibilities of the Steering Committee are as follows:

(1) The Steering Committee shall include at least three members appointed by the Senior Management with the DCIS as Chair; the Heads of the Risk Management, ICT and the CISO. The Board shall approve the Committee's composition.

(2) The Steering Committee shall help Senior Management to make decisions and to fulfil its responsibilities in the field of cyber and information security, including survivability, backup and recovery issues.

(3) The Steering Committee shall discuss and monitor

a) the implementation of plans and activities to reduce cyber and information security risks, including backup and recovery issues;

b) Debriefing and lesson learning following cyber and information security incidents and implementation of relevant recommendations. Debriefing shall begin immediately after the end of the incident and completed within seven days following its commencement;

c) potential risks involved in activating institutional systems in a cloud environment; and

d) Potential risks involved in outsourcing institutional activities.

(4) The Steering Committee shall meet at least once a month and document its discussions.

(5) The Steering Committee shall report to Senior Management about the implementation status of cyber and information security work plans and on any other related activities at least twice a year.

(6) At regular intervals, the Steering Committee shall report its activities, conclusions and recommendations to the Board.

13. Risk Management

Risks shall be managed from a cross-organisational perspective, considering the technological and human resources likely to be affected by this process. The Steering Committee shall be involved in this process and report to the Senior Management on the following area:

(1) Managing cyber and information security risks is part of the overall risk management in the institution.

(2) The institution shall manage the cyber and information security risks together with operational, business continuity and ICT risks.

(3) When addressing matters related to business continuity, the institution shall also evaluate cyber and information security risks that may affect its own operations and those of its suppliers and service providers. The institution shall also consider the availability of supportive infrastructures and any other relevant issues.

(4) The institutional risk management process shall rely on well-known methodologies and include surveys and tests as well as other useful risk assessment and mitigation processes.

(5) The Steering Committee shall be responsible for reporting to Senior Management about all aspects of Cyber and Information Security. This report shall include but not limited to the following issues:

a) cyber and information security risks;

b) new threats discovered worldwide or in Ghana and their implications for the institution;

c) security breaches in the institution and their implications; and

d) required changes in the institutional cyber and information security system due to these breaches and changes in the national and global threat environment.

14. Risk Surveys

(1) Each institution shall determine the cyber and information security threats and vulnerabilities to its environment which comprise internal and external networks, hardware, software applications, systems interfaces, operations procedures and people.

(2) The computer surveys and cyber and information security defence tests that must be performed regularly on the institution's ICT systems and processes must also be performed on any new or modified systems. The surveys are designed to ensure that the systems and infrastructure are resilient; assess the effectiveness of protective measures with reference to the risk assessment; and propose ways of correcting any issues discovered. Security and resiliency surveys should also be undertaken.

(3) The CISO is responsible for determining the annual and multiannual work plans for conducting cyber and information security surveys and tests; types of tests; and the timetable and scope of tests. The CISO shall budget and prioritise these surveys as part of his annual work plan.

(4) Senior Management shall discuss and approve any changes in the budgets allocated for surveys. These changes must be brought to the Board's knowledge.

(5) The CISO shall ensure that all institutional systems, business and technological processes are surveyed regularly, at least once a year.

(6) The CISO shall initiate controlled penetration and robustness tests for the institution's various systems to assess their resilience to both internal and external risks. This activity shall be performed at an interval appropriate to the specific risks of each system. Systems defined by the institution as high risk and/or connected directly to the internet and/or communicating outside the institution and/or using Wide-Area Network (WAN) shall be surveyed at least quarterly. The survey shall include, among other

matters, the various systems' technological infrastructures and their security and communication links.

(7) Survey findings and recommendations shall be submitted to the Steering Committee, which shall discuss them and set a schedule for implementing the corrective measures.

(8) This schedule shall be determined according to the risk level and technologies required to resolve the issue in question. Nevertheless, maximal repair time shall not exceed six months. Should a longer period be required; the Senior Management and the Board shall be notified.

(9) Every system, new, significantly modified or repaired, outsourced, or in cloud computing systems must be checked in cyber and information security surveys prior to moving it to the production environment.

(10) Significant survey and penetration test findings shall be reported to Senior Management and the Board's Cyber Committee.

15. Risk Assessments

Each institution is required to perform an analysis and quantification of the potential impact and consequences of information and Cyber risks on the overall business and operations. The analysis shall entail at least the following:

(1) A cyber and information security risk assessment shall be conducted at least once a year. The process shall identify the current risk environment; the effectiveness of existing controls; and the residual risks to each individual system and the institution as a whole.

(2) The institution shall rely on at least the following information in its risk assessment:

a) the findings of audits and surveys, and any other regularly available information that may suggest a vulnerability or breach;

b) external data, including information from third-party research and notification entities able to suggest a potential weakness or lead to the discovery of exposures or risks not yet identified;

c) lessons learned from cyber and information security incidents in the institution or elsewhere;

d) a mapping of business and operational processes in order to detect risks and to identify risk interdependencies and weaknesses in existing controls (and assessing their effectiveness) or in managing risk and threat and vulnerability matrix;

e) scenario analysis to assess the likelihood of the risk materialisation, its potential implications and ability to identify and respond to these scenarios; and

f) qualitative and/or quantitative indicators to assess risk exposure.

(3) The risk assessment shall refer to the various activity areas of the institution's operations.

(4) The risk assessment shall refer to the entire supply chain including risks due to outsourcing, service providers, customers and Internet usage.

(5) Methods for identifying, measuring and assessing cyber and information security risks shall be documented and approved by Senior Management.

(6) External companies with expertise in risk assessment may be authorised to conduct the risk survey

(7) The outcomes of the risk assessment process shall be integrated into the institution's overall risk assessment process.

(8) The annual risk survey shall be updated on an ongoing basis following any external changes such as new types of attack and internal changes, including technological, organisational and business changes, such as outsourcing.

(9) The annual risk assessment shall be discussed by the Senior Management and Board. The monthly updates shall be discussed by Senior

Management on a monthly basis. Assessments pointing to significant risks shall be brought before the Board.

16. Risk Mitigation

An institution shall develop and implement risk mitigation and control strategies. These shall include determining the residual risk and the likelihood of new incidents. These risk mitigation and control include but not limited to the following:

(1) An institution shall examine the effectiveness of existing controls and assess the residual risks using qualitative and/or quantitative methodologies and indicators. The process and its outcomes, including methodologies and indicators used, shall be documented.

(2) The institution shall identify options for treating vulnerabilities based on the risk assessment findings, determine the controls to be implemented, and assess their effectiveness and the residual risk.

(3) The CISO shall formulate a work plan to be implemented when controls are lacking and/or when controls need to be replaced or enhanced. The work plan, including timetable and budget, shall be formulated based on the degree of risk to the institution on account of the non-implementation of the activity required. The plan shall be submitted to the Steering Committee for approval.

(4) The CISO should review and update the institution's cyber and information risk controls and mitigation approach taking into account changing circumstances and variations in the institution's risk profile.

(5) The work plan shall be submitted to Senior Management for approval and determination of the residual risk level and discussion of its implications.

17. Risk Monitoring and Reporting

(1) An institution shall maintain a risk register to facilitate the monitoring and reporting of risks. Risks of the highest severity shall be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. The institution shall review the risk register periodically and put in place a monitoring and review process for continuous assessment and treatment of risks.

(2) The CISO is responsible for cyber and information risk monitoring and reporting.

(3) An institution is required to develop cyber and information risk matrix to highlight systems, processes or infrastructure that have the highest risk exposure. An overall cyber and information risk profile of the institution shall be provided to the Board and Senior Management. In determining the risk matrix, the institution shall consider risk events, regulatory requirements and audit observations.

PART V – ASSET MANAGEMENT

This section covers the institution's responsibility to analyse all ICT and data assets, determine their sensitivity and importance to the institution, and their vulnerability to potential cyber threats. The term "asset" refers to information and data, hardware, software, documents, communication equipment, business processes, buildings and employees.

18. Inventory

(1) Senior Management shall put in place an inventory register for all the institution's ICT and information assets and allocate budget required to implement these objectives.

(2) The inventory shall list all

a) tangible and intangible institutional assets;

b) tangible and intangible assets that are not located in the institution's premises but are under its responsibility;

c) ICT and data assets not under the institution's responsibility, but where a shortage of these assets or their malfunction could affect the institution.

19. Ownership

(1) An owner shall be designated for each asset.

(2) For the purpose of this subsection, an owner is an individual employee or unit in the institution responsible for:

a) Usage of the asset in question,

b) Ensuring its integrity and instructing on how it shall be treated in the case of a cyber and information security incident;

c) Backing it up and ensuring its recovery following the incident;

d) Controlling the asset and determining those authorised to use it and the type of use they are allowed to make of it;

e) Developing and maintaining the asset.

20. Acceptable Use

(1) Acceptable use of an asset is defined as its utilization for the work assignments of the user, subject to the authorisations for his role. The use of the asset may only be for institutional purposes and the user must not disrupt or harm the work of other authorised users.

(2) All employees, including outsourced and contract employees, must comply with acceptable use requirements and shall sign a document to that effect.

21. Asset Mapping and Classification

(1) The asset inventory shall include a mapping of the relations between all the institution's ICT and data assets and any other metadata describing them. These shall include but not limited to the owner's identity; the physical location of the assets; its applications; business and technological processes involving the assets, including the nature of its use – reading, updating, etc. – and relations and dependencies between the asset and others; the identity of its users; usage restrictions and access permissions; sensitivity; and cyber and information security measures designed to protect it. All this information must be current and updated on a regular basis.

(2) Every asset shall be classified, according to the following classifiers but not limited to them: business importance or the asset's value to the institution; sensitivity in terms of cyber and information security and legal aspects; and the degree of damage to the institution should the asset be compromised, tampered with or turned against the institution.

(3) The list of classifiers shall be approved by Senior Management once a year or following a significant change in classifiers.

(4) Each information item shall be tagged with a label indicating its sensitivity, business importance, etc.

PART VI – CYBER DEFENCE

22. Security Infrastructure

(1) The principles applicable to the institution's cyber and information security infrastructures shall be laid down in its policy document. These principles shall express the institution's commitment to a high level of protection of its privacy as well as its ICT and Information Assets including those of its employees; suppliers; service providers; and customers.

Security measures shall be selected with reference to the risk environment, the sensitivity of the information in question; predicted levels of loss; Ghanaian laws; and BoG regulations. In addition, to properly addressing the risks, these measures shall be continuously updated to the highest level possible.

(2) The institution shall implement and manage data security safeguards for its ICT and information resources, including but not limited to the following:

a) *Access control.* All access to the institution's ICT resources and information shall be accompanied by an identification and authentication process. (This includes appropriate identification and authentication processes for the equipment that is being used). Moreover, the institution shall segregate identification and authentication processes with the assurance level dictating the level of activity permitted.

b) *A certificate mechanism* for hardware, applications and users shall be maintained and managed to ensure that these entities are associated with or belong to the institution. This mechanism shall serve to identify the institution to these entities.

c) *Secure audit logs* shall document any event such as identification and authentication, access to and activities with resources, logging off, etc. All logs shall be streamed to a single focal point.

d) *Data integrity* shall be maintained using dedicated means such as electronic or digital signatures.

e) *Non-repudiation* shall be ensured using dedicated means such as electronic signatures.

f) *Encryption of data in motion* both in and outside the institution's premises. Information files shall be transferred to and from the institution using a relay mechanism such as electronic vaults.

g) *Encryption of data at rest* shall be considered by the CISO in accordance with the type and sensitivity of the data involved and the institution's technological capabilities. Any decision with regard to encrypting this data shall be submitted and approved by the Steering Committee and Senior Management.

h) *Physical security* shall be provided at all sites, including backup sites storing institutional information. In addition, the institution shall physically secure all sites where information could possibly be accessed such as offices.

i) *Maintenance and ongoing activation* of all the means listed above shall be performed at the highest level of professionalism with ongoing coordination between all parties involved. It is the CISO's responsibility to ensure that adequate and up-to-date procedures shall be followed in this regard.

(3) The institution shall ensure that its cyber and information security safeguards are capable of performing their tasks even during disasters. Moreover, these safeguards must also be able to recover from such disasters.

(4) The institution's Senior Management shall ensure that its cyber and information security safeguards comply with Ghanaian laws and regulations.

(5) Outsourced suppliers and service providers shall document and enforce the institution's procedures in a manner that ensures the highest level of confidentiality and integrity of institutional information while enabling the availability of this information and protecting the privacy of those providing this information.

In order to provide an in-depth defensive infrastructure, cyber and information security shall be coordinated and integrated with the institution's ICT and HR departments as well as its ongoing business and technological processes.

23. Architecture

(1) A financial institution shall implement a secure physical and logical architecture for preventing, detecting, rectifying and documenting breaches of its information technology system.

(2) The institution shall implement methods and mechanisms to prevent data breaches.

(3) The institution's communication networks shall be segregated from the outside world (physically or logically). The institution shall maintain strict separation between its internal networks and all entities located outside its premises: the internet, suppliers, service providers and customers.

(4) The institutional network shall be segmented such that each segment shall be separate from other segments. The institution shall maintain a strict separation between its networks and the outside world. It shall use measures such as a demilitarised zone (DMZ), relay mechanisms, information filtering and segmentation to prevent the injection of hostile codes; it shall install a proxy system to blur and conceal its infrastructures from hostile actors; and it shall use measures for identifying and detecting unauthorised attempts to access and penetrate its communication networks, servers, workstations and applications.

(5) The institution's internal communication network shall be segmented according to criteria related to organizational structure, functionality, information sensitivity, risk, etc.

(6) Different work environments shall be created, as required, for segregating development, testing and production. Development teams shall not be allowed to access the production environment at any time. Version deliveries/updates shall be carried out subject to full coordination

(7) The institution shall continually seek to enhance security policy for its network systems, workstation and safeguards.

(8) A directory of services shall be implemented to authenticate and authorize access to the institution's network and systems.

(9) The authentication to the network shall be based on two-factor authentication (2FA) such as smart card/token, one-time password (OTP), etc.

(10) The institution shall prevent its personnel from using unauthorized portable media.

(11) The institution shall prevent malware from infecting its network, systems and servers. Protective software against malware shall be implemented.

(12) The institution shall use sanitization software to prevent incoming and outgoing files from infecting the network.

(13) The institution shall protect sensitive files using encryption methods. Permission to inspect these shall be granted on a need-to-know basis and for audit purposes.

(14) The institution shall monitor its networks and systems for malicious activity or policy violations by internal and external intruders.

(15) The institution shall manage an employee's password by implementing a solution that shall involve storing the encrypted password, replacing it when it is compromised, allow system administrator to reset a password without knowing the real employee's access password to the system.

(16) The institution shall initiate a vulnerability audit of its network elements at least on a quarterly basis.

(17) It is recommended to implement cutting-edge technology based on anomaly detection algorithms for detecting zero-day attacks, malware and other malicious interventions.

24. Network Elements

(1) All unused ports in the network switches shall be disabled – either manually, using known standards, or using network access control software.

(2) Communication components shall be hardened to an adequate level based on institution procedures.

(3) The institution shall backup the configuration of the network elements and security safeguards to an encrypted backup

25. Network Management

(1) A management segment (or a dedicated network such as an out-of-band channel) shall be defined for each network as the only one allowing access to system/ communication components for management purposes.

(2) The management segment shall be protected by a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules, e.g. a firewall.

(3) The management segment shall be protected from known attacks. The institution shall prevent known attacks and monitor the network or system for malicious activity or policy violations by internal and external intruders.

(4) The management segment shall be logically divided into different parts according to the institution's environments.

(5) Security safeguard servers and management servers shall be allocated in this segment.

(6) Dedicated management workstations shall be allocated in this segment.

(7) The management segment shall be protected from unauthorized network access.

(8) The institution shall use enhanced 2FA (by implementing either smart cards; tokens with biometric matching abilities; one-time passwords etc.). Administrators shall have to access the network using 2FA.

(9) A policy shall be formulated for enhancing the security of the institution's network elements, systems and workstations.

(10) The institution shall audit all administrative activities. The activities shall be logged and sent to the institution's SIEM system.

26. Encryption

(1) Data in motion between various local networks shall be encrypted end-to-end.

(2) The institution shall consider whether to also encrypt traffic within the internal network. The Senior Management shall decide about this matter in light of its risk profile.

(3) All management traffic shall be encrypted, including both sessions and passwords.

a) The institution shall encrypt its information in compliance with international standards and best practices.

b) For *asymmetrical* encryption, RSA algorithms or elliptic curve cryptography (ECC) shall be used.

(4) The encryption algorithms and the handling of the institution's encryption keys must meet the most up-to-date FIPS-140 standards or similar up-to-date standards or those presented in any superseding document.

(5) BoG-regulated institutions shall use the maximal key length allowed for encryption and digital signatures.

(6) The institution shall use a digital signature algorithm recognised as an international standard, such as RSA.

(7) Encryption and authentication keys shall be exchanged according to established international protocols/standards.

(8) Encryption keys shall be produced and stored in a manner that ensures their protection and prevents theft, loss, leaks or any risk to the institution's production and/or storage processes. Production and storage of the institution's encryption keys must meet international standards such as FIPS PUB 140-2 or the most up-to-date equivalent.

27. Media Encryption

(1) All network traffic that includes identification details such as username and password shall be encrypted.

(2) The process of authenticating to web-based systems shall entail the use of HTTPS (TLS protocol) to encrypt the medium between the user and server.

(3) Encryption algorithms must be standard and of proven reliability (such that it does not enable key extraction or keyless encryption, such as AES).

28. Remote Access

(1) Remote access to the institutional network shall require a high level of identification and authentication (at least 2FA) such as a smart card with certificate or token; a user code with a one-time password (OTP); or a user code with biometric authentication.

(2) All equipment components that remotely access the institutional network shall be signed with a digital certificate in order to authenticate themselves.

(3) The institution shall grant remote access to the network and the core system only on a need-to-know basis. The access shall be granted for a

short period and limited time in accordance with the position of the individual requesting access.

(4) A remote access segment shall be allocated dedicated DMZ segment.

(5) The remote access safeguard shall support encryption abilities in order to connect securely.

(6) Remote access to the institution shall not be direct. The access shall be initiated via a secure server that has such capabilities as encryption; strong authentication protocols; separation of duties; password management; time control enforcement; and the ability to record (and replay) each of the activities conducted, enabling the institution to know, after the fact, who has accessed what and when.

29. Internet Access

(1) The institution's internet access networks shall be segregated from the internal networks.

(2) The institution shall implement and manage data security safeguards for securing its internet access, including but not limited to the following:

a) Availability –

i. Internet and Wide-Area Network (WAN) connectivity shall be protected against disruptions. Accordingly, the institution shall have at least two different internet connections.

ii. In order to ensure that there is continuity of operations in the institution, it shall implement a solution against an availability disruption or a denial of service attack that may pass through the internet service provider.

iii. The institution shall prevent known attacks and monitor the network or system for malicious activity or policy violations by external intruders.

iv. Internet connectivity shall be protected by a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules, e.g., a firewall.

b) Confidentiality

i. The institution shall monitor, detect, and block breaches of potentially sensitive data, disclosed or transmitted to an unauthorized party via internet services e.g., browsing, email.

ii. The institution shall monitor, detect and protect against attempts to obtain sensitive information such as usernames or passwords by a malicious entity disguised itself in an electronic communication as being trustworthy.

iii. The institution shall screen the contents of incoming and outgoing internet communications via the web and email. The institution shall formulate a policy to determine to what extent its communications shall or shall not be displayed to the user.

30. Websites and Web Applications Protection

(1) The institution shall protect its business and non-business websites.

(2) The institution shall be protected from application-based hacking attempts by securing the application code and by utilising an application security system that monitors and controls incoming and outgoing traffic based on predetermined security rules such as a web application firewall (WAF).

(3) The institution shall protect itself from database-directed hacking attempts by external or privileged users e.g. database administrator (DBA) by monitoring, controlling and blocking connectivity and access to sensitive information using such means, for example, as a database firewall (DBF).

(4) The institution shall monitor and block a fraudulent website user based on behavioural methodology.

31. Access Control and Authentication

(1) The institution shall manage a system of permissions to access its resources and information, including certificate mechanisms for remote equipment or users. It is recommended to implement an Identity and Access Management (IAM) system.

(2) The institution shall restrict employee and system access to information and resources based on role assignments and on a need-to-know basis.

(3) Access to the institution's communication network shall be granted only after the user has been identified and authenticated.

(4) 2FA (biometric/smartcard/token/OTP) shall be implemented to authenticate users. A user password can only be used for legacy systems or for those that were developed years ago. The institution's systems must support all three options (biometric, 2FA, username and password). The username and password must be identifiable based on Windows Authentication or Single-Sign-On (SSO) technology, rather than through the application.

(5) Users shall not be allowed to use a shared user account. Each system user shall be uniquely and actively identifiable in the Active Directory.

32. Biometric Authentication

(1) Whenever biometric authentication is required, the process shall be executed over a dedicated system that maintains an enhanced information security level in which biometric database is encrypted and a permission system is enforced to deny access.

(2) Only the authentication system shall be able to access the biometric database.

(3) Biometric data shall be transmitted in the network in encrypted format only.

33. Compartmentalization and Permissions

(1) The institution's permission policy shall be based on the least privilege principle.

(2) Any and all system components shall become inoperable if the user in question is not authorized

(3) Compartmentalization shall be based on implementing a role-based access control mechanism in all information systems according to the unique identification of each user and the system's ability to implement the mechanism.

(4) The working hours of users must be restricted.

(5) Permissions must be applied to the folder and file system on a need-to-know basis.

(6) The compartmentalization level required in the system shall be on a need-to-know basis.

a) Users shall not be able to erase any files and every file entering the system shall be saved.

b) Original files shall be saved to the database and users shall be unable to write into the fields.

34. Servers and Workstations

(1) The institution shall install in its servers and workstations operating systems, browsers, etc. versions which are supported by the Original Equipment Manufacturer (OEM)/Service Providers.

(2) The operating systems shall be installed with security updates, including antivirus software, updated to the installation day. The institution is responsible for providing all tools to ensure security updates for the various systems required, whether they are connected to the public network or not. An orderly process shall be set up for updating and managing the systems.

(3) For cases where the institution is using legacy systems that do not support the requirements in 34 (1) and (2) above, the institution shall record such cases and prepare a plan to be presented for BoG approval to solve such cases on a timely manner

(4) Endpoint security software shall be installed on all servers and stations to prevent the connection and disconnection of removable media. The systems shall be updated and managed from the central system in the network.

(5) The systems shall operate in a stable manner, aligned with all security updates known at the day of installation.

(6) Each institution server shall be hardened to an adequate security level, according to the institution's hardening policy. It is recommended to execute the hardening centrally.

(7) Each of the institution's workstations shall be hardened to an adequate security level, according to the institution's hardening policy. The hardening process shall prevent users from acting as local administrators and block any possibility of running local software without authorization. It is recommended to execute the hardening centrally through the security/control systems.

35. Databases

(1) The databases that the institution utilises must be the most suitable for its operation, taking into consideration information and cyber security requirements.

(2) Databases shall be installed with the security updates valid for the installation day.

(3) The systems proposed shall operate in a stable manner and in alignment with all security updates known on the day of system installation.

(4) The database shall support the possibility of encrypting fields/tables inherently, or, alternatively, using third-party software.

(5) The database shall be hardened according to the institution's hardening policy.

(6) Access to the database shall be allowed to three user groups only: application-level users, privileged users and the DBAs.

(7) The institution shall protect itself against database-based hacking attempts by securing the database with a system that monitors and controls incoming and outgoing traffic based on predetermined security rules such as a database firewall – host- or network-based.

36. Software Information Security

(1) Any software the institution develops and implements shall meet best practice information security requirements and rely on well-known and accepted standards in the information security industry.

(2) The institutions shall create a secure development life cycle (SDLC) methodology.

(3) The systems shall be protected against known attacks and, the following security issues, among others, must be addressed:

a) preventing SQL injection attacks;

b) checking the inputs received and processing them only after validation;

c) prohibiting password saving in system code;

d) session management;

e) enforcing authentication between users and system components;

f) implementing a mechanism for temporary access lockout in case of consecutive failed login attempts within a brief duration;

g) permission management;

h) system management;

i) secure database access;

j) preventing the saving of sensitive information at the end-station;

k) handling errors.

(4) The system's acceptance tests shall include application-level resilience tests; code review; risk assessment; and penetration tests. The developer/contractor shall rectify all security issues that are discovered following these tests.

37. Auditing

(1) All activities executed in the system, including security activities, must be logged.

(2) The logging must be tamper-proof, accessible and legible to any of the relevant systems.

(3) The basic log must audit all activities carried out in the system (application-level logs). The log requirements shall be defined when detailed design of the system's connectivity is being carried out. Basic requirements include:

a) monitoring of administrative actions executed in the system such as system definitions, updates, audits start, audit stop, viewing system permission, delegation, etc.;

b) monitoring all events on both the user and System Admin. level, both at the application and OS level;

c) authentication auditing: success/failure (login/logout) of all events, password reset/renewal; system permissions: granting and changing permissions, profile definition and creation, etc.;

d) input/output – monitoring data entered into system fields; incorrect attempts at entering data, logging the data entered in the database, etc. and

e) running application-related services: store procedures, jobs, transactions, etc. The system shall audit success, failure, duration, etc.

(4) Log file management:

a) access permissions to the log file: several permission levels must be defined for viewing, processing, copying, deleting, etc.;

b) the system log must enable ongoing maintenance – defining the size of the log saved, updates, backups, etc.; and

c) routing the log through additional security components. Since there is a possibility that the interim server might not be accessible directly from the proposed system and the logs would have to be sent through additional security components, the log in such cases shall not be modified as it is routed through filtering, partitioning, firewall, encryption and other systems.

(5) The log shall be sent to the institution's existing SIEM/SOC system.

(6) An audit trail (log) will be maintained for a period consistent with its purposes and in no case for less than 24 months.

38. Incident Preparedness

(1) The CISO is responsible for mapping potential cyber and information security threats. This mapping shall be updated regularly and presented quarterly to the Steering Committee.

(2) Subject to the provisions of clause (1) above, the CISO shall prepare the plan for treating cyber incidents in collaboration with other relevant units; the CISO shall coordinate this collaboration. The plan shall refer to the following stages: detection, analysis, containment, removal and recovery. The plan shall be updated annually or as required in response to the changing risk and technological environment, whichever emerges first. Updates made during the year shall be presented to the Steering Committee, while significant changes shall be presented to both the committee and Senior Management.

(3) The plan shall be presented to the Senior Management for approval and budgeting.

(4) The CISO is responsible for ensuring that the procedures of other units in the institution, whether technology or business-oriented, include references and action items related to cyber and information security incidents.

(5) On a quarterly basis, a small-scale exercise of the unit responsible for treating cyber and information security incidents shall be conducted together with another ICT(s) and/or (a) business unit(s). The lessons drawn from each exercise shall be reported to Senior Management through the Steering Committee.

(6) On an annual basis, a comprehensive exercise including most institutional units, and the Senior Management, shall be conducted. The lessons drawn

from this exercise shall be submitted to both the Steering Committee and the Senior Management. The latter shall discuss the exercise and the lessons learnt from it within 30 days of receiving the report.

(7) The CISO is responsible for monitoring the implementation of these lessons and reporting on it as provided in clauses (5) and (6) above.

(8) The CISO is responsible for forming a team for treating cyber and information security incidents. The main task of this team is to act as an institutional focal point for notification, analysis, response, recovery and coordination of all institutional actors charged with treating cyber and information security incidents. This unit shall be on call 24/7/365. It is the Senior Management's responsibility to provide the CISO with all the funds and resources required for this purpose.

(9) The CISO is responsible for providing this team with the means to perform their duties, such as a security information and event management (SIEM) system for processing the information and a security operations centre (SOC) for displaying it. In addition, the CISO must attend to the team's education and qualifications.

(10) The CISO is required to develop a prioritisation and estimation mechanism for cyber and information security incidents. This mechanism shall be informed by such parameters as risk levels and potential damage. It shall be updated from time to time following changes in risk levels and technologies, as well as lessons drawn from exercises. It shall be presented for the Senior Management's approval on an annual basis.

39. Research

(1) Ongoing cyber and information security research is one of the foundations of an efficient and effective cyber defence system. Senior Management shall provide adequate budgets for this research.

(2) The CISO is responsible for ongoing information gathering and research about new cyber and information security threats, cyber incidents in Ghana and worldwide, and for the analysis of this knowledge base with reference to known risks faced by the institution and its current level of preparedness for cyber-attacks and information security incidents.

(3) The CISO is responsible for constantly monitoring the institution's internet-facing and non-internet-facing network in an attempt to detect and/or substantiate suspected, intended or actual attacks against the institution.

The CISO is also responsible for conducting an ongoing learning process of the various cyber and information security methods and remedies; for assessing the possibility of integrating these methods into the existing cyber and information security system; and/or applying lessons drawn for them by performing the required changes and improvements in the existing cyber and information security defences.

PART VII – CYBER RESPONSE

The process for defining the institution's cyber response function and governing its implementation is set forth in ISO 27035.

40. Structure and Hierarchy

(1) This section defines the various functions and work processes of the cyber response unit and its interfaces with other units.

(2) The CISO is responsible for creating and directly supervising the cyber response unit.

(3) The team shall include employees with appropriate knowledge and education in cyber and information security, particularly in cyber defence and alert systems.

(4) In terms of specific qualifications, the team members shall include but not be limited to the following:

a) Researchers responsible for gathering information on global and national attack trends and developments and determining their relevance to the institution's preparedness efforts.

b) Analysts responsible for analysing relevant intelligence to determine whether the institution is under attack.

c) Cyber response experts specialising in providing primary and secondary responses.

d) Employees who are not an inherent part of the team but who can help in implementing the response and in assisting the institution to recover.

e) Forensics experts to assist both in handling the legal and insurance aspects following an attack as well as in lesson learning for future responses.

(5) The team shall include both permanent members and non-member experts called upon to assist in emergency efforts.

(6) The roles of the cyber response team include but are not limited to the following:

a) developing institutional preparedness for cyber and information security incidents;
b) detecting and alerting about security incidents;
c) intelligence gathering;
d) categorising the incident, evaluating its impact on the institution and what steps shall be taken to minimize harm to the institution as the incident escalates;
e) Cyber response;
f) coordinating with other institutional units treating the incident;
g) expanding the institution's defence and recovery capabilities by commissioning experts for assistance, i.e., both from within the institution but not included in the regular team and/or experts from other companies if necessary;
h) reporting to the Senior Management, the Board and other institutional units as required;
i) lesson learning: this process shall begin no later than two days after the incident has ended and be completed within 21 days, including the drafting and finalising of reports (after receiving comments) and preparing a work plan according to lessons drawn;
j) preparing the information required for external entities, such as the BoG, law enforcement authorities, and insurance bodies; and
k) On-going research.

(7) The CISO supervise the entire course of incident treatment. He is responsible for declaring a state of attack and determining when this state has ended. Such a declaration shall be made in writing and be communicated to Senior Management, the board and other institutional units.

41. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) technology provides real-time analysis of the security alerts that network hardware and applications generate. SIEM technology includes systems for monitoring, consolidating and analysing cyber and information security incidents documented in security system logs or the individual logs of each of the institution's ICT infrastructures.

(1) An institution is required to establish a cross-organisational SIEM system or, alternatively, receive SIEM services from a local Ghanaian company.

(2) An institution must connect its SIEM system to the BoG's SIEM system by sending alerts, aggregate information and reports.

(3) In addition to the system itself, the SIEM infrastructure must include a knowledge-based model that details the response to each incident identified in the system, and consolidate all the details required to appropriately handle the incident.

(4) The SIEM system shall be connected to all of the institution's core infrastructure and peripheral systems, including communication equipment, servers and applications. It shall collect, consolidate and analyse log information in order to detect and alert anomalies in the behaviour of networks, servers, applications, etc.

(5) All existing systems in the institution shall be connected to the SIEM system within 12 months of its activation.

(6) Every new system – whether software or hardware – must be connected to the SIEM system as soon as it becomes operational.

(7) The team responsible for the SIEM system shall be an integral part of the cyber incident team, as provided for in Part VII above.

(8) The SIEM team shall be responsible for the following issues but not limited thereto:

a) developing and implementing mechanisms for correlating and analysing information to detect anomalies;

b) providing real-time warnings of suspected incidents and mapping their source;

c) storing and analysing historical information;

d) supporting forensic investigations;

e) identifying non-compliance incidents; and

f) Implementing advanced mechanisms for detecting, analysing and alerting about cyber and information security incidents.

42. Security Operations Centre (SOC) – Situation Room (War Room)

(1) Each institution shall create a "situation room" operated by designated employees to serve as its cyber nerve centre.

(2) The SOC shall coordinate all institutional cyber and information security incidents shall be responsible for initiating a response process based on systematic procedures for determining, among other things, the level of defence in light of reported incidents.

(3) When the process is terminated, the SOC shall issue a summative report.

(4) Appropriate human and technological resources must be allocated and budgeted for the SOC. Its status vis-à-vis other technological units in the institution must be determined.

(5) The CISO is required to establish a SOC to act as the institution's focal point or situation room for all matters related to alerting about cyber and information security incidents and their treatment.

(6) The SOC shall be integral to the cyber and information security response team.

(7) The CISO can implement some of the required functions for handling a security incident using outsourced services. Nevertheless, he must ensure that the institution is able to audit all outsourced activities and that these meet this Directive.

(8) The SOC's roles include but are not limited to

a) gathering and consolidating intelligence on the materialisation or probability of materialisation of cyber & information security events;
b) determining when alerts are false or real;
c) determining the level of (potential) risk of the (potential) incident;
d) treating the incident immediately upon its detection;
e) coordinating with other institutional units handling the incidents
f) cross-institutional coordination and commissioning of external experts as required; and
g) gathering data for reporting to the Senior Management, Board and other institutional units as required.

43. Methodology

(1) A systematic methodology shall be developed for the process of receiving information about incidents, including all necessary tools and procedures for screening, consolidating and determining the nature of incidents communicated by the institution's various ICT platforms.

(2) Processes for responding to any scenario (as well as secondary processes that may occur as the incident progresses and the requisite escalation

develops) must be set forth, including but not limited to the following:

a) receiving reports;
b) scanning logs;
c) reporting to various interfaces in the institution;
d) determining the type of incident and the potential threat it poses to the institution;
e) initial incident response;
f) escalation, including the commissioning of external experts if necessary;
g) reporting to external entities, e.g., the BoG; and
h) Developing a restoration process methodology.

44. Intelligence

(1) The institution must either form a team of analysts to gather intelligence in cyberspace (including dark net websites) or hire external intelligence services.

(2) The intelligence services shall be provided on a monthly/bimonthly basis in the form of periodic reports, as well as on an ad-hoc/immediate basis by conveying alerts directly to the institution.

(3) All intelligence shall be consolidated and analysed in the SOC in order to formulate an informed response.

45. Data Mining

This section describes the major responsibilities of the research, which is a part of the SOC.

(1) As soon as a cyber and information security incident is suspected, the technological capabilities allowing the organisation to minimise risk and mitigate potential damages shall be assessed.

(2) Other institutions, vendors, etc. shall be contacted to obtain any information and assistance required in real time. Once the situation returns to normal, new institutional cyber tools shall be assessed based on the incident analysis.

(3) During and after the incident, a forensic study shall be conducted of the source of the attack and the information it uncovers shall be organised for legal purposes.

(4) As soon as operations return to normal, the lessons learned shall be collated, the effectiveness of existing defence mechanisms shall be assessed; developing/purchasing new defence mechanisms and/or defence methodologies shall be considered; a review the teams' involved and the current procedures and methodologies shall be conducted with a view to future improvement.

46. Reporting to the BoG

(1) All financial institutions shall report cyber and information security incidents to the BoG on a monthly basis.

(2) The report, which shall summarise all incidents in the past month, shall be submitted to the BoG in the required format by the 15th of each month.

(3) Without prejudice to (1) above, all financial institutions shall submit an 'NIL report' in cases where the financial institution did not record any cyber security incidents.

(4) In addition to the monthly reports, financial institutions shall submit ad-hoc reports to the BoG, immediately and automatically, in the form of alerts to its SOC. The reports shall inform the BoG about the incident as it starts, unfolds and terminates.

(5) An institution shall report to the BoG immediately in the following cases:

a) An incident damaging information integrity.

b) Damage or shutdown of production systems that contain sensitive information for over three (3) hours (except for scheduled shutdowns).

c) Indications that sensitive information about bank customers has been exposed or leaked outside the bank.

d) The occurrence of unusual events, including significant penetration and attack attempts, actual penetration of ICT systems, the collapse of central systems, the activation of an incident response mechanism, etc.

e) Cessation of essential services as the result of unplanned shutdown of systems for one business day or more.

f) Any other significant event that has (almost) occurred and (almost) had significant impact on data management and protection.

(6) The BoG shall set forth a reporting policy, including incident severity levels and associated reporting duties and processes.

(7) The BoG is entitled to instruct the institution to report the security incident according to the circumstances.

PART VIII – EMPLOYEE ACCESS TO ICT SYSTEMS

47. Access Control

(1) An entity seeking access to a financial institution's ICT systems must be uniquely identified and authenticated.

(2) In exceptional cases, where the requirements of (1) may be unfeasible, the institution shall provide appropriate alternative.

(3) An institution shall set rules, using appropriate identification and authentication mechanisms in granting permission to various users and components of its ICT systems.

(4) Access to an institution's ICT systems shall be granted on a need-to-know basis and support the user's job assignments.

(5) An institution shall have computerised systems in place to manage and control access permission. An (attempted) access to its ICT systems shall be monitored and documented in an audit log and relayed to the SIEM systems.

(6) Employees shall be informed that every activity in the institution's systems is documented and an authorised official monitor this documentation.

(7) Access techniques to the institution's ICT systems shall be standard, including identification and authentication, for example, user-ID and password; validating permissions and access using the operating system's access method. The institution shall prevent and continuously ensure that no access to computerised information is allowed along a path that bypasses the operating system access method.

(8) An institution shall use a technology that integrates user identification and authentication, confidentiality, data integrity and non-repudiation safeguards.

(9) Notwithstanding paragraph (8), an institution may use alternative access control technologies in the following cases:

a) Accessing high-risk systems, subject to the CISO's discretion, which shall be documented, explained in writing and approved by the Steering Committee. Access to high-risk system through a remote-access-path is, however, prohibited.

b) An audit trail shall be maintained for remote access by vendors, service providers and business partners, when the use of the technology stipulated in paragraph (8) proves impossible. For reasons that are external to the institution.

(10) An institution shall set criteria, determined by risk and technological considerations, for a session timeout mechanism, after a certain period of idleness by the authorised individual.

(11) The institution shall set activity hours and dates when access to its ICT resources is allowed. This schedule of hours and dates shall apply to all employees. Exceptions to this rule may be made with reference to employees such as administrators, technicians, shift workers and any other eligible employees.

(12) When an employee is transferred within the institution, old permissions shall be revoked, and new ones granted in line with new position. CISO shall consider and implement a re-authorisation procedure for situations when the old and new positions overlap from information security perspective.

Channels of Communication with External Entities

48. Data Transfer between Sites and Organisations

(1) Information transferred through the institution's internal systems shall be encrypted in line with its classification level.

(2) Information, regardless of its classification level, being transferred through a Wide-Area Network (WAN) or over the internet shall be encrypted at the highest level.

(3) The general permission/authorisation system or an alternative one shall apply to all information transfers and each information transfer shall require specific permission.

(4) Transferring information outside the institution shall be carried out as part of a recognised business process. The information shall be transferred in a manner to ensure confidentiality, integrity and non-repudiation by the sender and the receiver.

(5) Information shall be transferred through a relay mechanism that shall maintain a separation between the institutional network and the outside world and enable scanning for malware and data breach.

(6) The relay mechanism shall be kept separate from the institutional network.

(7) CISO shall set procedures for information transfer in routine and emergency circumstances.

49. Web Access

This section discusses the provision of web access to employees for work purposes from within an institution.

(1) Senior Management shall determine the permitted use of internet connectivity for employees based on a risk assessment and ensure appropriate controls are in place.

(2) An employee authorised to connect to the internet shall sign a document attesting to awareness of what is allowed and disallowed in internet access. The document shall indicate to the employee that online activities are continuously monitored. The CISO is responsible for preparing the

document and procedures that detail employee rights and obligations when using internet services.

(3) An employee shall be able to access the web from the assigned workstation under one of the following conditions:

a) Workstation is standalone, unconnected to the intranet and contains no institutional applications or sensitive information.

b) The intranet is separate from the network connected to the internet and it shall be kept segregated by using a DMZ. The internet-facing network shall be continuously monitored and equipped with safeguards as detailed in paragraph (4)

c) Internet connectivity is enabled through a separate institutional server. The server shall be continuously protected and monitored using safeguards as detailed in paragraph (4). Configuration and connectivity shall support only browsing and emailing activities.

(4) Safeguards shall be implemented to protect internet connectivity. These measures include but are not limited to the following:

a) content and spam filtering;

b) preventing the use of malicious links;

c) intrusion detection systems (IDSs);

d) firewalls;

e) antivirus and anti-malware software;

f) site blacklist filtering;

g) an employee's user code and password on the internet shall differ from those used by the employee on the intranet; and

h) secured, dedicated log documenting all user activities.

(5) An institution shall implement mechanised means for controlling the system that connects to the internet and scans it for vulnerabilities.

(6) CISO shall conduct resiliency and penetration tests for the servers, security mechanisms and communication infrastructures facing the

internet, including email infrastructures, at least quarterly. The findings of these tests, shall be discussed by the Steering Committee. CISO shall prepare employee procedures and Directives specific to internet usage.

(7) Every new system or major modification of a system shall undergo risk and information security surveys, including a penetration test before it is transferred to production. The project manager shall be apprised of the findings of these tests. The system shall be transferred to production only after passing these tests.

(8) Any expansion of an online service an institution provides, shall require prior BoG approval. The request for approval of the service expansion shall comprise of a risk assessment of the service.

50. Email

This section addresses the institution's email systems, their use by employees, allowed and disallowed activities.

(1) CISO is responsible for preparing procedures detailing allowed and disallowed activities with regard to the institution's email systems.

(2) An employee allowed to use the email system shall sign a document attesting to awareness of the allowed and disallowed activities, including the fact that the email activities are continuously being monitored.

(3) Once a year an employee shall sign an electronic version of the document cited in paragraph (2) and view an electronic presentation of the main security and care required when using the email system.

(4) A DMZ shall separate the mail servers from the institutional network and relay systems shall also be put in place.

(5) The mail servers and email system shall be secured using safeguards including but not limited to the following:

a) content and spam filtering;

b) a system for detecting, blocking and reporting data breaches;

c) IDSs;

d) Firewalls; and

e) Antivirus and anti-malware software.

Mobile Devices

51. Bring your own device (BYOD)

This section addresses the conditions for approving employee use of private mobile devices such as smart phones and laptops with the institution's systems.

(1) Senior Management shall make a strategic decision on allowing an employee to use their own devices at work, for work purposes. This decision shall be documented in writing and approved by the board. The decision shall be considered in line with the risks involved; employee convenience; benefits to the institution; the institutional inputs that is requested and the costs required to support it.

(2) CISO is responsible for determining the safeguards and usage policy regarding private mobile devices and areas of activity, such as email, diary, contact list, documents and any other relevant activity.

(3) Approved private mobile devices shall not be connected to the institutional network or workstations and shall be used as standard standalone workstations.

(4) Approved private mobile devices shall be installed with the institutions' security controls. Without such controls, the device shall not be connected to institutional systems.

(5) An institutional information stored or transferred to or from a private mobile device shall be highly encrypted.

(6) Any approved private mobile device shall be handed over to qualified employees to install and update the security controls and institutional

applications or in response to requests from the institution or law enforcement authorities for examination.

(7) Every device shall be password-protected, using built-in mechanisms for that purpose. A robust identification measure such as fingerprints shall be employed to use institutional applications such as email. The password shall meet the institution's password Directives.

(8) The device shall lock itself after a certain idle period. Reactivating the device shall require a PIN that is different from the password.

(9) The institution shall manage all these devices using a dedicated infrastructural management tool.

(10) User access to institutional information shall be restricted based on the employee's existing authorisation.

(11) Institutional information may be remotely erased from the device depending on one of the following conditions:

a) the device has been lost or stolen;
b) the employee has terminated his employment at the institution; or
c) The institution's ICT team has detected within the device a breach, penetration, malware or any other threat to the institution and its infrastructure.

(12) An employee interested in using a personal device shall sign a legal document consenting to the institution's security requirements including, but not limited to the following:

a) institutional monitoring of his device;
b) installing the institution's information security software on the device
c) avoiding any use of the device that violates the institution's procedures; and
d) Awareness of duty of care to handle and use the device in an appropriately responsible and cautious manner.

52. Institutional mobile device

This section addresses the conditions for approving an institution's owned mobile devices such as smart phones or tablets, for use with the institution's systems.

(1) The Senior Management shall make a strategic decision on allowing employees to use institutional mobile devices at work, for work purposes. This decision shall be documented in writing and approved by the Board. The decision shall be considered in view of the risks involved; employee convenience; benefits to the institution; the institutional inputs required; and the costs involved.

For all other cyber and information security purposes, the directives in Section 51 apply also to Institutional mobile devices.

PART IX – ELECTRONIC BANKING SERVICES

In recent years, banking customers around the world have increasingly been utilising technology and direct communication channels to access banks services. The growing number and scope of bank services provided over the internet, by phone and by the use of self-service machines such as ATMs, POS, NFC, etc. enable institutions to provide services at a lower cost and enhance their operational efficiency.

Electronic banking services which provide the options for using advanced technologies to enable customers to remotely perform transactions involve risks. Some of these risks include breaches of information and cyber security privacy, embezzlement, fraud, money laundering, legal risks and reputation risks. Institutions are required to adjust their risk management framework to the changing technological environment and update it on an ongoing and dynamic basis to deal with these risks. Institutions shall strictly observe information security principles to protect confidential customer information, privacy and information integrity of the institution and the availability of electronic banking services.

Institutions are also required to develop and refine their methods for detecting embezzlement and fraud, preventing money laundering and for handling failures quickly and properly to minimize damages to customers, legal and reputational risks involved in remote transactions.

53. General

(1) An institution shall define different electronic banking service levels and apply different levels of information security remedies with reference to these levels.

(2) When a customer accesses account remotely, details about the transactions from the previous access or logon shall be provided to the extent possible.

(3) An institution shall have in place a procedure for obtaining customer approval for account transactions with reference to such aspects as type, nature and amount.

(4) A customer shall be given the ability to save and or print in real time the details of the order actually given.

(5) A third-party transaction shall be carried out subject to the following conditions:

a) Transactions in accounts included in a beneficiary list shall be carried out in line with a ceiling determined by the institution and/or the customer, whichever is the lower of the two.

b) Transactions crediting other accounts shall be limited to ceilings determined by the institution.

c) Prior to entering the details of any money transfer order, the customer shall be required to enter an authentication code sent over a separate communication channel, such as short message service (SMS).

d) When a transfer order is issued, the customer shall be required to indicate the receiver's details and the purpose of the payment.

e) An institution shall transfer data about the payer and, to the extent possible, about the purpose of payment in a manner that shall enable the beneficiary to view this information clearly.

f) The institution shall set ceilings for a single payment, according to the type of customer.

g) The ceiling for third-party electronic transfers of any kind shall be in line with all other existing ceiling by BoG.

(6) An institution shall provide customers with information about the precautions required when operating in an online environment at least once a year.

(7) Every new service shall be approved in advance by the BoG. Its assessment of the service shall include the cyber and information security aspects.

54. Subscribing to Electronic Banking Services

(1) An institution shall sign an electronic banking service (hereafter, EBS) agreement with its customers.

(2) An institution may offer the customer a package of channels and services so long as the customer shall be allowed to deselect channels he/she does not want to use.

(3) Paragraph (2) shall not apply to cases where a cluster of channels is required to provide a certain service. A customer is entitled to revoke consent to receive a service or the use of a channel or a cluster of channels at any time.

(4) Prior to obtaining the customer's approval for an agreement, an institution shall present to the customer the EBSs that each channel provides and the risks they involve. An institution shall also inform the customer about cyber information security and recommended privacy protection principles for minimising these risks to the customer.

55. Identification and Authentication

(1) An institution shall determine individual identification and authentication factors for online and other remote transactions based on risk assessments and policies approved by the Board.

(2) An institution shall establish processes for creating, delivering, using, replacing and disposing all identification and authentication factors, allowed to ensure that no sensitive information is exposed during the creation and delivery process. Rules shall be put in place to determine

password length and complexity re-use limitations, the frequency of password change, and password blocking and unblocking.

(3) Identification and authentication factors shall be delivered to the customer securely and on separate channels.

(4) An institution may make certain services and transactions contingent on the use of additional factors such as a one-time code delivered on a different channel or generated by a dedicated component, biometric and identifications.

(5) A customer's authorisation to perform transactions and retrieve information through EBSs shall not exceed the authorisation that apply to the customer's bank account.

(6) Notwithstanding the above, the institution may reach an agreement with a company and/or corporation to the effect that whoever is so authorised by the customer shall be allowed to use EBSs independently, even when authorisations for brick-and-mortar accounts are different, subject to a verified confirmation by the authorised individual/entity in the company and/or corporation.

Online Services

56. Website

(1) An institution shall take measures to detect attempts to spoof its website, provide its customers with appropriate tools to verify the identity of its website.

(2) Traffic between the customer and website shall be encrypted using the highest level of standard mechanisms available.

(3) An institution shall utilise the means under its control to protect the computer or devices the customer uses for banking communications against unauthorised use and exposure of information about the customer's accounts. Typical steps might include, for example, preventing

passwords from being saved to the browser or web pages to cache memory.

(4) An institution shall protect its customer-facing website using all known and accepted technological means to protect banking websites, including, but not limited to, firewall, anti-malware products, DoS/ DDoS attack prevention, IPS/IDS and Web application Security.

(5) An institution shall maintain at least four separate zones: internet-facing zone, DMZ, internal networks (intranets) and the server farm in its infrastructure.

(6) Customer information shall be stored in the innermost zone of the server farm.

(7) Customer information shall not be stored on a public cloud, even if the customer-facing website of the institution is outsourced.

(8) Customer authentication method shall be based on a two-factor authentication.

(9) Institutions that operate a transactional website or web application shall also operate a technical support service and channels for reporting unusual incidents and other relevant issues. This service shall be available daily (24x7).

(10) An institution shall conduct the following to assess the effectiveness of the existing safeguards :

a) Security surveys and website penetration tests at least half yearly and/or following any significant modification;

b) Security surveys and robustness and penetration tests for the internal servers every six months and/or following any significant modification; and

c) DoS/DDoS attack robustness tests, including SOC exercises at least every six months and/or following any significant modification in the website or DMZ environment.

57. Mobile Applications

(1) Senior Management shall determine the uses and types of transactions allowed to customers using mobile applications.

(2) Usage of devices supporting mobile applications that do not support an appropriate encryption level such as AES with at least a 128-bit key length and digital signature are not be allowed.

(3) CISO shall compile a list of devices and operating system versions the institution supports.

(4) A user shall provide his express agreement to using the institution's application. A record of this agreement shall be saved to the institution's computers. Notification of receiving the user's agreement to using the application shall be sent to the user utilising a channel such as SMS.

(5) An application shall be tested and examined by the institution with regard to its cyber and information security prior to its release to customers. Any application update shall require a re-examination of the application. Applications shall be developed with attention to the following issues, among others:

a) An application shall not seek authorisation beyond those absolutely necessary to perform its ordinary functions.

b) Information transferred through the application shall be the minimal necessary for using it.

c) Application shall not store sensitive information on the mobile device. Data shall be stored in encrypted form using the device's mechanisms when required.

d) Storing historical information, GPS data or any other sensitive information shall not extend beyond the time span required for the application's operations.

e) Sensitive personal information shall be erased upon quitting the application.

(6) An institution shall develop a mechanism to ensure the authenticity of the applications and the connection between them and the institution. The applications shall be authenticated over the device whenever the user starts using them.

(7) An institution shall provide a dedicated website for communicating with mobile applications.

(8) An institution shall have in place an identification and authentication mechanism to verify the identity of application users. It shall for example use multi-factor authentication, such as fingerprints, as an additional layer of user authentication assuming the device supports such a capability.

(9) The information transferred to or from the application shall be encrypted and digitally signed, all within the device's capabilities.

(10) An institution shall examine at least once every 24 hours whether the third-party applications actually used indeed match those it has distributed to the store when a third party is used to distribute the application.

58. Email

(1) The Senior Management shall determine the type of uses and transactions allowed over the email.

(2) Issuing orders to perform customer transactions over the email shall be defined as a high-risk activity and only allowed by using technologies that combine identification and authentication of the customer giving the order and other confidentiality, data integrity and non-repudiation safeguards.

(3) Information shall be emailed from the institution to the customer by adhering to the following:

a) in a safe environment, taking proper measures to ensure its confidentiality;

b) protected by a digital signature allowing the sender's authentication;

c) using computerised mechanisms allowing the institution to determine with absolute certainty whether the customer has received and opened the email, downloaded it to his personal computer and/or printed it; and

d) Information on customer activities as noted in paragraph 3(c) is securely saved in the institution.

59. Telephony Services

(1) Call centre

a) The Senior Management shall determine the types of uses and activities allowed to customers through the institution's call centre.

b) Customers utilising call centre services shall be provided with an identification code and unique authentication factors exclusively dedicated to call centre use.

c) The CISO shall decide how to authenticate the customer with reference to the transaction the customer seeks to perform, the risk level associated with it and available technologies (such as numerical password, voice identification, etc.).

d) Recording the calls:

i. All calls between a customer and a call centre operator shall be recorded, including both the conversation itself and the information presented to the operator.

ii. The recordings shall be considered sensitive information.

iii. This information shall be saved on the call centre's servers for not more than 12 hours.

iv. A process of continuous backup of all recordings to an environment separate from the call centre shall be put in

place. Information shall be saved in encrypted form as long as required by law.

v. An institution shall use computerised mechanisms to process recorded information, including its correlation with the information presented to the operator.

vi. Only authorised individuals shall be allowed access to these recordings.

e) In call centre computers and servers,

i. No access to the internet or any other external service shall be allowed, apart from the call service.

ii. Employees shall not be allowed to connect any removable media to call centre computers.

iii. An operator's computers shall contain only the software necessary to perform the duties.

f) CISO shall implement, with the required modifications, a cyber and information security policy and conduct security, risk and robustness surveys and penetration tests for the call centre environment, including the telephony equipment.

g) Transactions allowed by the institution without a human response, using Interactive Voice Response (IVR) system, shall be restricted to obtaining summary information only, without any data related to the customer's identity, such as account number, name of customer, address, credit card number and other relevant information, a customer shall authenticate to the IVR system using a username and password dedicated to the call centre environment.

(2) Fax

The following applies to the transfer of information between the institution and its customers using a computerised fax only, that is, a computer simulating a fax machine.

a) The Senior Management shall determine the types of uses and activities customers shall be allowed to perform using a fax.

b) Giving orders to perform customer transactions over the fax shall be defined as a high-risk activity, allowed only by using technologies that combine identification and authentication of the customer giving the order and other confidentiality, data integrity and non-repudiation safeguards.

c) Information shall be transferred from the institution to the customer

i. in a safe environment, taking proper measures to ensure its confidentiality;

ii. protected by a digital signature allowing the sender's authentication;

iii. Using computerised mechanisms allowing the institution to determine with absolute certainty whether the customer has received the fax and opened it, downloaded it to his personal computer and/or printed it.

(3) Text Messages (SMS)

Any information transferred using SMS shall not include complete identifying details about the customer and the account, such as name, account number and other relevant information.

60. Customer Security

(1) An institution shall implement an automatic mechanism for detecting and monitoring anomalies in customer accounts, particularly when high-risk transactions may be underway in order to detect suspicious transactions in real time.

(2) An institution shall follow the development of fraud techniques and other threats relevant to its operations in Ghana and worldwide and update its monitoring mechanisms as required. It shall use information received from both internal and external sources to update its monitoring mechanisms.

(3) An institution, according to its discretion, shall alert customers to any unusual activities it has identified with regard to certain transactions. It shall also monitor the risks involved in adding a channel and services that are not being used solely for informational purposes, transfers and payments and any other transactions beyond the ceiling determined by the institution. The institution shall take immediate steps such as obtaining the customer's approval or revoking a transaction with regard to any suspicious activities.

(4) Notifications and requests for approval shall be delivered through a different communication channel or device other than those being used for the transaction in question. These activities shall only include the minimal details required for identification of the transaction. Under no circumstances shall these actions include full identification of details about the account or customer.

(5) Selecting the communication channel as stipulated in paragraph (4) shall be made with due attention to how quickly the customer must be notified, the level of risk involved in the transaction, and the level of information security required given the sensitivity of the information in transit.

(6) The institution shall make clear to customers the major risks involved in EBSs and recommend reasonable precautionary measures that shall be observed.

(7) This information shall be provided over a variety of channels, including the institution's website, notifications upon accessing an EBS, email, brochures, newsletters and other relevant information.

(8) An institution shall manage the risk entailed in spoofed websites or applications when it is suspected that fraudulent activities may be involved that lead customers to provide sensitive information such as passwords and account numbers to unauthorised parties.

(9) When an institution suspects EBS fraud that may affect a large number of customers within a short time, it shall not only act immediately to remove the threat and mitigate potential damages but also notify all those at risk, report to the BoG, and consider making a public announcement according to the circumstances of the case.

61. Passwords and Password Management

(1) Minimal password length shall be eight characters or in line with current standards or Ghanaian law. The more stringent requirement of the two.

(2) All passwords shall be complex, that is, strong.

(3) When managing passwords for customer identification and authentication, an institution shall refer to the risk and service levels of the system in question.

(4) An institution shall use a mechanism for generating an initial password which shall be considered a strong password. The initial password shall be random.

(5) The initial password shall be delivered to the customer on a separate channel. Initial passwords include those issued to customers when unblocking a password.

(6) The institution shall initiate customer password change:

a) immediately after the first login using the initial password; and

b) At least every four months or in line with the system's service and risk levels.

(7) The institution shall revoke a password issued to a customer hereafter, "blocked password" in one of the following cases:

a) the initial password has not been used within three days of its issue;

b) at the customer's request or whenever the institution suspects unauthorised use of the password;

c) after several failed login attempts, as determined by the institution but involving no more than five consecutive attempts; and

d) After a period of six months of not using the specific system to which the password has been assigned.

(8) An institution may unblock a blocked password so long as the customer has been identified not only using ordinary identification details but also using specific details provided by the customer in advance, or according to details stored by the institution not updated in communications therewith.

(9) The stipulations of paragraph (8) shall not apply to EBSs using biometric identifications or devices that generate OTPs.

PART X – TRAINING, AWARENESS AND COMPETENCE

62. Sensitive Positions

(1) An employee in sensitive position shall receive in-depth training about privacy protection and cyber and information security.

(2) An employee in a sensitive position shall be required to go on vacation for at least two consecutive weeks.

(3) The following are examples of employees holding sensitive positions:

a) those who handle finances, whether physically or administratively;

b) those with access to encryption keys and/or equipment and to the personal information of other employees and/or customers;

c) those operating in an environment defined as sensitive;

d) ICT employees including technicians, system administrators and programmers;

e) Cyber and Information Security employees; and

f) Internal Audit employees.

63. New Employee

(1) Each potential employee, for any position at an institution, shall sign a legal document stipulating:

a) the duties with regard to protecting the confidentiality of the institution's information assets, including processes, customers, employees, suppliers and business partners;

b) awareness and agreement that all activities with the institution's ICT systems shall be for work assignments only, including the use of the institutional email;

c) awareness and agreement that all activities on the institution's ICT systems shall be controlled and monitored;

d) allowed and disallowed activities with regard to all institutional operations;

e) the principle of individual employee accountability and

f) that after the employee's termination, an authorised institution representative shall be allowed to view his mailbox and files stored on the intuition's computers.

(2) All the provisions of paragraph (1) shall apply to employees recruited through HR companies, to those employed by contractors providing services to the institution or to individuals seeking temporary employment.

(3) A hired employee shall receive basic training in privacy protection and cyber and information security. This training shall also explain the obligations with regard to the requirements and directive issues and the sanctions applicable to employees who violate them. The training shall be followed by a test.

(4) The institution is required to provide new employees with a document detailing any security training provided as per paragraph (3) and all the warnings and potential disciplinary measures applicable to violators.

64. New Positions

(1) An employee moving to a new position within the institution shall receive training in privacy protection and cyber and information security in line with the new position. The training shall be provided during the first month of employment in the new position or during the on-the-job training period whichever occurs first.

(2) An employee moving to a position where less security training is required shall be exempt from the additional training provided for in paragraph (1).

65. Cyber Education

(1) An employee shall receive cyber and information security training at least on an annual basis. This training shall be adjusted to the various positions and levels in the institutions, such as Senior Executives, ICT employee administrators and programmers and other non-ICT employees. An employee shall be tested following the training.

(2) CISO is required to provide diverse and comprehensive training programs in line with an employee's position. CISO shall conduct an annual review of the training sessions and update them as required.

(3) Senior Management shall allocate adequate funds for all required training and exercises as part of its cyber and information security budget.

(4) Employees directly employed in cyber and information security shall be required to undergo in-depth and dedicated cyber and information security education, including external training and examination by internationally recognised certification authorities.

66. Cyber Exercises

(1) An institution employee, temporary, contractual and outsourced employee, shall undergo exercises within their institutional units on how to handle suspected and/or actual cyber and information security events at least once a year. The level of training shall be appropriate to the employee positions. These exercises shall be included in the annual training program required of all employees.

(2) Employees directly in charge of treating cyber and information security incidents shall undergo quarterly exercises.

(3) The entire institution, including executives, Senior Management and Board members shall undergo a cyber and information security exercise and training in handling cyber and information security incidents once a year.

This exercise shall address issues including but not limited to the following:

a) decision-making processes in business and ICT environments;
b) backup and survivability processes, including business process continuity;
c) processes for identifying malicious applications;
d) attacks that threaten the robustness of the institution's ICT systems; and
e) Processes for reporting to the Senior Management, the Board and the BoG.

(4) The exercise provided for in paragraph (3) shall also include business partners, suppliers and service providers.

PART XI – EXTERNAL CONNECTIONS

This section addresses direct computerised communication for the purpose of conveying messages, such as trading orders, between two different institutions, bank and a stock market, a bank and a financial and/or other organisation. This is referred to as *external connection*.

67. Direct Connectivity

(1) Connection between two institutions shall be considered with respect to the risk estimate involving the contact between them.

(2) A risk survey and information security and cyber resilience surveys shall be conducted to cover all threats derived from the communication infrastructure in the connection(s) between the institutions and between test environments if applicable each year.

(3) Inter-institutional connectivity shall be protected, at the very least, by the following safeguards:

a) Communication between the two connected institutions shall begin with a procedure for identifying and authenticating the communication end-points.

b) Throughout the communication and once every random time unit, the identification and authentication procedure shall be repeated in a manner transparent to the application-level communication. Communication shall be immediately suspended where there is a suspected flaw in the identification and authentication.

c) Confidentiality, integrity, availability and non-repudiation of both communication partners shall be maintained.

d) Information transferred between the two institutions shall be encrypted at the highest level allowed between financial institutions.

e) The institution shall implement measures to ensure immediate detection of any damage to the information transferred, including exposure, tampering, erasure and concealment of all the information. Notification of any untoward incident shall be provided as required.

f) Business information transferred between end-points shall be saved to an application-level log.

g) Event in the course of the session, such as initiating contact and information transfer, shall be relayed to the SIEM.

(4) Connectivity shall be implemented in line with the following conditions, but not limited to them where the test environment of the institutions need to be connected:

a) Cyber and information security safeguards as detailed in paragraph (3).

b) The test environment shall be isolated from all other institutional environment.

c) The information in the test environment shall be highly restricted.

d) Information shall be masked and anonymized when it has to be transferred from production to test environment.

e) The execution and timing of any experimental procedures shall be coordinated between the two parties to the communication.

f) A connection shall be activated manually and shut down manually at the end of the experiment.

g) It is an institution's responsibility to install a mechanism that shall automatically cut off a session when the connection has not been manually shut down.

(5) A BoG-regulated institution that seeks to connect to another institution shall first obtain BoG approval.

68. Other Financial and non-institutions

This section addresses connectivity between financial institutions and other stakeholders and complement rather than substitute sections.

(1) The two parties shall meet all requirements in this Directive prior to seeking its approval for a connection.

(2) The two parties shall meet the directives included in paragraph 69.

(3) Risk, information and cyber security surveys of the connectivity between the two parties shall be conducted in the operational environment at least every six months. Equivalent survey shall be conducted in the test environment.

(4) The responsibility for conducting these surveys lies with both parties.

(5) The survey findings of each party shall be presented reciprocally to the respective Steering Committee. Any shortcoming found shall be repaired immediately.

(6) Survey findings shall also be sent to the BoG, together with a timetable for repairing any faults.

69. Business Partners

This section addresses connectivity between two business partners and related to BoG-regulated institution.

(1) Any connectivity between two parties shall be approved by the BoG. The following are the minimum requirements for this connection:

a) The institution meets the directives of this Directive.

b) The institution has conducted a due diligence process to ensure its business partner complies with risk management processes, including ICT and cyber and information security risks.

c) The business partner shall meet the minimum requirements of the directives.

d) Risk and information security surveys, penetration tests and cyber resilience assessment shall be conducted at the business partner's premises and all shortcomings repaired.

(2) The following tests, assessments and surveys shall be performed by the partners.

a) Risk and cyber and information security surveys shall be conducted at the business partner's premises every two years.

b) Risk, cyber and information security surveys, penetration tests and cyber resilience assessments shall be conducted in the operational and test environment of the connectivity between the partners at least once every six months.

c) Findings from these tests, surveys and assessments shall be presented to the Steering Committee and to the business partner. Any shortcoming shall be repaired immediately.

d) Any shortcoming that was not repaired promptly and/or a significant defect is found, shall be presented to the institution's Senior Management, which shall then decide whether to maintain connectivity, suspend it temporarily or, shut it down. The institution shall state the rationale for its decision.

e) A summary of survey findings shall be sent to the BoG, including a timetable for repairing all identified shortcomings.

70. Remote Access

Remote access to the institution's resources is designed to enable external companies to support ICT equipment at the institution for the purpose of maintenance and/or inquiries and/or repairs.

(1) Approving remote access to institutional resources shall be avoided as much as possible, including access by suppliers and service providers.

However, when remote access must be enabled in certain cases, this shall be done in a controlled and restricted manner and limited to cases such as repairing a code that supports a provider's hardware.

(2) Clear criteria and procedures shall be laid down when Senior Management decide to enable remote access.

(3) All remote access not provided for in clause (2) above shall be implemented using a technology that meets the requirements of Sections 29, and 48(8)and compatible with the following:

a) Serves as a gateway to the institution's, ICT resources that could not be accessed without it passing through an ICT component shall be inspected to determine whether it allows remote access. This functionality shall be disabled and the component shall be connected to a dedicated mechanism installed by the institution to allow controlled and supervised remote access;

b) uses an authentication mechanism and one-time passwords to identify and authenticate the caller;

c) uses a mechanism that ensures automatic and/or manual disconnection when no data has been transferred over a predefined timeframe;

d) uses technological measures to secure the communication, such as continuous identification and authentication of communication end-points; and logging all traffic in a dedicated log; encryption

e) Any access shall require manual activation and intervention by the employee in charge;

f) The system shall support logging, including computerised management of the administrative process accompanying the communication.

(4) CISO shall determine Directives for remote access that take into account the risks, the possibility of technological alternatives and the necessity of

the communication. the following procedures shall be followed in determination of the remote access:

a) Any request for a remote access session shall be presented to the CISO who shall determine its necessity and then approve or reject the request.
b) Prior to initiating the session, the callers shall be identified and authenticated.
c) During the communication session, a parallel communication channel shall be used to ensure that the communication in question is still required and that the party seeking it is indeed interested in holding the session.
d) A session shall be terminated manually or after its predetermined time span has lapsed, the earlier of the two.
e) The communication procedure shall be documented.

71. External Parties

(1) As a rule, any external communication performed over a Wide-Area Network (WAN) shall meet the provisions of Sections 49, and 72 with particular emphasis on the following:

a) The encryption implemented shall be end-to-end.
b) For the purpose of this section, it shall refer to the following aspects: intrusion detection and prevention systems (IDS/IPS); firewalls; and monitoring traffic such as by using content filters. Identifying malware shall be enabled only after decryption.

(2) Notwithstanding paragraph (1) above, the use of Wide-Area Network (WAN) between the institution's premises shall implement

a) end-to-end encryption;
b) Firewall, IDS/IPS; and
c) Any other measures as decided by the institution.

72. Data in Motion

(1) The institution shall ensure that the transfer of any information within its premises and/or outside its premises and/or between two of its facilities shall maintain its confidentiality, integrity, authenticity and non-repudiation.

(2) The institution shall implement measures to ensure immediate detection of any damage to the information being transferred, including exposure, tampering, erasure and concealment of all the information or any part of it. Notifications of any untoward incidents shall be provided as required.

PART XII – CLOUD SERVICES

73. Corporate Governance

(1) An institution considering the use of cloud computing must bring this issue to the Board prior to implementing this technology. The Board shall discuss the risks involved and decide whether to grant its preliminary approval and direct Senior Management on steps required accordingly.

(2) The Senior Management shall formulate a policy document governing the use of cloud computing which addresses but not limited to the following:

a) assessing the risks involved in the transition to cloud computing on various levels, such as applications alone, a specific activity area, core business and any other relevant risk;

b) the authority, responsibility and activities of cloud computing management units; approval processes; and hierarchy of required approval;

c) control and auditing entities;

d) type and scope of cloud services;

e) legal aspects;

f) monitoring the traffic between the institution and the provider and between the applications active in the provider's premises and their users, and employees;

g) privacy protection and cyber and information security;

h) cyber incidents and recovery; and

i) Terms and conditions of contract termination.

(3) The board shall either reject or approve the institution's use of cloud computing based on sub section (2).

(4) The Senior Management and board shall discuss the agreement prior to finalising its contract with a cloud service provider.

(5) An institution shall seek BoG for approval to transit to cloud services.

(6) The Senior Management shall ensure that any use of cloud computing complies with the policy provided for in paragraph (2), and that this use is subject to the terms of its general approval of the transition to the cloud.

74. Risk Management

(1) An institution shall conduct a due diligence of the provider's financial strength, professionalism and experience in providing similar services to other institutions prior to contracting with any cloud service provider.

(2) During the contract period or at least every two years, the institution shall conduct an additional due diligence.

(3) An institution shall conduct risk mapping and assessment prior to contracting with a cloud service provider. The assessment shall be updated on a regular basis throughout the contract period and following technological, business (transitioning a new activity area or application to the cloud), organisational and regulatory changes in the institution and/or provider. The survey shall focus on risks unique to cloud computing.

(4) A Senior Management shall discuss and approve transitioning to the cloud is any activity area or application not included in the original contract.

(5) An institution shall ensure that all controls are in place, including appropriate compensatory controls for the risks that have been mapped.

(6) The institution must ensure that it is able to monitor cyber and information security incidents related to its use of cloud services. The institution shall ensure it meets accepted standards and its own regulations when capabilities are provided by the provider. Moreover, it must be possible to integrate these capabilities with existing monitoring systems within the institution.

(7) Data in motion between an institution and the provider must be encrypted.

(8) Data at rest stored at cloud service provides shall be encrypted. The data classified by an institution as sensitive and whose exposure is liable to compromise the institution and/or its customers shall be encrypted

(9) The encryption keys shall be stored with the institution rather than the provider.

75. The Cloud Computing Service Contract

(1) The contract with the provider shall provide for, but not be limited to

a) receipts of provider's internal and external cyber and information security auditing reports about its activity, including those prepared by regulatory bodies;

b) enabling the institution to conduct independent cyber and information security audit surveys, including resilience and penetration tests and/or any other tests that substantiate and confirm the provider's compliance with this Directive;

c) enabling the institution, under special circumstances, to require that the provider conduct an ad-hoc security audit of a specific issue;

d) Allowing the institution to unilaterally suspend use of the provider's services or switch to a different provider. The institution shall have the option of moving all relevant data from the provider's system within a short time, as determined by its policy and subsequently delete this data from the provider's systems when it switches to another provider. The provider shall undertake that the data transfer including backups shall no longer be restorable from its systems;

e) Authorising the BoG to perform cyber and information security audits at the provider premises.

(2) The contract shall also provide for implementation of all cyber and information security mechanisms and controls that the institution requires to protect its data, including customers' data and ICT resources.

(3) Any cloud provider to an institution regulated by the BoG shall also be subject to this Directive in all issues pertaining to the institution, including international standards applicable to institutions subject to this Directive.

(4) An institution shall review the contract to ensure that the new owners comply with the same undertakings as the original owner when there is change in ownership of the cloud provider.

76. Institutional Application Development

(1) A provider shall enable the institution to have at least three, structurally separate environment namely development, testing and operational.

(2) The provider shall enable and support all development services required by this Directive and all best practices related to secure development.

(3) The provider shall enable cyber and information security tests, whether by the institution or by an outsourced specialist on behalf of the latter.

(4) All activities in all environments shall be documented in a log and relayed to the institutional SIEM for control and analysis.

77. Promotional Material

(1) The cloud service provider shall protect the integrity, reliability and availability of all the institution's promotional material that it hosts.

(2) Updating promotional material shall ensure a level of security that protects the confidentiality, integrity, availability, non-reputability and accountability of the employees involved.

PART XIII – BANKS WITH INTERNATIONAL AFFILIATION

78. Foreign Banks in Ghana

(1) This Directive shall apply to foreign banks as is, except for the following revisions:

a) Whenever a directive refers to the institution's ICT and/or infrastructural and/or any other institutional systems, the present phrasing shall be replaced by:

i. Local ICT systems in Ghana, including their interfaces with the foreign bank's ICT systems overseas; and

ii. Other local institutional systems in Ghana, in including their interfaces with the bank's systems abroad.

b) Whenever the Board's obligations are defined, they shall apply to the local management, that is, the foreign bank's management in Ghana.

c) The local CISO's reporting duties shall also include reporting to the CISO in the foreign parent bank abroad, or an equivalent in the foreign parent bank abroad.

d) Whenever a reporting duty to the BoG is referred to, the duty to report to the foreign parent bank Senior Management abroad shall be added.

(2) A foreign bank shall report to the BoG regarding its compliance with the following Directives: ICT and risk management, cyber and information security, and disaster recovery. It is also required to report on compliance with any regulations applicable to the foreign parent bank, including any changes therein.

(3) When a regulation of the foreign parent bank is less stringent than the comparative regulation in Ghana, the foreign branch shall not expect this regulation be relaxed.

(4) These directive shall apply when the foreign parent bank's regulation is more stringent

79. Ghanaian Banks Abroad

(1) A Ghanaian bank operating abroad shall comply with This Directive in, including reporting to the BoG and supervision by the BoG.

(2) A Ghanaian bank operating abroad shall comply with the privacy protection and cyber and information security laws applicable both abroad and in Ghana.

(3) The CISO of a Ghanaian bank operating abroad must report to the CISO of the local parent institution in Ghana.

PART XIV – PHYSICAL SECURITY

80. General

(1) All the institution's physical sites and facilities shall be mapped and classified to determine the access permission level required of employees. Mapping shall include both manned and unmanned sites; facilities with IT equipment such as servers, information platforms, sites where institution employees are employed such as offices; and sites or sites storing equipment such as generators, air-conditioners,.

(2) An institution shall implement physical security perimeters equipped with access, detection and deterrence controls, on the site, on secured zone and on individual segment level.

(3) All sites shall be supervised daily 24x7 by monitoring and surveillance systems transmitting to a manned control room. Traffic to the control room shall be secured to prevent damage and disruption of its integrity and availability.

(4) An institution shall use technologies to ensure that all visual and auditory surveillance records are saved and analysed.

(5) Every employee shall receive an identification device for example, card defining the allowed physical environments access.

(6) Guards and various technologies shall control access to site with IT equipment such as servers and information platforms, including sites where institution employees work.

(7) An institution shall implement a system to correlate employees' attendance record with their identification and authentication to its ICT systems.

81. Secured Zones

(1) Work areas shall be divided into several secured zones in line with sensitivity of the information in or accessible through them and the

potential damage to the institution in case the zone is in any way compromised.

(2) Servers and communication equipment including storage device of all kinds shall be placed in secured zones.

(3) Employee access to secured zones shall be allowed in line with their assigned roles.

(4) All entries and exits to and from a secured zone shall be monitored daily 24x7

(5) All entries and exits to and from a secured zone shall be controlled using a 2FA or 3FA mechanism, depending on the zone's sensitivity level.

(6) When an employee is transferred to a different position, the assigned access permissions shall be upgraded / downgraded in line with the current position. All permissions granted an employee shall be revoked immediately upon termination.

82. Segmentation

(1) Each segment of a secured zone shall be physically protected in a manner that prevents entrants into the secured zone and access to a segment not under the subzones or segments.

(2) Secured zones that serve the entire institution such as communication cable ducts shall be constructed so as to enable daily 24x7 surveillance.

(3) Notwithstanding paragraph (1) when it proves impossible to divide a site/facility into separate secured zones and implement physical protection as provided under this Section, the institution shall divide the work environment into segments. This division shall be based on the sensitivity of the information located or accessible and the potential damage to the institution when the information is compromised in any way.

(4) The level of protection of the entire environment shall be aligned with the security level required for the most sensitive segment.

83. Physical Security of Hardware and Other Equipment

(1) ICT equipment requiring protection includes any unit that saves electronic information or is used as part of equipment, servers, workstations, laptops, information platforms, telephone exchanges, routers, and any applicable equipment.

(2) The level of protection provided for this equipment shall be determined in line with the higher of the following two criteria:

a) the business impact of any compromise to the confidentiality and/or integrity and/or availability of the information stored over the equipment in question; or

b) Physical loss or unavailability of the equipment.

(3) An institution shall implement a "one-way-in/no-way-out" policy for any physical IT equipment placed in its premises.

(4) Notwithstanding paragraph (3) an institution shall determine procedures for removing equipment from its premises. This shall be allowed subject to the risk involved and the reason for removal. Borrowed equipment for example has to be repaired off-premises, and replaced while disposable equipment may be removed at some point.

(5) Whenever physical equipment needs to be removed from the institution's premises, the provisions of paragraph (4) shall be followed. All institutional information, including log files; parameters and/or other operational information shall be erased and/or distorted and/or reset to the manufacturer's configurations.

(6) Magnetic or optical information platforms shall be physically destroyed on the premises, and destruction certificate shall be generated and filed.

PART XV – HUMAN RESOURCE MANAGEMENT

84. Hiring

(1) An institution shall create an induction process which all newly hired employees shall undergo. This process shall include, but is not limited to the following (see also Part X):

a) the training required for the employees to fulfil their duties;
b) training in privacy protection and cyber and information security;
c) a platform for discussing the duty to safeguard the privacy and the confidentiality of institutional information and processes;
d) a platform for discussing the employee's individual accountability;
e) allowed and disallowed institutional activities;
f) a platform for discussing cyber and information security issues in general;
g) a platform for discussing the security of the institution's ICT systems in general, and those for which the employee is directly responsible.

(2) Criminal background check, reference check and background verification shall be conducted for every candidate.

(3) Every candidate shall undergo personality and reliability tests.

(4) A newly engaged employee shall be:

a) Given a unique user code and an initial password and/or additional identifiers such as biometric identifiers or a device/token that generates one-time passwords. The employee shall use, subject to his access permissions, a dedicated user code for accessing the institution's network and for using assigned workstation on the institution's premises.
b) Provided with additional identifiers which the assignment/enrolment process shall be carried out by a designated employee on the institution's premises if necessary.

c) Given access permissions to the institution's ICT systems on a need-to-know basis and in line with the employee's assignments

d) Informed that all activities in the paragraphs (a), (b) and (c) shall be documented and logged.

e) Trained to become aware of the issues stipulated in paragraph (1).

f) Given the documents as stipulated in Part X to sign and receive signed copies.

g) Informed of the security of the institution's ICT systems in general and those for which the employee is directly responsible in particular.

(5) A new employee shall not be allowed to transfer to the institution information from organisations where he has previously been employed.

85. Termination

(1) CISO shall ensure that procedures for employee termination include, but are not limited to the following:

a) blocking the user code in the employee's work environment; revoking his authorisations for all work environments; and denying his access to the institution's physical facilities;

b) briefing the employee on his continued accountability for maintaining the confidentiality of the institution's information and related privacy concerns;

c) the handling of employee data both in electronic media such as email and in physical media, such as printed discussion summaries;

d) the employee must be directed to back up the information on his workstation to a specific server and then to remove/delete it from his workstation;

e) Encrypted information with the employee's encryption keys, shall be decrypted;

f) CISO is responsible for ensuring that no information assets remain in employee's possession.

(2) Provisions of paragraph (1) shall apply where the institution initiates an employee's termination.

(3) CISO shall define procedures and provide Directives regarding the status of terminated employees in the interim period between the notice and actual termination. These measures shall include, but not limited to the employee's use of email and an ICT system for document management, archiving, and access control.

(4) Management shall determine the length of time for which an employee shall remain personally accountable for various aspect of work after termination.

86. Sensitive Positions

(1) Senior Management shall discuss whether to add but not remove specific positions to the existing list of sensitive positions.

(2) All employees for sensitive positions shall be subject to the fit and proper test directive issued by Bank of Ghana

(3) The activities of employees in sensitive positions such as ICT employees shall be monitored continuously using automatic log scanning, as in the SIEM system, and manual methods to detect conduct that is contrary to the institution's needs or interests.

(4) Any anomalous activity and or one that is contrary to the institution's needs or interest and or is considered inappropriate by the institution and or any other activity that is deemed suspicious shall be brought to the attention of the internal audit team.

(5) The workstation of an employee in a sensitive position shall not be directly connectable to the internet.

(6) All employees in sensitive positions shall take annual vacation of at least two consecutive weeks.

(7) An employee in sensitive position shall undergo personality and reliability tests every five years or frequently as determined by Senior Management.

87. Employee Lifecycle

(1) Whenever an employee moves to a different position within the institution, all authorisation associated with the old role shall be revoked and replaced by new ones consistent with new position. The CISO shall consider whether to also replace the assigned user code.

(2) An institution shall have appropriate and documented processes in place governing the On-the-Job Training (OJT) of employees in job transit, including close monitoring of their activities.

(3) CISO shall review all employee authorisation and their compatibility with their job assignments at least once a year.

(4) CISO shall ensure that employees is aware of and understand the following:

a) the essence of the institution's cyber and information security policy;
b) email usage procedures;
c) acceptable internet usage procedures;
d) software usage procedures;
e) the policy governing access to institutional ICT resources; and
f) How to respond to and manage cyber and information security incidents.

(5) An employee shall receive annual refresher training on the procedures and issues detailed in paragraph (4).

(6) An employee in position not considered sensitive shall go on an annual vacation of at least ten (10) consecutive days.

PART XVI – CONTRACTUAL ASPECTS

88. Cyber Security Contracts

This part covers the cyber and information security aspects of the various contracts about ICT aspects and/or cyber and information security aspects, between the institution and employees, suppliers, business partners, service providers, and customers.

(1) BoG-regulated institution shall be allowed to contract with a service provider and/or business partner only in line with following conditions:

a) Service providers and/or business partners that meet international cyber and information security standards such as ISO27000 family of standards. This is a mandatory requirement for any contract to be signed.

b) Service provider and/or business partners shall comply with this Directive with regard to their mutual activity with the institution (see also Part XII).

c) An institution shall conduct a risk survey of a service provider and/or business partner at least annually.

d) An institution and a service provider and or business partner shall include in the agreement a commitment to resolve cyber and information security incidents as swiftly as required by This Directive and/or by any other standard or regulation that binds the service provider and/or business partner. Parties to be contracted shall regard the more stringent commitment as binding and act jointly to exchange information about cyber and information security issues, including those arising as a result of lesson-learning processes after a security event occurs.

e) Repairing and improving cyber and information security issues shall be prioritised and handled without any delay whatsoever.

f) Authorisation to unilaterally terminate the contract or take any other actions as it sees fit when Senior Management finds the service provider and/or business partner is not compliant to a satisfactory degree thus creating a risk for the institution.

g) The provisions of Part XII – The Cloud Computing Service Contract – shall apply to paragraph (f).

(2) In its contracts with software vendors, an institution is required, but not limited, to refer to and include the following matters:

a) The software vendor undertakes to meet Cyber and Information Security Requirements as per best practices and commonly accepted standards in the field.

b) The institution may conduct inspections to ensure that the software vendor's work processes comply with its contractual undertakings and support development processes that diminish cyber and information security vulnerabilities. The institution shall demand that these processes are hardened if necessary.

c) In addition to the cyber and information security tests that the vendor shall perform, an institution shall test the software. Other companies specialising in software tests and in cyber and information security tests in particular may assist the institution.

d) The software maintenance provider shall meet the cyber and information security requirements stipulated in clauses 2(a), 2(b), and 2(c).

e) An institution shall include in the contract with the provider a systematic process of rapid and efficient treatment of any software vulnerability detected.

f) The institution and the provider shall agree on a process in order to resolve escalating incidents as quickly, efficiently and effectively as possible.

g) The provider is required to maintain the software's confidentiality and share the source code and all information about its development, testing and transfer to production, to be kept by the institution.

(3) In its contracts with software vendors providing off-the-shelf programs, the institution is required to include such aspects that include but are not limited to:

a) the vendors' commitment to cyber and information security issues in their software;

b) their assurance that their software has passed cyber and information security tests; and

c) The option to suspend any purchase shall the institution find that a certain software product does not meet its cyber and information security requirements.

(4) Whenever the institution develops and/or purchases hardware/software, the contract shall include a proprietary, intellectual property and copyright clauses.

(5) In every contract with service providers whose employees are required to enter the institution's premises, the providers shall take full responsibility for their employees. The contract shall include the following issues, but not be limited thereto:

a) Both the provider's management and employees shall sign a confidentiality agreement or an NDA with the institution.

b) The institution shall be entitled to examine the background of any provider employee about to be employed in its premises, as

stipulated in Section 86. The institution may specifically require that the employee pass personality and reliability tests.

c) An institution is entitled to reject any candidate who fails to meet the requirements and tests provided for in paragraph (b).

(6) In every contract with service providers hired to provide remote support, the provider shall be required to accept full responsibility for its employees, including, in particular, assurances that the provider's employees and representative shall maintain the confidentiality of all information in their possession on institutional processes, events and activities.

PART XVII – INTERPRETATION

In This Directive, unless the context otherwise requires, words used have the same meaning as assigned to them in the applicable law or as follows:

"Accountability" means:

a) the principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information (source: CNSSI-4009); and

b) The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action (source: SP 800-27).

"Advanced Encryption Standard (AES)" means the Advanced Encryption Standard Specifies a U.S. Government-Approved Cryptographic Algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits (source: FIPS 197)

"Advanced Persistent Threat (APT)" means an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives (source: SP 800-39).

"Adversary" means Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities (source: SP 800-30).

"Alert" means notification that a specific attack has been directed at an organisation's information systems (source: CNSSI-4009).

"Application" means a software program hosted by an information system. (source: SP 800-37).

"Assessment" means the testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (sources: SP 800-37; SP 800-53; SP 800-53A (See Security Control Assessment)).

"Assessment Findings" means assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a *satisfied* or *other than satisfied* condition (source: SP 800-53A).

"Asset" means a major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems (source: CNSSI-4009).

"Attack" means an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity (source: SP 800-32).

"Authentication" means verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system (sources: SP 800-53; SP 800-53A; SP 800-27; FIPS 200; SP 800-30).

"Authentication factors" means an item available to the user, such as a one-time password (OTP) created by a hardware component available to the user and connected to his account; a temporary password generated by the institution and communicated

to the customer as a text message; any other component available to the user; or a digital certificate saved on a smart card; an item known only to the user such as a permanent password; or a biometric characteristic of the user such as fingerprints, vocal or facial features.

"Automated Password Generator" means an algorithm that creates random passwords that have no association with a particular user (source: FIPS 181).

"Availability" means:

a) Ensuring timely and reliable access to and use of information (sources: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542); and

b) The property of being accessible and useable upon demand by an authorized entity (source: CNSSI-4009).

"Awareness" means activities which seek to focus an individual's attention on an (information security) issue or set of issues (source: SP 800-50).

"Baseline Security" means the minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection (source: SP 800-16).

"Blacklist" means:

a) A list of email senders who have previously sent span to a user (source: SP 800-114); and

b) A list of discrete entities, such as hosts or applications, which have been previously determined to be associated with malicious activity (source: SP 800-94).

"Candidate" means anyone being considered for employment but not yet hired by the institution. All employment categories are included in the definition.

"Cloud Computing" means a model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).

Note: Both the user's data and essential security services may reside in and be managed within (source: CNSSI-4009).

"Computer Forensics" means the practice of gathering, retaining, and analysing computer-related data for investigative purposes in a manner that maintains the integrity of the data (source: CNSSI-4009).

"Computer Security Incident Response Team (CSIRT)" means a capability set up for the purpose of assisting in responding to computer security-related incidents; also, called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Centre, Computer Incident Response Capability) (source: SP 800-61).

"Content Filtering" means the process of monitoring communications such as email and Web pages, analysing them for suspicious content, and preventing the delivery of suspicious content to users (source: SP 800-114).

"Computer Forensics" means the practice of gathering, retaining, and analysing computer-related data for investigative purposes in a manner that maintains the integrity of the data (source: CNSSI-4009).

"Continuous Monitoring" means:

a) The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: (1) The development of a strategy to regularly evaluate selected IA controls/metrics, (2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, (3) Recording changes to IA controls, or changes that affect IA risks, and (4) Publishing the current security status to enable information-sharing decisions involving the enterprise (source: CNSSI-4009); and

b) Maintaining ongoing awareness to support organizational risk decisions (source: SP 800-137).

"Controlled Access Area/Zone" means physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance (source: CNSSI-4009).

"Controlled Access Protection" means a minimum set of security functionalities that enforces access control on individual users and makes them accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation (source: CNSSI-4009).

"Controlled Area/Zone" means any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system (source: SP 800-53).

"Controlled Space" means three-dimensional space surrounding information system equipment, within which unauthorized individuals are denied unrestricted access and are either escorted by authorized individuals or are under continuous physical or electronic surveillance (source: CNSSI-4009).

"Countermeasure" means:

a) Actions, devices, procedures, or techniques that meet or oppose (i.e., counter) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. (source: CNSSI-4009); and

b) Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards (source: SP 800-53; SP 800-37; FIPS 200).

"Cyber Attack" means:

a) An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying; or

b) Maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information (source: CNSSI-400).

"Cyber Incident" means:

a) Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident (source: CNSSI-4009); and

b) An event during which computer systems and/or computer-embedded systems are attacked by, or on behalf of, adversaries (external or internal to the banking corporation), which could lead to the materialization of cyber risk. It shall be noted that this definition includes an attempt to carry out such an attack even if no actual damage is caused.

"Cyber Incident Alert" means a notification that refers to an imminent cyber incident, or to an incident that has already occurred, or is still occurring, but has not yet been identified by the entity under attack.

"Cyber Incident Management" means a structured process that refers to following stages:

a) *Detection* – initial inquiry concerning the occurrence of a cyber incident and the rapid formulation, as soon as possible, of the mode of operation required for next steps.

b) *Analysis* – a comprehensive and in-depth inquiry regarding the cyber incident to enable operative decision making, formulation of possible counter measures to thwart the attack, and a recommendation for the primary mode of operation for the containment stage.

c) *Containment* – achieving initial control of the incident to prevent escalation. Conducting a process of neutralizing the attack vectors within the banking corporation, and preventing damage escalation.

d) *Eradication* – neutralizing the attack elements located in the banking corporation's systems, while striving to remedy or mitigate the damage that has already been inflicted.

e) *Recovery* – resume normal operation and complete activity at the targeted banking corporation whose operation was shut down, limited or disrupted. Each stage includes reporting to the relevant internal and external entities.

"Cyber Infrastructure" includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example, computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure (source: NISTIR 7628).

"Cyber Risk" means the potential for damage resulting from an occurrence of a cyber incident, taking into account its probability and its impact.

"Cyber security" means the ability to protect or defend the use of cyberspace from cyber-attacks (source: CNSSI-4009).

"Cyber Threat" means a threat of occurrence of a cyber incident.

"Damage" means an adverse outcome, including disruption/disturbance/activity shut down; theft of an asset; intelligence gathering; harm to reputation/ public trust.

"Data Asset" means:

a) Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or Web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a Web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset; and
b) An information-based resource (source: CNSSI-4009).

"Data Integrity" means the property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit (source: SP 800-27).

"Defence Control Assessment" means activities intended to examine the adequacy of actual implementation of defence controls (administration, operational and technical), their regular operation, and their effectiveness vis-à-vis applicable defence requirements.

"Demilitarised Zone (DMZ)" means:

a) An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied (source: SP 800-41); or
b) A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet (source: SP 800-45); or

c) Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance Policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks (source: CNSSI-4009).

"Denial of Service (DoS)" means the prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided) (source: CNSSI-4009).

"Direct Connectivity" is connection done directly, for instance, a direct communication line between the parties under the Wide-Area Network (WAN).

"Disaster Recovery Plan (DRP)" means management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan (source: CNSSI-4009).

"Disruption" means an unplanned event that causes an information system or major applications, to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction) (sources: SP 800-34, CNSSI-4009).

"Distributed Denial of Service (DDoS)" means a Denial of Service technique that uses numerous hosts to perform the attack (source: CNSSI-4009).

"Electronic Banking Service" levels

- Service level 1: Transferring account information from the institution to the customer.
- Service level 2: Performing transactions in customer accounts.
- Service level 3: Performing transactions for a third party determined in advance by a beneficiary list.

- Service level 4: Performing money transfers to accounts not included in the previous service levels.

"E-Banking" means retrieval of information on accounts of a customer of the banking corporation or executing transactions or instructing to execute transactions initiated by the banking corporation's customer via communication systems connected to the banking corporation's computer that use a communications network (such as: telephony, Internet, cellular) or a combination of the above.

"Employee" means the term employee refers to persons the institution employees both directly and indirectly such as contractors, temporary, and outsourced employees, or anyone employed by any legal entity that provides services to the institution, whether on a regular or occasional basis.

"End-to-End Encryption" means:

a) Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible (source: SP 800-12); or

b) Encryption of information at its origin and decryption at its intended destination without intermediate decryption (source: CNSSI-4009).

"End-to-End Security" means safeguarding information in an information system from the point of origin to the point of destination (source: CNSSI-4009).

"Entity" means an institution, employee, including a contractor, outsourced person, vendor, business partner employed, applications and specific hardware.

"Event" means:

a) Any observable occurrence in a network or system (source: SP 800-61); and

b) Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring (source: CNSSI-4009).

"External Information System Service Provider / Service provider" means a provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures;

business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges (sources: SP 800-37; SP 800-53).

"External Network" means a network not controlled by the organization (sources: SP 800-53; CNSSI-4009).

"Financial Institutions" means an entity that may be either a depository financial institution such as a commercial bank, savings and loans company, mutual savings company, credit union or a non-depository financial institution such as a brokerage firm, insurance company, pension fund, investment company, which carries on the business of or part of whose business is any of the following activities:

a) taking of deposits of money from the public repayable on demand and withdrawable by cheques, drafts, orders or by other means;
b) financing of any activity by way of creating financial assets such as loans and advances, securities, bank deposits or otherwise, other than its own;
c) companies dealing in shares, stocks, bonds or other securities;
d) leasing, letting or delivering goods to a hirer under a hire purchase agreement;
e) carrying on by insurance companies of any business other than insurance;
f) collecting of money or accepting employer contributions and paying it out for legitimate claims or for retirement benefits (sources: Bank of Ghana Act, 612 clause 69 (2002)).

"Firewall" means:

a) A gateway that limits access between networks in accordance with local security policy (source: SP 800-32); or
b) A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy (source: CNSSI-4009).

"Forensics" means the practice of gathering, retaining, and analysing computer-related

data for investigative purposes in a manner that maintains the integrity of the data (source: CNSSI-4009).

"Guard (System)" means a mechanism limiting the exchange of information between information systems or subsystems (source: CNSSI-4009).

"Hacker" means unauthorized user who attempts to or gains access to an information system (source: CNSSI-4009).

"Identification" means the process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system (source: SP 800-47).

"Identity" means a set of attributes that uniquely describe a person within a given context (source: SP 800-63).

"Incident" means:

a) A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (source: SP 800-61).
b) An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (source: CNSSI-4009).

"Incident Correlation" means correlating different incidents using techniques such as statistics and artificial intelligence.

"Incident Handling" means the mitigation of violations of security policies and recommended practices (source: SP 800-61).

"Indicator" means a sign that an incident may have occurred or may be currently occurring (source: SP 800-61).

"Information Security" means the protection of information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

(sources: SP 800-37; SP 800-53; SP 800-53A; SP 800-18; SP 800-60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542).

"Information Security Continuous Monitoring (ISCM)" means maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analysed at a frequency sufficient to support risk-based security decisions to adequately protect organization information (source: SP 800-137).

"Information Security Operations Centre (ISOC)" means the facility where all ICT equipment, applications, infrastructure, data centre, network, and all endpoints are monitored, assessed and defended. The ISOC is associated with SOC which is related to people, processes and technology involved in providing detection, containment and remediation of IT and cyber threats (source: HP).

"Information Security Policy" means Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information (sources: SP 800-53; SP 800-37; SP 800-18; CNSSI-4009).

"Information Security Risk" means the risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See Risk (source: SP 800-30).

"Information System-Related Security Risks" means Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation),

individuals, other organizations, and the Nation. See Risk (source: SP 800-37; SP 800-53A).

"Intrusion" means unauthorized act of bypassing the security mechanisms of a system (source: CNSSI-4009).

"Intrusion Detection Systems (IDS)" means hardware or software product that gathers and analyses information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations) (source: CNSSI-4009).

"Intrusion Detection and Prevention System (IDPS)" means software that automates the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents and attempting to stop detected possible incidents (source: SP 800-61).

"Intrusion Prevention System(s) (IPS)" means system(s) able to detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets (sources: SP 800-36; CNSSI-4009).

"IT Security Awareness (or just Awareness)" means the purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly (source: SP 800-50).

"IT Security Awareness and Training Program" explains proper rules of behaviour for the use of agency IT systems and information. The program communicates IT Security Policies and Procedures that need to be followed (source: SP 800-50).

"Least Privilege" means:

a) The security objective of granting users only those accesses they need to perform their official duties (source: SP 800-12); and

b) The principle that a security architecture shall be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function (source: CNSSI-4009).

"Malicious Code" means software or firmware intended to perform an unauthorized process that shall have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (sources: SP 800-53; CNSSI-4009).

"Malware" means:

a) A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim (source: SP 800-83); or

b) A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host (source: SP 800-61).

"Mobile Device" means:

a) Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory).

b) Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) (source: SP 800-53).

"Mutual Authentication" occurs when parties at both ends of a communication activity authenticate each other (source: SP 800-32).

"Need-To-Know" means a method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-

know is generally applied to people, while least privilege is generally applied to processes (source: CNSSI-4009).

"Non-repudiation" means:

a) Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information (sources: CNSSI-4009; SP 800-60); or

b) A service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (i.e., the signatory) (source: FIPS 186).

"Penetration" (see Intrusion).

"Penetration Testing" means:

a) Documentation (e.g., system design, source code, manuals) and working under specific constraints, in attempt to circumvent the security features of an information system (source: SP 800-53A); or

b) Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves conducting real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability (source: SP 800-115).

"Perimeter" means all system components that are to be accredited by the CISO, and excludes separately accredited systems to which the system is connected. (Authorization) Encompasses all those components of the system or network for which a body of evidence is provided in support of a formal approval to operate (source: CNSSI-4009).

"Post-Incident Activity" means a structured process that refers to following stages:

a) *Investigation and lessons learned* – a process of inquiry and methodological analysis of the response to and management of the entire cyber incident, from beginning to end, from the perspectives of people, processes and technology. The investigation is carried out, as soon as possible, upon concluding the operative management of the incident in order to provide insights and lessons that shall improve and expedite a more efficient response to future cyber incidents.

b) *Monitoring the implementation of lessons and insights* – a process intended to ascertain that all recommendations and insights raised during the incident are implemented.

"Privacy" means restricting access to subscriber or 'relying party' information in accordance with law and regulations (source: SP 800-32).

"Proxy" means an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, Hyper Text Transfer Protocol (HTTP) proxy which is used for Web access, and Simple Mail Transfer Protocol (SMTP) proxy used for email (source: SP 800-44).

"Remediation" means the act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings and uninstalling a software application (source: SP 800-40).

"Remediation Plan" means a plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation (source: SP 800-40).

"Residual Risk" means the remaining potential risk after all IT security measures have been applied. There is a residual risk associated with each threat (source: SP 800-33).

"Resilience" means the ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a timeframe consistent with mission needs (source: SP 800-137).

"Risk" means:

a) The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring (source: SP 800-60); or

b) A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

   i. the adverse impacts that would arise if the circumstance or event occurs; and

   ii. the likelihood of occurrence.

   Note: Information system-related security risks are those that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. Adverse impacts to the nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations (source: SP 800-37; SP 800-53A).

"Risk Analysis" means the process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional

safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment (source: SP 800-27).

"Risk Assessment" means the process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. It uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF) (source: CNSSI-4009).

"Risk Management" means the process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system, and includes:

- the conduct of a risk assessment;
- the implementation of a risk mitigation strategy; and
- employment of techniques and procedures for the continuous monitoring of the security state of the information system (sources: SP 800-53; SP 800-53A; SP 800-37).

"Risk Management Framework" means a structured approach used to oversee and manage risk for an enterprise (source: CNSSI-4009).

"Risk Mitigation" means prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process (sources: CNSSI-4009; SP 800-30; SP 800-39).

"Risk Monitoring" means maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions (sources: SP 800-30; SP 800-39).

"Safeguards" means protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures (sources: SP 800-53; SP 800-37; FIPS 200; CNSSI-4009).

"Sandboxing" means a method of isolating application modules into distinct fault domains enforced by software. The technique allows untrusted programs written in an unsafe language, such as C, to be executed safely within the single virtual address space of an application. Untrusted machine interpretable code modules are transformed so that all memory accesses are confined to code and data segments within their fault domain. Access to system resources can also be controlled through a unique identifier associated with each domain (source: SP 800-19).

"Security Association" means a relationship established between two or more entities to enable them to protect data they exchange (source: CNSSI-4009).

"Security Control Assessment" means the testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (sources: SP 800-37; SP 800-53; SP 800-53A).

"Security Control Effectiveness" means the measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance (source: SP 800-137).

"Security Controls" means the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

(sources: SP 800-53; SP 800-37; SP 800-53A; SP 800-60; FIPS 200; FIPS 199; CNSSI-4009**).**

"Security Information and Event Management (SIEM)" tools are a type of centralized logging software that can facilitate aggregation and consolidation of logs from multiple information system components, audit record correlation and analysis, correlation of audit record information with vulnerability scanning information in order to determining the veracity of the vulnerability scans and correlating attack detection events with scanning results (source: SP 800-137).

"Security Operations Centre" (see Information Security Operations Centre (ISOC)).

"Security Perimeter" means a physical or logical boundary that is defined for a system, domain, or enclave, within which a particular security policy or security architecture is applied (source: CNSSI-4009).

"Security Policy" means:

a) The statement of required protection of the information objects (source: SP 800-27); or

b) A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data (source: FIPS 188).

"Security Requirements" means requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted (sources: FIPS 200; SP 800-53; SP 800-53A; SP 800-37; CNSSI-4009).

"Security Safeguards" means protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices (source: CNSSI-4009).

"Senior Management" means the highest level of managers in the institution, immediately below the board of directors. Its members actively participate in the daily

supervision, planning and administrative processes required by a business to help meet its objectives. The Senior Management of a corporation is often appointed by its Board of Directors and approved by Stockholders (sources: Business Directory; Oxford Dictionary).

"Sensitivity" means a measure of the importance assigned to information by its owner for the purpose of denoting its need for protection (sources: SP 800-60; CNSSI-4009).

"Sensitive Position" is defined as one, which if attacked or if an attack against it is leveraged/ exploited, directly or indirectly, can cause serious and extensive damage to the institution.

"Social Engineering" is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious (source: SP 800-114).

"Supply Chain" means a system of organizations, people, activities, information, and resources, possibly international in scope that provides products or services to consumers (source: SP 800-53; CNSSI-4009).

"System Integrity" means the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental (source: SP 800-27).

"Technical Controls" means the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system (sources: SP 800-53; SP 800-53A; SP 800-37; FIPS 200).

"Test" means a type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behaviour, the results of which are used to

support the determination of security control effectiveness over time (source: SP 800-53A).

"Threat" means any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability (source: FIPS 200).

"Threat Analysis" means the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment (source: SP 800-27).

"Threat Assessment" means process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat (source: CNSSI-4009; SP 800-53A).

"Threat Event" means an event or situation that has the potential for causing undesirable consequences or impact (source: SP 800-30).

"Threat Monitoring" means analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security (source: CNSSI-4009).

"Threat Scenario" means a set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time (source: SP 800-30).

"Total Risk" means the potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability) (source: SP 800-16).

"Unauthorized Access" occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use (source: FIPS 191).

"Vulnerability" means weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (sources: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200).

"Vulnerability Assessment" means systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation (sources: SP 800-53A; CNSSI-4009).

"Web Application Firewall (WAF)" means a proactive defence against web application attacks that offers protection against zero-day attacks which antivirus signatures cannot detect.

PART XVIII – ANNEX A - IMPLEMENTATION SCHEDULE

Ch. No.	Chapter / content	Implementation Schedule (no later than)
	PART I – PRELIMINARY MATTERS	6 months
	PART II– GOVERNANCE	6 months except ISO 27001, PCI-DSS, ISMS Management within 12 months
	PART III – THE CHIEF INFORMATION SECURITY OFFICER	6 months
	PART IV – CYBER SECURITY RISK MANAGEMENT	12 months except risk mitigation, surveys, assessments, mitigation and reporting within 6 months
	Cyber and Information Security Policy and Procedures	6 months
	Cyber and Information Security Management Framework	6 months
	PART V – ASSET MANAGEMENT	12 months
	PART VI – CYBER DEFENCE	See details below except data integrity 36 months
22	Security Infrastructure	24 months
23	Architecture	24 months
24	Network Elements	12 months
25	Network Management	12 months
26	Encryption	12 months
27	Media Encryption	12 months
28	Remote Access	24 months
29	Internet Access	24 months
30	Website Protection	24 months except database protection within 12 months
31	Access Control and Authentication	24 months except Identity management 36 months
32	Biometric Authentication	24 months
33	Compartmentalization and Permissions	12 months

Ch. No.	Chapter / content	Implementation Schedule (no later than)
34	Servers and Workstations	12 months
35	Databases	12 months
36	Software Information Security	24 months
37	Auditing	12 months
38	Incident Preparedness	12 months
39	Research	12 months
	PART VII – CYBER RESPONSE	12 months
	PART VIII – EMPLOYEE ACCESS TO ICT SYSTEMS	12 months except BYOD and institutional mobile devices 24 months, data integrity requirements 36 months
	PART IX – ELECTRONIC BANKING SERVICES	24 months except establishment of fraud monitoring 12 months
	PART X – TRAINING, AWARENESS AND COMPETENCE	12 months
	PART XI – EXTERNAL CONNECTIONS	24 months, except data in motion 36 months
	PART XII – CLOUD SERVICES	12 months with exclusions for existing contracts / cloud services for 24 months
	PART XIII – BANKS WITH INTERNATIONAL AFFILIATION	24 months
	PART XIV – PHYSICAL SECURITY	12 months (some of it is already being enforced)
	PART XV – HUMAN RESOURCE MANAGEMENT	24 months
	PART XVI – CONTRACTUAL ASPECTS	12 months with exclusions for existing contracts / services for 24 months

PART XIX – Annex B - Enhanced Competency Framework

89. Guide to Enhanced Competency Framework (ECF) on Cyber Security

1. All institutions are encouraged to use this ECF to raise and maintain professional competence of their cyber security practitioners. The framework is not a mandatory licensing regime, however, it is expected that institutions will adopt it to enable cyber security talent and build the professional competencies and capabilities of staff involved in cyber security responsibilities.
2. The ECF is aimed at a new entrant or an existing practitioner engaged by an institution to perform in roles ensuring operational cyber resilience. For the purpose of the ECF, institutions may have key roles based on the three lines of defence concept under cyber risk governance.
   a. First line of defence: IT Security Operations and Delivery
   b. Second line of defence: IT Risk Management and Control
   c. Third line of defence: IT Audit
3. Employees performing key roles solely in the information technology operating function of the institution, such as system developers, system operators, helpdesk operators, and IT support are excluded.
4. The proposed qualification structure of the ECF may comprise the following two levels based on the year of work experience.
   a. Core Level - This level is applicable for entry-level staff with less than 5 years of relevant work experience in the cybersecurity function.
   b. Professional Level - This level is applicable for staff with 5 and above years of relevant work experience in the cybersecurity function.
5. Under the qualification structure, the following list of recognised certificates are encouraged.

	First Line of Defence	Second Line of Defence	Third Line of Defence
RECOGNISED CERTIFICATES	**IT Security Operations and Delivery**	**IT Risk Management and Control**	**IT Audit**
Core Level			
CSX Fundamentals Certificate	✓	✓	✓
CSX Practitioner Certificate (CSX-P)	✓	✓	✓
Cybersecurity Audit Certificate		✓	✓
GIAC Information Security Professional (GIAC GISP)	✓	✓	
GIAC Security Essentials (GSEC)	✓	✓	✓
ISC² Systems Security Certified Practitioner (SSCP)	✓		
Professional Level			
Certified Information Systems Auditor (CISA)	✓	✓	✓
Certified Information Security Manager (CISM)	✓	✓	✓
Certified in Risk and Information Systems Control (CRISC)		✓	
Certified in the Governance of Enterprise IT (CGEIT)		✓	
ISC² Certified Information Systems Security Professional (CISSP)	✓	✓	✓
ISC² Certified Cloud Security Professional (CCSP)	✓	✓	

6. Where the qualifications held by staff are different from the qualifications above, the institution may apply judgement in evaluating such qualifications and see if those qualifications are equivalent qualifications. The institution may determine the equivalence based on the following three factors:
    a. recognition of the qualification by the local industry;
    b. technical qualification of the certificates; and
    c. ethical requirement of the qualification.

7. Staff who have successfully obtained the qualifications listed under Section 5 should fulfil the Continuing Professional Development (CPD) requirement of the relevant certification scheme.

PART XX – Annex C – Return on Cyber Security Incidents

90. Return on Cyber and Information Security Incidents

Institution Name:

Reporting Period:

Date of incident Detection	Type of incident[a]	Summary of incident	Physical location/ branch (if applicable)	Estimated/actual impact of the incident (Financial and Operational)[b]	Internal reporting Authority[c]	Law enforcement authorities involved (if applicable)

Notes:

a) **Type of incident:** Intrusion/hacking, Malware, Malicious code, Virus, Phishing, Denial of service, social engineering, unauthorized system usage, Other(specify)

b) Please provide the amount in case of financial impact and description in case of operational impact

c) To whom the event has been internally escalated.

NB: This return shall be emailed to bsd@bog.gov.gh with the title "Return on Cyber Security Incidents"