# CISD 2026

# CYBER AND INFORMATION SECURITY DIRECTIVE

MARCH 2026

# CYBER AND INFORMATION SECURITY DIRECTIVE

MARCH 2026

# PREFACE

In recent years, cyber-related systems and networks have played an increasingly critical role in the financial sector. The financial sector relies heavily on these infrastructures to support its core operations, making them attractive and susceptible targets for cyberattacks. Being high-profile targets creates a distinct challenge for Regulated Financial Institutions (RFIs), 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 RFIs 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 weaknesses or vulnerabilities within the cyber and information security defences of financial systems.

This document outlines the framework for Cyber and Information Security procedures for both routine operations and emergency situations. It also sets out roles, communication procedures, reporting mechanisms, physical security requirements, and measures to protect data and network systems.

# Table of Contents

# PART I - PRELIMINARY MATTERS

## 1. OBJECTIVE

The overall objective of this Directive is for RFIs to establish, implement, maintain and continually improve a cyber and information security management system to ensure Confidentiality, Integrity and Availability (CIA) of information assets. Specifically to:

1. Create a secure digital environment for the RFIs, fostering trust and confidence in ICT systems and ensuring the integrity of transactions conducted within 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 digital 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 operation of information resources;
5. Maintain a high level of digital operational resilience ensuring the financial services industry can withstand, respond to, and recover from ICT-related disruptions and cyber threats;
6. Improve the integrity of financial products and services by establishing a framework for testing and validating the safety of these products and services;
7. Promote effective third-party risk management;
8. Promote continuous cyber and information security risk assessment; and
9. Promote awareness creation and ensure human resource security.

## 2. APPLICABILITY

This Directive is issued under the powers conferred by Section 4 of Bank of Ghana Act 2002 as amended, Section 92(1) of the Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930), as well as Section 84 of the Development Finance Institutions Act, 2020 (Act 1032).

This Directive shall apply to:

a. Institutions licensed or registered under the Banks and Specialised Deposit-Taking Institutions Act, 2016 (Act 930);
b. Institutions licensed under the Development Finance Institutions Act, 2020 (Act 1032);
c. Institutions licensed under the Non-Bank Financial Institutions Act, 2008 (Act 774);
d. Institutions licensed under the Payment Systems and Services Act, 2019 (Act 987);
e. Institutions licensed under the Credit Reporting Act, 2007 (Act 726);
f. Institutions licensed under the Foreign Exchange Act, 2006 (Act 732);
g. Institutions licensed under the Virtual Service Providers Act, 2025 (Act 1154); and
h. Any other institution licensed or regulated by Bank of Ghana under any other enactment, collectively referred to in this Directive as RFIs.

Failure to comply with the provisions contained in this Directive will attract appropriate sanctions in accordance with applicable laws.

## 3. PROPORTIONALITY AND CASE-BY-CASE ASSESSMENT

1. In recognising the diverse operational environments of regulated financial institutions, this Directive introduces a proportional implementation approach to ensure that cybersecurity requirements are applied in a manner that aligns with the size, complexity, risk exposure, and technological maturity of each institution.
2. The Directive sets a unified baseline for cyber and information security resilience, it acknowledges that institutions differ significantly in their business models, resource capacity, operational scale, and digital infrastructure. Refer to Annexure A – Proportionality Framework for implementation guidance.
3. The determination of applicable provisions of the CISD for any RFI shall be based on that institution's assessed Cyber and Information Security risk profile. This determination shall be made notwithstanding the RFI's classification, however, the final classification will be based on Bank of Ghana's assessment and approval.

## 4. OBLIGATIONS OF REGULATED ENTITIES

RFIs shall:

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 resilience to operational disruptions due to the materialisation of cyber and information security risks; reduce their impact on the RFI's business continuity; and to minimise damage to its ICT assets and information as well as those of its customers (see PART VI for the definition of asset).
4. Determine the extent of the implementation process while seeking to maintain a degree of flexibility as required by the unique nature of this Directive.
5. Manage its cyber and information security risks with a systemic, organisation-wide view, within the framework of Ghanaian law and subject to its Directive pertaining to risk, operational risk, business continuity, and ICT management.
6. Manage its operational risks, identify, document and address the cyber and information security 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. Be ISO/IEC 27001 certified and adopt ISO/IEC 27032.
10. An RFI, including its agents that handle, process, store, or transmit debit card, credit card, prepaid card, e-purse, ATM cards, and/or POS and related information be PCI-DSS certified.
11. Ensure that methodology for managing and handling cyber and information security events complies with international standards such as National Institute of Standards and Technology (NIST) and International Organisation for Standardisation (ISO).
12. An RFI shall have the responsibility to conduct due diligence on its third-party service providers and suppliers to ensure they meet the cybersecurity standards outlined in this Directive.

# PART II - GOVERNANCE

## 5. THE BOARD

The Board of an RFI shall have the overall responsibility for complying with the directive in addition to the following:

1. Approve the RFI's cyber and information security risk management strategy.
2. Approve institutional policies of cyber and information security, access identification and authentication, outsourcing, survivability, backup and recovery from cyber incidents and attacks, and disaster events.
3. Appoint a Board Committee on Cyber and Information Security risks and countermeasures with a well-defined charter. At least one member of the Board shall possess verifiable qualification or expertise in Cyber and Information Security Risk Management.
4. Approve the annual and other work plans for cyber and information security, business continuity and disaster recovery.
5. The Board shall review and approve the RFIs annual cyber and information security budget.
6. Receive quarterly reports on all cyber and information security incidents and cyber and information security Key Performance Indicators (KPI) and exercise its oversight responsibility.
7. Receive immediate reports on significant cyber and information security incidents and exercise oversight responsibility.
8. Hold an annual discussion about the adequacy of the RFI's cyber and information security policies and strategies.
9. State and extend its support for inter-institutional collaboration on cyber and information security defence.
10. Ensure effective internal controls and risk management practices are implemented to achieve security, reliability, availability, resiliency, and recoverability.
11. Approve all new cyber and information security related products and services.

## 6. THE SENIOR MANAGEMENT

The Senior Management of an RFI shall have the following responsibilities:

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. Review policies in paragraph 6(2) at least once every two (2) years or when significant changes occur.
4. Allocate the necessary resources for the institutional cyber and information security framework and policies.
5. Hold a meeting at least twice a year to review the implementation and effectiveness of the RFI'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. Review significant cyber and information security incidents and analyse their implications and report to the Board promptly.
8. Appoint a Cyber and Information Security Risk Management Committee with a well-defined charter.
9. Promote inter-institutional collaboration on cyber and information security defence.
10. Report to Bank of Ghana, all significant and suspected cyber and information security incidents immediately.
11. Senior Management should understand the risks associated with ICT Outsourcing. A due diligence report should be prepared before a service provider is appointed.

## 7. INTERNAL AUDITS

1. The RFI shall ensure that an independent internal unit is responsible for auditing Cyber and Information Security.
2. Senior Management shall allocate adequate resources for the audit function and 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 RFI.
4. An audit shall review the RFIs 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. Where internal cyber and information security audits are conducted through outsourced service providers, the responsibility for evaluating and validating audit findings shall rest solely with the RFI's internal audit unit or Senior Management.
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.

## 8. INFORMATION SECURITY DEPARTMENT

1. **Governance & Structure:** The RFI shall establish a dedicated Information Security Department with clear responsibilities, authority and accountability led by the Chief Information Security Officer (CISO).
2. **Protected Funding:** Secure an independent, adequate budget that does not compete with Information Technology (IT) components, covering personnel, solutions, and training.
3. **Skilled Personnel:** Build a team with diverse expertise, invest in competitive compensation and continuous skill development, with clearly established career paths.
4. **Technology, Safeguards, and Security Solutions:** Implement an enterprise security architecture (based on security layers) with integrated solutions for prevention, detection, and response, tailored to the RFIs information systems and technology environment.
5. **Operational Resilience:** Maintain readiness through including but not limited to adaptive security framework, ongoing risk assessments, proactive threat intelligence, periodic incident simulations, and a culture of continuous improvement.

## 9. INFORMATION SECURITY BUDGET MANAGEMENT

1. Cybersecurity budget which includes cybersecurity activities and solutions, shall be allocated to the cybersecurity department. This budget shall be sufficient to achieve the required level of cyber preparedness.
2. Crucially, it must be separate from the general IT budget to prevent competition for funds between system and technology management and security protection.

# PART III - THE CHIEF INFORMATION SECURITY OFFICER

## 10. APPOINTMENT

1. The Board of an RFI shall appoint a Chief Information Security Officer (CISO) subject to the prior written approval by Bank of Ghana.
2. The CISO shall be competent on the basis of appropriate education, training and experience.
3. The CISO shall not hold any other position or bear any additional responsibility in the RFI which can bring him/her into conflict in relation to his/her responsibilities.
4. The RFI shall provide the CISO with all the resources necessary to fulfil his/her duties.

## 11. STATUS IN THE INSTITUTIONAL HIERARCHY

1. The CISO shall be a Senior Management person and shall possess adequate authority, independence and status within the RFI to enable him/her function adequately.
2. The CISO shall report directly to the Managing Director/Chief Executive Officer and have unfettered access to the Board.

## 12. RESPONSIBILITIES

The CISO shall:

1. Advise Senior Management and Board on Cyber and Information Security Management.
2. Develop a cyber security strategy and programme in line with the RFIs business strategy.
3. Formulate an institutional methodology for managing cyber and information security risks.
4. Develop the RFI's Cyber and Information Security policies and submit it to Senior Management and Board for approval.
5. Develop and update specific and general work procedures to align with the RFI's cyber and information security policy.
6. 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 RFI's technological and business activities;
    b. The controls required to ensure systems confidentiality, integrity and availability; and
    c. The level of residual risk and exposure to cyber and information security threats the RFI is willing to accept in implementing these activities.
7. Integrate and coordinate all institutional cyber and information security efforts, including oversight and control of all institutional units participating in these efforts.
8. Create a framework for receiving ongoing and ad-hoc reports from various institutional units.
9. 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 departments, offices, units and branches to deal with a cyber-attack; and

   b. Once a year, an exercise shall be undertaken to assess the preparedness of the entire RFI to withstand cyber-attacks.
10. Coordinate cyber and information security activities, including joint exercises with business partners and service providers.
11. Personnel of an RFI and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of its information security and topic-specific policies and procedures, as relevant for their role.
12. 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.
13. Form a Cyber-Incident Response Team (CIRT) capable of executing the full lifecycle if incident handling, including detection, analysis, containment, and post-incident reporting.
14. Analyse cyber and information security incidents that have occurred in Ghana and worldwide, and assess their potential impact on the RFI, as well as implement the relevant measures proposed.
15. Develop metrics and indicators to assess the effectiveness of cyber and information security systems and procedures.
16. Assess regular and ad-hoc institutional cyber and information security controls.
17. Draw up annual work plans, including budgeting, prioritisation and schedules for implementing the assessment processes.
18. 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.
19. Be responsible for collaborating with relevant RFIs involved in cyber and information security issues.
20. Submit reports on major cyber and information security incidents to Bank of Ghana.

# PART IV - CYBER AND INFORMATION SECURITY POLICY AND PROCEDURES

## 13. POLICY

1. Policies for managing cyber and information security risks shall be presented to and approved by the Board. These policy documents shall cover at least the following areas:
    a. The cyber threat environment and its potential impact on the RFI;
    b. The RFI's approach to managing cyber and information security risks and in determining and monitoring the level of exposure to cyber and information security threats; and
    c. The principles behind implementing cyber and information security measures.
    d. The cyber and information security change management process.
    e. The policy shall align with all relevant laws and regulations, as well as international cyber and information security standards such as ISO/IEC 27000 family of standards.
2. The policy shall be reviewed at least once every two (2) years regardless of and in addition to whatever updates are required during this time.
3. Senior Management is responsible for writing a framework document about managing the RFI'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; and
    c. Description of the RFI's risk assessment and management processes and methods and how they are to be utilised and reported.
4. Senior Management shall define the RFI's cyber and information security policy in line with this Directive (see PART II paragraph 6)). This policy document shall be consistent with the RFI's cyber and information security strategy. It shall refer to all controls and methods for achieving the RFI's cyber and information security targets and shall be reviewed at least once every two years, or where there are significant changes in the RFIs environment.
5. The cyber and information security policy document shall 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 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 or third parties ;
    j. The use of implementation, maturity and effectiveness indicators to assess the RFI's cyber and information security controls; and

   k. Evaluation, control and reporting on cyber and information security risk management.
6. Specific policies for implementation of security controls shall be formulated based on the overall cyber and information security policy and be updated regularly.

## 14. PROCEDURES

1. Based on the institutional cyber and information security policy, specific procedures shall be developed to cover cyber and information security activities and approved by Senior Management.
2. Procedures shall be detailed and related to each stage, process and unit involved in managing operations, security, backup, survivability, recovery and control.
3. Senior Management shall implement compliance processes to verify that information and cyber security policies are enforced.
4. The procedures shall be reviewed on an annual basis or as required following changes in the relevant business or technological environment.

## 15. THE CYBER AND INFORMATION SECURITY RISK MANAGEMENT COMMITTEE

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

1. The Committee shall include at least three members appointed by the Senior Management with the Chief Executive Officer(CEO)/Managing Director(MD) as Chairperson (in the absence the CEO/MD, the Deputy Managing Director(DMD) shall act as Chairperson); the Chief Risk Officer (CRO), Chief Information Officer(CIO)/Chief Technology Officer (CTO) and the CISO. The Board shall approve The Committee's composition with terms of reference.
2. The Committee shall help Senior Management to make decisions and to fulfil its responsibilities in the field of cyber and information security, including the RFIs resilience to cyber attacks.
3. The Committee shall at a minimum discuss and monitor the following:
   a. Implementation of plans and activities to reduce cyber and information security risks, including the RFIs resilience to cyber attacks;
   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 and outsourcing institutional systems.
4. The Committee shall meet at least quarterly and document its discussions.
5. The Committee shall report to the Board Committee on Cyber and Information Security 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 Committee shall report its activities, conclusions and recommendations to the Board.

# PART V - CYBER AND INFORMATION SECURITY RISK MANAGEMENT

This part establishes the framework for managing cyber and information security risks within RFIs. It outlines a structured and proactive approach to identifying, analysing, evaluating, treating, monitoring and reporting risks that could affect the confidentiality, integrity, and availability of information assets.

## 16. RISK MANAGEMENT

Risk management shall be integrated into the RFI's overall enterprise risk management framework and applied from a cross-organisational perspective, considering both technological and human elements. The Committee shall oversee the process, ensuring that risks are continuously monitored, mitigated, and reported to Senior Management and the Board for informed decision-making.

1. Managing cyber and information security risks is part of the overall risk management in the RFI.
2. The RFI, in its institutional risk management process, shall include emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) among all categories of risks.
3. An RFI shall manage the cyber and information security risks together with operational, business continuity and Information and Communication Technology (ICT) risks.
4. When addressing matters related to business continuity, an RFI shall also evaluate cyber and information security risks that may affect its own operations and those of its suppliers and service providers including affiliates. An RFI shall also consider the availability of supportive infrastructures and any other relevant issues.
5. The institutional risk management process shall rely on well-known methodologies that incorporates threat intelligence, surveys, tests and other relevant risk assessment and mitigation mechanisms.
6. The supply chain cyber-risk view shall include mapping of direct and indirect dependencies, concentration risk, tier-n suppliers, as well as cascading, systemic, or transitive dependencies.
7. The Committee shall be responsible for reporting to the Board Committee on cyber and information security issues. This report shall include but not limited to the following:
    a. Cyber and information security risks;
    b. Newly discovered threats, both within Ghana and worldwide, and their possible impact on the RFI;
    c. Security breaches in the RFI and their implications; and
    d. Required changes in the RFI's cyber and information security system due to these breaches and changes in the national and global threat environment.
8. An RFI shall evaluate the necessity of obtaining dedicated cyber and information security insurance as a component of its risk transfer strategy. This evaluation shall base on a formal risk assessment that considers factors such as risk appetite, potential financial impact of potential cyber incidents, residual risk after technical controls, and best practice requirements. Any policy obtained must be periodically reviewed to ensure alignment with the evolving threat landscape and organisational risk profile.

## 17. RISK IDENTIFICATION

Risk identification establishes the process by which an RFI shall identify and document potential sources of information and cyber security risk.

1. Each RFI shall identify the cyber and information security threats and vulnerabilities to its environment which comprise but not limited to internal and external networks, hardware, software applications, systems interfaces, operations, procedures and people.
2. The computer security assessments and cyber and information security defence tests that must be performed regularly on the RFI's ICT systems and processes must also be performed on any new or modified systems. The assessments are designed to ensure that the systems and infrastructure are resilient; assess the effectiveness of protective measures with reference to the risk identification; and propose ways of correcting any issues discovered.
3. The RFI shall perform regular computer security assessments and cyber and information security defence tests on its ICT systems and processes and must also be performed on any new or modified systems. These assessments and tests shall:
    a. ensure that the systems and infrastructure are resilient;
    b. assess the effectiveness of protective measures with reference to the risk identification; and
    c. propose ways of correcting any issues discovered.
4. The CISO shall determine the annual work plans for conducting cyber and information security assessments and tests; types of tests; and the schedule and scope of tests. The CISO shall budget and prioritise these activities as part of an annual work plan.
5. The Committee shall discuss and approve any changes in the budget allocated for the work plan. These changes must be brought to the Board's knowledge.
6. The CISO shall ensure that critical RFI systems, business and technological processes are assessed regularly, at least once a year.
7. The CISO shall initiate controlled penetration and robustness tests for the RFI'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 RFI as high risk and/or connected directly to the internet and/or communicating outside the RFI and/or using Wide-Area Network (WAN) shall be assessed at least quarterly. The assessment shall include, among other matters, the various systems' technological infrastructures and their security and communication links.
8. Assessment findings and recommendations shall be submitted to The Committee, which shall discuss them and set a schedule for implementing the corrective measures.
9. 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.
10. Every system, new, significantly modified or repaired, outsourced, or in cloud computing systems shall be checked in cyber and information security assessments prior to moving it to the production environment.
11. Significant security assessment and penetration test findings shall be reported to Senior Management and the Board's Committee on Cyber and Information Security Risk.

## 18. RISK ANALYSIS

Each RFI 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 analysis 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 RFI as a whole.
2. An RFI shall rely on at least the following information in its risk analysis:
    a. Findings from audits, vulnerability assessments, penetration tests, and other technical reviews that may reveal potential weaknesses or breaches;
    b. External threat intelligence, vulnerability disclosures, and research from credible third-party or regulatory sources indicating potential exposures or emerging risks;
    c. Lessons learned from the RFI or industry-wide cyber incidents and related post-incident analysis;
    d. 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 and simulations to assess the likelihood and potential business impact of risk materialisation, including the institution's capacity to detect, respond, and recover; and
    f. The use of qualitative and/or quantitative metrics to assess risk exposure and prioritise treatment actions.
3. The risk analysis shall cover information assets, including ICT infrastructure, business applications, critical business processes and other cyber and information security components.
4. The risk analysis shall include third-party service providers, outsourcing arrangements, and customer-facing digital channels, to ensure a holistic assessment of external dependencies and exposures.
5. To ensure consistency and uniformity, methodologies and tools used for identifying and analysing cyber and information security risks shall be duly documented, standardised, and approved by the highest level of Management.
6. Where necessary, independent subject matter experts shall be engaged to support or validate the RFI's risk analysis in accordance with best practice (such as ISO 31000 and ISO/IEC 27005) requirements.
7. The outcomes of the risk analysis process shall be integrated into the RFI's overall risk analysis process.
8. An RFI shall continuously review and update all significant internal or external changes, including new cyber threats, technology upgrades, organisational restructuring, or major outsourcing projects.
9. The outcomes of the annual risk analysis shall be reviewed and discussed at Senior Management and Board meetings. High or emerging risks relating to interim updates and assessments shall be escalated promptly for Senior Management and Board action.

## 19. RISK ASSESSMENTS IN CLOUD ENVIRONMENT

1. In addition to paragraph 16 above, regarding the cloud environment, the RFI must include cloud deployments (public, private, and hybrid) within its scope of risk identification and assessment. Risks arising from the cloud service providers (CSPs), shared responsibility models, multi-tenancy, cross-tenant attacks, Application Programming Interface (API) exposure, and dynamic scaling should be considered.
2. The risk assessment shall include, but not be limited to:

   a. The mapping of used cloud services Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and the responsibility boundaries (i.e., which controls are handled by the RFI versus the CSP).
   b. The likelihood and impact of cloud-specific attack vectors (e.g., privilege escalation, insecure API endpoints, credential compromise, container escape).
   c. Risks related to vendor lock-in, portability, and data egress costs or limitations.
   d. The resilience of the CSP's core infrastructure, including Service Level Agreements (SLAs), availability zones, disaster recovery features, and geographic segmentation.
   e. The chain of dependencies (e.g., third-party services used by CSP, supply chain risk).
3. The residual cloud risk after mitigation should be documented and included in the RFI's overall risk register. High residual risk exposures must be escalated to Senior Management and the Board, primarily when the cloud deployment hosts critical systems or sensitive data.
4. The RFI shall periodically verify (at least annually) that its cloud risk profile remains up to date, reflecting changes in usage, expansion of cloud services, or changes in CSP capabilities, contract terms, or geography.

## 20. RISK MITIGATION

An RFI 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 RFI 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 RFI 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 or update a work plan to be implemented when controls are not effective and/or need to be replaced or enhanced. The work plan, including schedule and budget, shall be formulated based on the degree of risk to the RFI on account of the non-implementation of the activity required. The work plan shall be submitted to The Committee for approval and determination of the residual risk level and discussion of its implications.
4. The CISO shall review and update the RFI's cyber and information risk controls and mitigation approach taking into account changing circumstances and variations in the RFI's risk profile.

## 21. RISK EVALUATION

Risk evaluation involves comparing the results of the risk analysis with the RFI's established risk acceptance criteria to determine which risks require treatment or escalation.

1. An RFI shall establish and maintain a documented process for evaluating identified cyber and information security risks in accordance with its approved risk assessment methodology.
2. The RFI shall:
   a. Define and approve clear likelihood and impact rating criteria consistent with its risk appetite and enterprise risk management framework;
   b. Apply a risk scoring or prioritisation mechanism to classify risks as high, medium, or low, based on quantitative or qualitative measures;
   c. Document the basis for all risk ratings and maintain traceability between identified risks, assessed controls, and evaluation outcomes.

Risks exceeding the RFI's defined acceptance threshold shall be escalated to The Committee for consideration of treatment options.

3. Residual risks that remain after mitigation shall be reviewed and approved by The Committee and reported to the Board's committee on Cyber and Information Security.
4. The CISO shall ensure that the risk evaluation results are integrated into the RFI's overall enterprise risk profile, and that periodic reviews are conducted at least once a year or whenever there are material changes to the threat landscape, business processes, or technology environment.

## 22. RISK MONITORING AND REPORTING

This paragraph sets out requirements for continuous monitoring and reporting of identified cyber and information security risks.

1. An RFI 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.
2. An RFI shall review the risk register periodically and put in place a monitoring and review process for continuous assessment and treatment of risks.
3. An RFI shall 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 RFI shall be provided to the Board and Senior Management. In determining the risk matrix, the RFI shall consider risk events, regulatory requirements and audit observations.

# PART VI - ASSET MANAGEMENT

This part covers the RFI's responsibility to analyse all ICT and data assets, determine their sensitivity and importance to the RFI, 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.

## 23. INVENTORY

1. Senior Management shall put in place an inventory register for all the RFI's ICT and information assets and allocate budget required to implement the objectives of asset management.

## 24. OWNERSHIP

1. An owner shall be designated for each asset.
2. For the purpose of this part, an owner is an individual employee or a unit in the RFI 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; and
    e. Developing, maintaining and disposing the asset.

## 25. ACCEPTABLE USE

1. Acceptable use of an asset is defined as its utilisation 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. Suppliers, service providers and all employees, including outsourced and contract employees, must comply with acceptable use requirements and shall sign a document or consent to that effect.

## 26. ASSET MAPPING AND CLASSIFICATION

1. RFIs shall maintain an up-to-date inventory of all critical ICT and information assets that support business operations. The inventory shall, at a minimum, record the asset name, owner, location and its criticality to operations.

2. Each asset shall be classified based on its criticality and sensitivity, considering factors such as:
    a. Importance to business operations;
    b. Potential impact on confidentiality, integrity, and availability if compromised; and
    c. Applicable legal or regulatory requirements.
3. The asset classification framework shall be approved by Senior Management and reviewed periodically or upon significant operational changes.
4. RFIs shall label or otherwise identify assets in accordance with their classification level to ensure appropriate protection and handling.

# PART VII - CYBER DEFENCE

## 27. SECURITY INFRASTRUCTURE

1. The principles applicable to the RFI's cyber and information security infrastructures shall be laid down in its cyber and information security policy document. These principles shall express the RFI'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.
2. 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.
3. The RFI shall implement and manage data security safeguards for its ICT and information resources, including but not limited to the following:
    a. Access control to the RFI's ICT resources and information shall be accompanied by an identification and authentication process. All identification and authentication factors must be clearly defined and documented with a comprehensive risk assessment conducted. Moreover, the RFI 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 RFI. This mechanism shall serve to identify the RFI to these entities.
    c. Secure audit logs shall document any event such as identification and authentication, access to and activities with resources, logging off, among others. 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 digital signatures.
    f. Information files shall be transferred to and from the RFI 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 RFI's technological capabilities. Any decision with regard to encrypting this data shall be submitted and approved by The Committee and Senior Management.
    h. Physical security shall be provided at all sites, including backup sites storing institutional information. In addition, the RFI shall physically secure all sites where information could possibly be accessed such as offices.
    i. Change management process shall be implemented to control changes to all systems, applications, products, including security testing and validation, prior to deployment into the production environment.
    j. 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 are followed.

4. The RFI 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.
5. The RFI's Senior Management shall ensure that its cyber and information security safeguards comply with all applicable laws and regulations.
6. RFI shall ensure that outsourced suppliers and service providers shall document and enforce the procedures in a manner that ensures the highest level of confidentiality and integrity of institutional information while maintaining the availability of this information and protecting the privacy of those providing this information.
7. To ensure a strong and effective defence, cyber and information security shall be coordinated with the RFI's IT and HR departments and aligned with its business and technological processes.

## 28. ARCHITECTURE

1. An RFI shall implement a secure physical and logical architecture with Zero Trust principles for preventing, detecting, rectifying and documenting breaches of its information technology system.
2. The RFI shall implement methods and mechanisms to prevent data breaches.
3. The RFI's communication networks shall be segregated from the outside world (physically or logically). The RFI shall maintain strict separation between its internal networks and all entities located outside its premises: the internet, suppliers, service providers and customers.
4. The RFI shall segment its network to ensure segregation and maintain strict separation between internal and external systems (zones). Controls such as demilitarised zone (DMZ), secure relays and firewalls must be implemented to reduce risks of unauthorised traffic flows.
5. The RFI shall deploy security systems to protect its infrastructure from hostile actors.
6. The RFI shall also implement monitoring and detection mechanisms to identify and respond to unauthorised attempts to access communication networks, servers, workstations and applications.
7. The RFI's internal communication network shall be segmented according to criteria related to organisational structure, functionality, information sensitivity, risk, etc.
8. Different work environments shall be created, as required, to segregate development, testing, and production. Development teams shall not be allowed to access the production environment at any time. Version deliveries or updates shall be carried out under proper change management procedures.
9. The RFI shall continually seek to enhance security policies for its network systems, workstation and safeguards.
10. A directory services shall be implemented to authenticate and authorise access to the RFI's network and systems.
11. The authentication to the network shall be based on multi-factor authentication (MFA).
12. The RFI shall prevent its personnel from using unauthorised portable media.
13. The RFI shall prevent malware from infecting its network, systems and servers. Protective software against malware shall be implemented.
14. The RFI shall use sanitisation software to prevent incoming and outgoing files from infecting the network.
15. The RFI shall protect sensitive files using encryption methods. Permission to inspect these shall be granted on a need-to-know basis and for audit purposes.
16. The RFI shall monitor its networks and systems for malicious or fraudulent activity and policy violations by internal and external intruders.
17. The RFI 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.

18. The RFI shall initiate a vulnerability assessment of its network elements at least on a quarterly basis (for the required testing frequency, refer to Annexure H – Testing Frequency).
19. It is recommended to implement cutting-edge technology based on anomaly detection algorithms for detecting zero-day attacks, malware and other malicious interventions.

## 29. NETWORK ELEMENTS

1. All unused ports (logical and physical) on network devices shall be disabled, either manually or through network access control mechanisms.
2. Communication components shall be hardened in line with the RFI's approved procedures, taking into account their risk exposure and operational requirements.
3. The RFI shall backup the configuration of the network elements and security safeguards to an encrypted backup.

## 30. 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 RFI 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 RFI'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 unauthorised network access.
8. The RFI shall use enhanced MFA (by implementing either smart cards, tokens with biometric matching abilities, one-time passwords, among others.). Administrators shall access the network using MFA.
9. A policy shall be formulated for enhancing the security of the RFI's network elements, systems and workstations.
10. The RFI shall audit all administrative activities. The activities shall be logged and fowarded to the RFI's SIEM system.

## 31. ENCRYPTION

1. Data in motion between various local networks shall be encrypted end-to- end.
2. All management traffic shall be encrypted, including sessions and passwords. The RFI shall encrypt its information in compliance with international standards and best practices.
    a. The encryption algorithms and the handling of the RFI'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.

3. RFIs shall use a key length for encryption and digital signatures to preserve confidentiality and integrity.
4. The RFI shall use a publicly vetted, industry standard digital signature algorithm in the year of implementation.
5. Encryption and authentication keys shall be exchanged according to established international protocols/standards.
6. Encryption keys shall be produced and stored in a manner that ensures their protection and prevents theft, loss, leaks or any risk to the RFI's production and/or storage processes. Production and storage of the RFI's encryption keys must meet international standards such as FIPS PUB 140-2 or the most up-to-date equivalent.

## 32. MEDIA ENCRYPTION

Media encryption is a key component of the RFI's information protection and cryptographic controls. It ensures that information stored on storage media, including removable media, and data transmitted across internal and external networks are protected against unauthorised access, interception, modification, or disclosure. The following controls may apply:

1. The use of removable media shall be formally authorised. An inventory of approved removable media shall be maintained, and usage shall be restricted to legitimate business purposes only.
2. The process of authentication to systems using storage or removable media shall employ the use of cryptographic protocols that guarantee data integrity and confidentiality.
3. All sensitive or confidential information stored on removable media shall be protected using strong, industry-approved encryption mechanisms to prevent unauthorised access in the event of loss or theft.

## 33. REMOTE ACCESS

1. Remote access to the RFI's network shall require a high level of identification and authentication (at least Two-Factor Authentication (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. The RFI shall grant remote access to the network and the core system only on a business need. The access shall be granted for a short period and limited time in accordance with the role of the individual requesting access.
3. A remote access segment shall be allocated a dedicated DMZ segment.
4. The remote access solution shall support encryption abilities to ensure secure connection.
5. Remote access to the RFI 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 RFI to know, after the fact, who has accessed what and when.

## 34. INTERNET ACCESS

1. The RFI's internet access networks shall be segregated from the internal networks.
2. The RFI 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 RFI shall have at least two independent internet connections from at least two distinct service providers.
    ii. RFI shall implement appropriate protective controls to ensure continuity of operations against availability disruptions, including denial of service attacks.
    iii. The RFI 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 RFI shall monitor, detect, and block breaches of potentially sensitive data, disclosed or transmitted to an unauthorised party via internet services e.g., browsing, email.
    ii. The RFI shall monitor, detect and protect against attempts to obtain sensitive information such as usernames or passwords by a malicious entity disguised in an electronic communication as being trustworthy.
    iii. The RFI shall screen the contents of incoming and outgoing internet communications via the web and email. The RFI shall formulate a policy to determine to what extent its communications shall or shall not be displayed to the user.

## 35. WEBSITES AND WEB APPLICATIONS PROTECTION

1. The RFI shall protect its business and non-business websites and web applications.
2. The RFI 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 RFI shall protect itself from database-directed hacking attempts by external or internal users. The protection shall be achieved by monitoring, controlling and blocking connectivity and access to sensitive information.
4. The RFI shall monitor and block a fraudulent website or web application user, based on behavioural patterns using technologies such as User and Entity Behavioural Analytics (UEBA) or by implementing challenges like Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

## 36. ACCESS CONTROL AND AUTHENTICATION

1. The RFI shall manage a system of permissions to access its resources and information, including certificate mechanisms for remote equipment or users (albeit on-prem or cloud). It is recommended to implement an Identity and Access Management (IAM) system.
2. The RFI 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 RFI's communication network shall be granted only after the user has been identified and authenticated.
4. MFA shall be implemented to authenticate users. A user password can only be used for legacy systems that cannot support MFA. RFIs shall discontinue the use of legacy systems two (2) calendar

years from the date of issue of this Directive.

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 and other equivalent identity management systems.
6. RFIs shall ensure that all service accounts are uniquely identifiable, strictly limited to necessary automated processes, regularly reviewed and monitored to prevent misuse.
7. RFIs shall implement Privileged Access Management (PAM) controls to enforce the principle of least privilege, require multi-factor authentication for all privileged accounts, and ensure continuous monitoring and audit logging of privileged activities.
8. RFIs shall review all accounts, accesses and permissions at least twice a year and/or when significant changes occur.

## 37. BIOMETRIC AUTHENTICATION

1. Whenever biometric authentication is required, maintain 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.

## 38. COMPARTMENTALISATION AND PERMISSIONS

1. The RFI's permission policy shall be based on the least privilege principle.
2. Systems and applications shall be accessible to only authorised users.
3. Compartmentalisation 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. User access to RFI systems shall be restricted to defined working hours based on job role and business requirements.
5. Permissions must be applied to folders and file systems on a need-to-know basis.
6. The compartmentalisation level required in the system shall be on a need- to-know basis. Unauthorised users shall not be able to erase any files and every file entering the system shall be saved.

## 39. SERVERS AND WORKSTATIONS

1. The RFI shall take steps to replace any system (hardware or software) that has been declared end-of-life by the Original Equipment Manufacturer (OEM)/Service Providers in its production environment within one (1) calendar year of the system being declared end-of-life by the OEM.
2. The Operating Systems (OS) shall be installed with security updates, including antivirus/antimalware and must be up to date. The RFI 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. Where the RFI is using legacy systems that do not support the requirements in paragraphs 39(1) and (2) above, the RFI shall prepare a plan to migrate to systems that comply with the requirements in paragraphs 39(1) and (2) as approved by BoG.
4. Endpoint security software shall be installed on all servers and workstations to manage access to removable media.

5. The systems shall operate in a stable manner, aligned with the most current security updates.
6. Each RFI's server shall be hardened to an adequate security level, according to the RFI's hardening policy. It is recommended to execute the hardening centrally.
7. Each of the RFI's workstations shall be hardened to an adequate security level, according to the RFI's hardening policy. The hardening process shall prevent users from acting as local administrators and block any possibility of running local software without authorisation. It is recommended to execute the hardening centrally through the security/control systems.

## 40. DATABASES

1. The databases that the RFI utilises must be the most suitable for its operation, taking into consideration information and cyber security requirements.
2. Databases shall be installed with the most current security updates.
3. The databases shall operate in a stable manner and in alignment with the most current security updates.
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 RFI's hardening policy.
6. Access to the database shall be allowed to three user groups only: application-level users, privileged users and the Database Administrators (DBAs).
7. The RFI 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 (DBF) (host or network based) and Database Activity Monitoring (DAM).
8. The RFI shall ensure all sensitive data stored within databases are protected using anonymisation, masking and salting techniques to mitigate the risk of unauthorised disclosure, identity linkage and credential exposure.

## 41. SOFTWARE INFORMATION SECURITY

1. Any software the RFI 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 RFI shall establish and apply 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 application security assessment. The developer/contractor shall rectify all security issues that are discovered following these tests.

## 42. APPLICATION PROGRAMMING INTERFACE (API)

API security aligns with the broader Information and Communications Technology (ICT) security principles, which include:

a. Safeguarding against intrusions and data misuse.
b. Ensuring accurate and prompt data transmission without major disruptions.
c. Implementing a robust ICT risk management framework that identifies, assesses, treats, monitors, reviews, and reports risks.

RFIs shall formulate API policies that at minimum covers the following areas:

1. Due Diligence and Security Assessment for Third-Party API Integration: Before allowing third parties to connect to an RFI's IT systems via APIs, a well-defined vetting process is required to assess their suitability. This process should consider factors such as the third party's nature of business, cybersecurity posture, industry reputation, and track record. A comprehensive risk assessment must be performed, ensuring that the security implementation for each API is commensurate with the data's sensitivity, business criticality, and confidentiality and integrity requirements.
2. Design and Development Standards: RFIs must establish security standards for designing and developing secure APIs. These standards shall at a minimum cover key control areas such as:
    a. Access control;
    b. Authentication;
    c. Authorisation;
    d. Data integrity and confidentiality;
    e. System activity logging;
    f. Security event tracking; and
    g. Exception handling.

    The security-by-design approach, where security is built into every phase of the SDLC, shall be incorporated to minimise system vulnerabilities and reduce the attack surface. Source code reviews (static and dynamic testing) and security testing for internet-exposed systems and applications are also required.
3. Authentication and Access Control
    a. **API Keys and Access Tokens:** Measures shall be in place to protect API keys or access tokens, which are used to authorise access and exchange confidential data. An appropriate timeframe shall be defined and enforced for access token expiry to reduce the risk of unauthorised access.
    b. **Strong Authentication:** Access rights should be managed on a need-to-know, need-to-use, and least privilege bases. For remote access, privileged access, or access to publicly accessible critical ICT assets, strong authentication methods based on leading practices are required. The use of Multi-Factor Authentication (MFA) is mandated for access to critical systems and sensitive information via the internet.
4. Encryption and Cryptographic Controls
    a. **Data in Transit:** Strong encryption standards and key management controls shall be adopted to secure the transmission of sensitive data through APIs. Information transferred over wide-

area networks (WAN) or the internet must be encrypted at the highest level.

b. **Cryptographic Key Management:** A policy covering the entire lifecycle of cryptographic keys (generation, distribution, installation, renewal, revocation, recovery, expiry, and secure destruction) shall be established and implemented. Keys shall be securely generated, protected from unauthorised disclosure and managed in accordance with any national encryption policy. Diversification of cryptographic keys (using separate keys for different purposes) is recommended to limit the impact of key exposure. RFI shall monitor developments in cryptanalysis and update cryptographic algorithms to remain resilient against evolving threats, including quantum advancements. Keys must be managed in line with the national encryption.

5. Testing and Monitoring
   a. **Security Testing:** Robust security screening and testing of APIs should be performed between the RFI and its third parties before deployment to production. Periodic vulnerability assessments and penetration testing shall be carried out to identify and remediate exploitable vulnerabilities and weaknesses in software applications, including those using APIs (for the required testing frequency, refer to Annexure H – Testing Frequency).
   b. **Continuous Monitoring:** Detective measures, such as technologies providing real-time monitoring and alerting, should be instituted to offer visibility into API usage and performance, and to detect suspicious activities. RFIs must ensure their ICT systems are monitored for anomalous activities and security events.
   c. **Logging:** Access sessions by third parties, including the identity of the party, date, time, request, response and data accessed, shall be logged. Logging procedures are critical for detecting anomalous activities, with clear definitions for events to be logged, retention periods, and measures to secure log data.
6. **Capacity and Resilience:** RFIs must ensure adequate system capacity is in place to handle high volumes of API call requests. Measures to mitigate cyber threats like DoS attacks are also required.
7. **Incident Response:** Robust measures must be established to promptly revoke API keys or access tokens in the event of a breach. RFIs shall have in place a written incident response management plan to promptly respond to, contain, and recover from disruptions caused by cyber incidents materially affecting their information systems. This plan should include communication, coordination, and response procedures to address cyber threats effectively.
8. **Risk Management Framework:** RFIs shall continuously review the adequacy and effectiveness of their risk management frameworks, considering the evolving cyber threat landscape.

## 43. AUDITING

1. The RFI shall define and implement a logging policy that specifies which system and security activities must be recorded.
2. The logging shall be tamper-proof, accessible and legible to any of the relevant systems.
3. The audit log shall include 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, audit start, audit stop, viewing system permission, delegation, among others;
   b. Monitoring all events on both the user and system administrator level, both at the application, database 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,

among others;

d. Input/output: monitoring data entered into system fields, incorrect attempts at entering data, logging the data entered in the database, among others; and
e. Running application-related services: store procedures, jobs, transactions, among others. The system shall audit success, failure, duration, among others.

4. Log file management
   a. access permissions to the log file: several permission levels must be defined for viewing, processing, copying, deleting, among others;
   b. the system log must enable ongoing maintenance defining the size of the log saved, updates, backups, among others; 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. An audit trail (log) will be maintained for a period consistent with its purposes in line with the Electronic Transactions Act, 2008 (Act 772) and relevant laws.

## 44. 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 Committee.
2. Subject to the provisions of paragraph 44(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 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 RFI, 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 ICT and/or other business unit(s). The lessons drawn from each exercise shall be reported to Senior Management through The 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 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 paragraphs 44(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 at all times. 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 equipping this team with the necessary tools and resources to perform their duties. This includes providing a centralised system for processing security data and events and

a dedicated facility or platform for continuous security monitoring and response.

10. The CISO is required to develop a prioritisation and estimation mechanism for cyber and information security incidents. This mechanism shall be informed by parameters such 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.

## 45. CYBER INTELLIGENCE AND RESEARCH

1. An RFI shall establish a dedicated Cyber Intelligence and Research Function under the supervision of the CISO. This function shall be responsible for the continuous collection, analysis, and dissemination of actionable cyber and information security intelligence to strengthen the institution's cyber defence posture.
2. The scope of the Cyber Intelligence and Research function shall at a minimum cover the following:
    a. Gathering and analysing intelligence on new and emerging cyber threats, incidents, and vulnerabilities;
    b. Monitoring both internet-facing and internal networks to identify, validate, or respond to potential attacks;
    c. Conducting continuous research and learning on evolving cyber defence methodologies, technologies, and mitigation strategies; and
    d. Recommending and implementing necessary changes to enhance the RFI's cyber resilience.
3. The RFI shall form a team of analysts to gather intelligence across the cyberspace on emerging threats, vulnerabilities, and potential attacks. Where external intelligence services are engaged, due diligence shall be conducted to ensure the provider's credibility, data protection practices, and compliance with applicable laws and regulations.
4. Intelligence services shall be provided on a regular basis (monthly or bimonthly) in the form of periodic reports, and on an ad-hoc or immediate basis for time-sensitive alerts. All intelligence inputs shall be consolidated and analysed within the RFI's SOC or its outsourced equivalent to enable timely and informed response actions.
5. Ongoing cyber and information security research shall form the foundation of the RFI's proactive defence and resilience strategy. Senior Management shall allocate sufficient budgetary resources to support continuous research activities.
6. The CISO shall submit quarterly Cyber Intelligence and Research Reports to The Committee, summarising key findings, observed trends, and recommended control measures.

# PART VIII - CYBER RESPONSE

This part outlines the process for defining and managing the RFI's cyber response function in accordance with ISO/IEC 27035.

## 46. STRUCTURE AND HIERARCHY

This paragraph defines the various functions and work processes of the cyber response unit and its interfaces with other units.

1. The CISO is responsible for creating and directly supervising the cyber response unit.
2. The team shall include employees with appropriate knowledge and education in cyber and information security, particularly in cyber defence and alert systems.
3. In terms of specific qualifications, the team members shall include but not be limited to the following:
    a. Researchers responsible for gathering information attack trends and developments and determining their relevance to the RFI's preparedness efforts.
    b. Analysts responsible for analysing relevant intelligence to determine whether the RFI 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 RFI to recover.
    e. Digital forensics experts to assist in the identification, preservation, analysis, and presentation of digital evidence following an attack. This may include engaging Bank of Ghana forensics services.
    f. The team shall include both permanent members and non-member experts called upon to assist in emergency efforts.
4. 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 RFI and what steps shall be taken to minimise harm to the RFI as the incident escalates;
    e. Cyber response;
    f. Coordinating with other institutional units treating the incident;
    g. Expanding the RFI's defence and recovery capabilities by commissioning experts for assistance, i.e., both from within the RFI 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, Cyber Security Authority (CSA), law enforcement authorities, and insurance bodies; and

k. On-going research.

5. The CISO shall supervise the entire course of incident treatment. He/She 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.

## 47. 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 RFI's ICT infrastructure.

1. An RFI shall implement and own a SIEM, outsource or subscribe to a SIEM-as-a-service. A SIEM subscribed to by an RFI, must be operated by a CSA accredited entity with Ghanaian majority shareholding.
2. An RFI that is a member of a group is allowed to rely on its group SIEM subject to the following conditions:
    a. The group SIEM shall be a verified multi - tenancy solution;
    b. The RFI shall have visibility of all reports; and
    c. The RFI shall have its own dedicated local team to monitor and analyse information security events at all times.
3. An RFI must connect its SIEM system to the BoG's SIEM system by sending security logs, aggregate information and reports.
4. 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.
5. The SIEM system shall be connected to all of the RFI'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.
6. All existing systems in the RFI shall be connected to the SIEM system within 12 months of its activation.
7. Additionally, every new system must be connected to the SIEM system as soon as it becomes operational.
8. The team responsible for the SIEM system shall be an integral part of the cyber incident team, as provided for in PART VII above.
9. The SIEM team shall be responsible for the following issues but not limited to:
    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 of cyber and information security incidents.

## 48. SECURITY OPERATIONS CENTRE (SOC)

1. The CISO is required to establish a SOC to act as the RFI's focal point or situation room for all matters related to alerting of cyber and information security incidents and their treatment to be operated by designated employees to serve as its cyber nerve centre.
2. The SOC shall be integral to the cyber and information security response team.
3. The SOC shall coordinate all institutional cyber and information security incidents and 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.
4. When the process is terminated, the SOC shall issue a summative report.
5. Appropriate human and technological resources must be allocated and budgeted for the SOC.
6. The CISO can implement some of the required functions for handling a security incident using outsourced services. Nevertheless, he must ensure that the RFI is able to audit all outsourced activities and that these meet this Directive.
7. The SOC's role include but are not limited to:
    a. Gathering and consolidating intelligence on the materialisation or probability of materialisation of cyber and information security events;
    b. Determining when alerts are false or real;
    c. Determining the level of severity of the 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 Senior Management, Board and other institutional units as required.

## 49. INCIDENT HANDLING

This paragraph describes the major responsibilities of the cyber intelligence and 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 RFIs, or Third Parties, etc. shall be contacted to obtain any information and assistance required in real time.
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 learnt 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 of the teams' involved and the current procedures and methodologies shall be conducted with a view to future improvement.
5. RFIs shall establish and maintain formal procedures for the timely identification, reporting, and management of information security incidents.

## 50. REPORTING TO BOG

1. Each RFI shall establish and maintain a post-incident plan that addresses both internal and external stakeholders. The plan shall include procedures for notifying regulators, customers, service providers, and, where applicable, law enforcement authorities, in line with legal and regulatory requirements.
2. For the purposes of supervision, the RFI shall submit any information or data that BoG may require. BoG may prescribe the following:
    a. The details of the information required;
    b. Form in which the information is to be reported; and
    c. Period within which the report is to be submitted to BoG
3. All RFIs shall report cyber and information security incidents to BoG on a monthly basis.
4. The report, which shall summarise all incidents in the past month, shall be submitted to BoG in the required format by the 15th of each month.
5. Without prejudice to paragraph 50(1) above, all RFIs shall submit a "NIL report" in cases where the RFI did not record any cyber security incident.
6. In addition to the monthly reports, RFIs shall submit ad-hoc reports to BoG, immediately. The reports shall inform the BoG about the incident as it starts, unfolds and terminates.
7. An RFI shall notify 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. 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, 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 occurred and had significant impact on data management and protection.
8. BoG shall set forth a reporting policy, including incident severity levels and associated reporting duties and processes.
9. BoG is entitled to instruct the RFI to report the security incident according to the circumstances.

## 51. MANAGED SECURITY SERVICE PROVIDERS (MSSP)

An RFI may choose to engage a Managed Security Service Provider (MSSP) to supplement or host its Security Operations Centre (SOC) functions, subject to a formal risk assessment and the approval of its Board. The RFI shall seek prior approval from The BoG to engage the services of an MSSP.

Additionally, the RFI must comply with the detailed requirements, controls, and oversight mechanisms set out in Annexure B – Managed Security Service Provider Guidelines of this Directive. The provisions of Annexure B are mandatory and form an integral part of any MSSP engagement.

1. **MSSP Selection:** The decision to engage an MSSP shall be based on the RFI's size, complexity, operational risk profile, and technological maturity, as defined by the Proportionality Framework in Annexure A of this Directive. RFIs classified under Tier 1 and 2 are expected to maintain a significant internal SOC capability and may only use MSSPs for specific advanced functions (e.g., threat hunting, 24/7 after-hours monitoring). Tiers 3, 4, and 5 may utilise MSSPs for a broader range of SOC services, provided they maintain internal oversight.

2. **Regulatory Compliance:** Any engagement of an MSSP shall be in full compliance with all applicable laws and regulations of the Republic of Ghana, including but not limited to:
    a. The Cybersecurity Act, 2020 (Act 1038), specifically the requirement for accreditation of cybersecurity service providers by the Cyber Security Authority (CSA);
    b. The Data Protection Act, 2012 (Act 843), regarding the processing and protection of personal data;
    c. The Bank of Ghana's Outsourcing Directives and any other relevant regulations.
3. **MSSP Accreditation:** The RFI shall only contract with an MSSP that is duly accredited by the Cyber Security Authority (CSA) as a Cybersecurity Service Provider, as required by the Cybersecurity Act, 2020 (Act 1038). Proof of this accreditation must be verified and maintained on file.
4. **Mandatory Due Diligence and Guidelines:** Prior to engagement and at least annually thereafter, the RFI shall conduct a comprehensive due diligence assessment of the MSSP. This assessment must align with the mandatory criteria outlined in Annexure B – Managed Security Service Provider Guidelines of this Directive, which covers, at a minimum:
    a. Legal and Regulatory Compliance (including CSA accreditation and Data Protection Commission registration).
    b. Technical Capability and Expertise (including 24/7 SOC operations and Digital Forensics and Incident Response (DFIR) capabilities).
    c. Security Posture and Certifications (e.g., independent audits like SOC 2 Type II).
    d. Business Continuity and Resilience (ISO 22301 alignment);
    e. Data sovereignty, ownership, and destruction protocols.
5. **Contractual and Service Level Agreements (SLAs):** The contract with the MSSP shall incorporate the supply chain security requirements detailed in paragraph 96 and Annexure D – Supply Chain Cyber Resilience Framework. At a minimum, the contract and SLAs must explicitly define:
    a. The scope of services, roles, and responsibilities using a RACI matrix;
    b. Service levels, including "Time to Detect," "Time to Respond," and escalation procedures;
    c. The MSSP's obligation to notify the RFI, and by extension the Bank of Ghana (through the FICSOC and existing channels), of any major security incidents impacting the RFI without undue delay;
    d. Unambiguous data ownership, data sovereignty (data must remain within jurisdictions approved by the Bank of Ghana), and secure data destruction clauses upon contract termination;
    e. The RFI's and Bank of Ghana's right to audit the MSSP's controls, processes, and facilities.
6. **Integration and Visibility:** The RFI shall retain full ownership of its security logs and data. The MSSP's systems must integrate with the RFI's internal systems (e.g., SIEM) to ensure the RFI maintains complete visibility and does not become entirely dependent on the MSSP for its security posture. The RFI's CISO remains ultimately accountable for the institution's cyber resilience.
7. **Residual Risk and Reporting:** The RFI shall document the residual risk associated with using the MSSP and include this in its enterprise risk register. Oversight of the MSSP's performance and compliance shall be a standing agenda item for the Cyber and Information Security Risk Management Committee and reported to the Board.
8. **MSSP Engagement:** The MSSP and the engagement itself must comply with all applicable laws and regulations of the Republic of Ghana, including but not limited to:
    a. The Cybersecurity Act, 2020 (Act 1038), including the requirement for the MSSP to be accredited by the Cyber Security Authority (CSA) where applicable;
    b. The Data Protection Act, 2012 (Act 843);
    c. Relevant provisions of the Bank of Ghana's directives and regulations; and
    d. Other relevant international standards such as ISO/IEC 27001:2022 and the NIST Cybersecurity Framework, as specified in the contract.

# PART IX - HUMAN RESOURCE SECURITY, ACCESS CONTROL AND CYBER COMPETENCY FRAMEWORK

## 52. ACCESS CONTROL

1. An entity seeking access to a RFI's ICT systems must be uniquely identified and authenticated.
2. In exceptional cases, where the requirements of paragraph 53(1) may be unfeasible, the Management of the RFI shall approve an alternate access.
3. An RFI 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 RFI's ICT systems shall be granted on a need-to-know basis and support the user's job assignments.
5. An RFI shall have an automated system in place to manage and control access permission. All access attempts (successful or unsuccessful) shall be logged and monitored and where applicable, relayed to the SIEM system.
6. Employees shall be informed that every activity in the RFI's systems is logged and monitored by an authorised person.
7. An RFI shall use a technology that integrates user identification and authentication, confidentiality, data integrity and non-repudiation safeguards.
8. Notwithstanding paragraph 52(7), an RFI may use alternative access control technologies in the following cases:
    a. Accessing high-risk systems shall be documented and approved by The Committee.
    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 52(7) proves impossible. For reasons that are external to the RFI.
9. The RFI shall define session time-out criteria based on risk and technological considerations after a specified period of inactivity.
10. The RFI 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.
11. When an employee is transferred within the RFI, 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.

## 53. HIRING AND ONBOARDING

1. An RFI shall create an induction process which all newly hired employees shall undergo. This process shall include, but not limited to the following:
    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. Authorised and unauthorised institutional activities;
f. A platform for discussing cyber and information security issues in general;
g. A platform for discussing the security of the RFI's ICT systems in general, and those for which the employee is directly responsible.

2. RFI shall conduct criminal background check, reference check and background verification on every candidate.
3. RFI shall conduct an integrity check on every candidate against the BoG engaged and disengaged database.
4. A newly engaged employee shall be:
   a. Given a unique user account 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 RFI's network and for using assigned workstation on the RFI's premises.
   b. Provided with additional identifiers which the assignment/enrolment process shall be carried out by a designated employee on the RFI's premises if necessary.
   c. Given access permissions to the RFI'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 54(4) (a), (b) and (c) shall be documented and logged.
   e. Trained to become aware of the issues stipulated in paragraph 53(1).
   f. Informed of the security of the RFI'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 RFI information from organisations where he has previously been employed.

## 54. NEW EMPLOYEE

1. The RFI shall:
   a. Determine the necessary competence of person(s) doing work under its control that affects its cyber and information security performance;
   b. Ensure that these persons are competent on the basis of appropriate education, training, or experience;
2. Each potential employee, for any position at an RFI, shall sign an undertaking stipulating:
   a. The duties with regard to protecting the confidentiality, integrity and availability of the RFI's information assets, including processes, customers, employees, suppliers and business partners;
   b. Awareness and agreement that all activities with the RFI'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 RFI's ICT systems shall be controlled and monitored;
   d. Authorised and unauthorised activities regarding all institutional operations;
   e. The principle of individual employee's accountability; and
   f. That after the employees termination, an authorised RFI representative shall be allowed to view the employee's mailbox and files stored on the institution's computers.
3. All the provisions of paragraph 54(1) shall apply to employees recruited through HR companies, to those employed by contractors providing services to the RFI or to individuals seeking temporary employment.
4. A hired employee shall receive basic training in privacy protection and cyber and information security.

This training shall also explain the obligations regarding the requirements and directive issues and the sanctions applicable to employees who violate them. The training shall be followed by a test.

5. The RFI is required to provide new employees with a document detailing any security training provided as paragraph 54(3) and all the warnings and potential disciplinary measures applicable to violators.

## 55. SENSITIVE POSITIONS

1. Senior Management shall periodically review and update the list of sensitive positions, determining whether to add or remove specific roles.
2. All employees for sensitive positions shall be subject to the fit and proper test directive issued by Bank of Ghana.
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.
4. An employee in sensitive position shall receive in-depth training about privacy protection and cyber and information security.
5. An employee in a sensitive position shall be required to go on vacation for at least two consecutive weeks.
6. The activities of employees in sensitive positions such as ICT employees shall be monitored continuously using automatic log scanning, such as the SIEM system, and manual methods to detect conduct that is contrary to the RFI's needs or interests.
7. Any anomalous activity and/or one that is contrary to the RFI's needs or interest and/or is considered inappropriate by the RFI and/or any other activity that is deemed suspicious shall be brought to the attention of the internal audit team.
8. Internet access for workstations assigned to employees in sensitive roles shall be restricted in line with their job assignments and monitored.

## 56. EMPLOYEE LIFECYCLE

1. Whenever an employee moves to a different position within the RFI, all authorisation associated with the old role shall be revoked and replaced by new ones consistent with the new position. The CISO shall consider whether to replace the assigned user account.
2. An RFI 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. The CISO shall review a report on employee authorisation and their compatibility with their job assignments at least once a year.
4. At a minimum, the CISO shall ensure that employees are aware of and understand the following:
    a. The essence of the RFI'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 56 (4).
6. An employee in position not considered sensitive shall go on an annual vacation of at least ten (10) consecutive days.

## 57. TERMINATION

1. CISO shall ensure that procedures for employee termination or exit include, but are not limited to the following:
   a. Blocking the user account in the employee's work environment, revoking his authorisations for all work environments, and denying his access to the RFI's physical facilities;
   b. Briefing the employee on his continued accountability for maintaining the confidentiality of the RFI'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 RFI shall backup the information on the employee's workstation to a specific server and then to remove/delete it from their workstation;
   e. Encrypted information with the employee's encryption keys, shall be decrypted;
   f. The CISO is responsible for ensuring that no information assets remain in employee's possession.
2. Provisions of paragraph 57(1) shall apply where the RFI initiates an employee's termination.
3. The 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.

## 58. 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 RFI's various ICT platforms.
2. All Processes for responding to any incident scenario must be set forth, including but not limited to the following:
   a. Receiving reports;
   b. Analyse reports or incidents;
   c. Reporting to various interfaces in the RFI;
   d. Determining the type of incident and the potential threat it poses to the RFI;
   e. Initial incident response;
   f. Escalation, including the commissioning of external experts if necessary;
   g. Reporting to external entities such as the BoG; and
   h. Developing a restoration process methodology.

## 59. 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 RFI, such as Senior Executives, ICT employee administrators, programmers and other non-ICT employees. An employee shall be tested following the training with evidence of training documented.
2. The 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 positions shall be required to undergo in-depth and dedicated cyber and information security education at least every two years as outlined in Annexure C - Enhanced Competency Framework, including external training and examination by internationally recognised certification authorities.

## 60. CYBER EXERCISE

1. An RFI 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's position. These exercises shall be included in the annual training program required of all employees with evidence of exercise documented.
2. Employees directly in charge of treating cyber and information security incidents shall undergo quarterly exercises with evidence of exercises documented. The entire RFI, 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 with evidence of exercises documented. 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 RFI's ICT systems; and
    e. Processes for reporting to the Senior Management, the Board and the BoG.
3. The exercise provided for in paragraph 59(3) shall also include business partners, suppliers and service providers.

## 61. ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) AWARENESS AND EDUCATION

1. To ensure effective governance and responsible adoption of AI and ML technologies, RFI's must establish ongoing AI and ML awareness and education programs across all organisational levels (e.g., the Board, senior management, data scientists, and operational staff).
2. The educational programs must emphasise aspects such as ethics, legal, and security implications of AI and ML use in financial services.
3. Training must cover understanding aspects such as the risks associated with AI and ML models (e.g., bias, explainability, and data integrity) as well as regulatory expectations for accountability, transparency, and data privacy protection.

4. RFI's should implement regular workshops, certification pathways, and scenario-based simulations to develop competence in identifying and mitigating AI and ML related risks.
5. The Board should demonstrate informed oversight by integrating AI and ML literacy into its governance processes, ensuring that decisions about AI and ML deployment align with the RFI's risk appetite, compliance obligations, and BoG supervisory principles for trustworthy and secure AI and ML.

# PART X - CHANNELS OF COMMUNICATION WITH EXTERNAL ENTITIES

## 62. DATA TRANSFER BETWEEN SITES AND ORGANISATIONS

1. Information transferred through the RFI'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. All information transfer shall receive appropriate authorisation.
4. Transferring information outside the RFI 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 in a separate zone within the institutional network.
7. The CISO shall set procedures for information transfer in routine and emergency circumstances.

## 63. EMAIL

This paragraph addresses the RFI's email systems, their use by employees, authorised and unauthorised activities.

1. The CISO is responsible for preparing procedures detailing authorised and unauthorised activities with regards to the RFI's email systems.
2. An employee allowed to use the email system shall sign a document, once a year, attesting to awareness of the authorised and unauthorised activities, including the fact that the email activities are continuously being monitored.
3. A DMZ may separate the mail servers from the institutional network and relay systems shall also be put in place.
4. 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. Intrusion Detections Systems/Intrusion Prevention Systems;
    d. Firewalls; and
    e. Antivirus and anti-malware software.

## 64. WEB ACCESS

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

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. 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.
2. Controls be deployed to mitigate risk associated with assets that are connected to the internet.
3. 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;
    d. Intrusion Prevention Systems;
    e. Firewalls;
    f. Antivirus and anti-malware software;
    g. Site blacklist filtering;
    h. An employee's user code and password on the internet shall differ from those used by the employee on the intranet; and
    i. Secured, dedicated log documenting all user activities.
4. An RFI shall implement automated means for controlling the system that connects to the internet and scans it for vulnerabilities.
5. The CISO shall conduct resiliency and penetration tests for the servers, security mechanisms and communication infrastructure facing the internet, including email infrastructure, at least annually. The findings of these tests and remediation plans, shall be discussed by The Committee. The CISO shall prepare employee procedures and directives specific to internet usage.
6. Every new system or major modification of a system shall undergo risk and information security assessments, 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.
7. Any expansion of an online service an RFI provides, shall require prior BoG approval. The request for approval of the service expansion shall comprise of a risk assessment of the service.

## 65. BRING YOUR OWN DEVICE (BYOD)

This paragraph addresses the conditions for approving employee use of private mobile devices such as smart phones and laptops with the RFI'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 RFI, the institutional inputs that is requested and the costs required to support it.
2. The CISO is responsible for determining the safeguards and usage policy regarding private mobile devices and areas of activity, such as email, calendar, contacts, documents, teleconferencing tools and any other relevant activity.
3. Approved private mobile devices shall be installed with the RFI's security controls. Without such controls, the device shall not be connected to institutional systems.

4. An institutional information stored or transferred to or from a private mobile device shall be encrypted.
5. 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 RFI or law enforcement authorities for examination.
6. Every device shall be password-protected, using built-in mechanisms for that purpose. A robust identification measure such as biometrics shall be employed to use institutional applications such as email. The password shall meet the RFI's password policy.
7. The device shall lock itself after an approved idle period. Unlocking the device shall require reauthentication.
8. The RFI shall manage all these devices using a dedicated infrastructural management tool.
9. User access to institutional information shall be restricted based on the employee's existing authorisation.
10. Institutional information may be remotely erased from the device depending on the occurrence of one of the following conditions:
    a. The device has been lost or stolen;
    b. The employee ceases to be under the employment of the RFI; or
    c. The RFI's ICT team has detected within the device a breach, penetration, malware or any other threat to the RFI and its infrastructure.
11. An employee interested in using a personal device shall sign a legal document consenting to the RFI's security requirements including, but not limited to the following:
    a. Institutional monitoring of the device;
    b. Installing the RFI's information security software on the device;
    c. Avoiding any use of the device that violates the RFI's procedures; and
    d. Awareness of duty of care to handle and use the device in an appropriately responsible and cautious manner.

## 66. INSTITUTIONAL MOBILE DEVICE

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

1. Senior Management shall make a strategic decision on allowing employees to use institutional mobile devices for work purposes. This decision shall be documented in writing and approved by the Board.
2. The decision shall be considered in view of the risks involved, employee convenience, benefits to the RFI, the institutional inputs required, and the costs involved.
3. The use of the approved institutional mobile device shall comply with the RFIs information security policy.

# PART XI - ELECTRONIC BANKING PLATFORMS

This Part addresses RFIs' use of electronic banking platforms, including identification and authentication, digital channel security, and customer protection requirements.

## 67. GENERAL CONTROLS

1. An RFI shall have an approved electronic banking policy and define different electronic banking platform levels and apply different levels of information security remedies with reference to these levels.
2. When a customer accesses an account remotely, details about the transactions from the previous access or logon shall be provided to the extent possible.
3. An RFI shall have in place a procedure for obtaining customer approval for account transactions taking into account type, nature and amount.
4. A customer shall be provided with the option to save and or print, in real time, the full details of any transaction or service request they initiate.
5. A third-party transaction shall be carried out subject to the following conditions:
    a. Transactions shall be carried out in line with a limit determined by the RFI and/or the customer.
    b. As part of a transfer order, the customer shall be required to indicate the receiver's details and the purpose of the payment.
    c. Prior to committing 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) or email. A customer may also authenticate transactions with biometric authentication.
    d. An RFI shall transfer data about the payer and, to the extent possible, about the purpose of payment and amount in a manner that shall enable the beneficiary to view this information clearly.
    e. The RFI shall set transaction limit according to the category of customer.
    f. The transaction limit for third-party electronic transfers of any kind shall be in line with all other existing transaction limit by BoG.
6. An RFI shall provide precautionary information to its customers accessing electronic banking platform(s) at least quarterly.
7. Every new service shall be approved in advance by the BoG. The RFI's request for approval shall include an assessment of cyber and information security aspects.

## 68. SUBSCRIBING TO ELECTRONIC BANKING PLATFORMS

1. An RFI shall sign an electronic banking platform (hereafter, EBP) agreement with its customers.
2. An RFI 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 67(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 RFI shall present to the customer the EBPs that each channel provides and the risks they involve. An RFI shall also inform the customer about cyber information security and recommended privacy protection principles for minimising these risks to the customer.

## 69. IDENTIFICATION AND AUTHENTICATION

1. An RFI 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 RFI 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, password 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 RFI may make certain services and transactions contingent on the use of additional factors such as a biometric authentication or one-time-password code delivered on a different channel.
5. A customer's authorisation to perform transactions and retrieve information through EBPs shall not exceed the authorisation that apply to the customer's bank account.
6. Notwithstanding the above, the RFI 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 EBPs independently, even when authorisations for traditional bank accounts are different, subject to a verified confirmation by the authorised individual/entity in the company and/or corporation.

## 70. WEBSITE

1. An RFI shall take measures to detect and mitigate attempts to spoof or clone its website and provide its customers with appropriate tools to verify the identity of its website.
2. Traffic between the customer and the website shall be encrypted using strong and industry-accepted encryption protocols in accordance with current best practices.
3. An RFI 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 may include preventing passwords from being saved to the browser or web pages to cache memory.
4. An RFI shall protect its customer-facing website using appropriate and industry accepted security controls, including, but not limited to, firewalls, anti-malware products, DoS/DDoS attack prevention, IPS/IDS and Web application security.
5. An RFI shall maintain at least four separate zones: internet-facing zone, DMZ, internal networks (intranets) and the server farm in its network infrastructure.
6. Customer information shall be stored in the innermost zone of the server farm.
7. Collection, processing and storage of customer data shall adhere to all local relevant laws and regulations.
8. Customer authentication method shall be based on multi-factor authentication.
9. RFIs 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 at all times.

10. An RFI shall conduct the following to assess the effectiveness of the existing safeguards:
    a. Penetration tests on website and internal servers shall be conducted in line with the testing frequency outlined in Annexure H; and
    b. Security assessment and resilience tests shall be conducted on websites and internal servers every six months and/or following any significant modification.

## 71. 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 industry accepted encryption levels and digital signature are not to be allowed.
3. The CISO shall maintain a compiled list of devices and operating system versions that the RFI supports.
4. A user shall provide his express agreement to using the RFI's application. A record of this agreement shall be stored. Notification of receiving the user's agreement to using the application shall be sent to the user utilising a channel such as SMS or email.
5. An application shall be tested and examined by the RFI with regards 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 RFI shall develop a mechanism to ensure the authenticity of the applications and the connection between them and the RFI. The applications shall be authenticated over the device whenever the user starts using them.
7. An RFI shall provide a dedicated secure API gateway for communicating with mobile applications.
8. An RFI 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 biometrics, 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 RFI shall examine at least once every 24 hours whether the third-party applications used indeed match those it has released to the application distribution platform when a third party is used to distribute the application.

## 72. EMAIL

1. The use of email shall follow the acceptable use policy of the RFI.
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 RFI 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 tracking mechanisms allowing the RFI to determine with absolute certainty whether the customer has received and opened the email, downloaded it to a personal computer and/or printed it; and
    d. Information on customer activities as noted in paragraph 72(3)(c) is securely saved in the RFI.

## 73. TELEPHONY SERVICES

1. Call centre
    a. Senior Management shall determine the types of uses and activities allowed to customers through the RFI'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 be consulted on 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, among others).
    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. The RFI shall ensure that customers are notified that the calls are being recorded.
        iv. This information shall be saved on the call centre's servers for not more than 12 hours.
        v. 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.
        vi. An RFI shall use computerised mechanisms to process recorded information, including its correlation with the information presented to the operator.
        vii. Only authorised individuals shall be allowed access to these recordings.
    e. An RFI shall implement security controls for call centre environments where computers are used to access customer or institutional data:
        i. Internet access on call centre computers shall be restricted to only the resources required for official duties.
        ii. Call centre systems shall be configured to prevent the download, storage, or transfer of customer data to unauthorised locations.
        iii. Access to customer information shall be limited to authorised staff based on the principle of least privilege, and all activities on call centre computers shall be logged and subject to continuous monitoring.
    f. The CISO shall implement, with the required modifications, a cyber and information security policy and conduct security, risk, resilience and penetration tests for the call centre environment, including the telephony equipment at least once a year (for the required testing

frequency, refer to Annexure H – Testing Frequency).

g. Transactions allowed by the RFI 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. Short Messaging Service (SMS)
   Any information transferred using SMS shall not include complete identification details about the customer and the account, such as name, account number and other relevant information.

## 74. CUSTOMER SECURITY

1. An RFI shall implement an automated system 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 RFI shall incorporate fraud rules and scenarios in its automated system 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 RFI shall alert customers immediately of any unusual activities it has identified with regards to 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 transaction limit determined by the RFI. The RFI shall take immediate steps such as obtaining the customer's approval or revoking a transaction regarding 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 74(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 RFI shall make clear to customers the major risks involved in EBPs and recommend reasonable precautionary measures that shall be observed.
7. This information shall be provided over a variety of channels, including the RFI's website, notifications upon accessing an EBP, email, brochures, newsletters and other relevant information.
8. An RFI 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 RFI suspects EBP fraud, 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.
10. The RFI shall conduct regular cyber and information security awareness for customers to ensure they are well-informed about potential security risks and threats. Customers shall be educated on their rights and responsibilities in safeguarding sensitive information and protecting the institution's digital assets.

## 75. PASSWORDS AND PASSWORD MANAGEMENT

1. Minimal password length shall be twelve (12) characters or in line with current information security standards. The more stringent requirement of the two shall apply.
2. All passwords shall meet RFI's defined complexity requirements.
3. When managing passwords for customer identification and authentication, an RFI shall refer to the risk and service level agreement of the system in question.
4. An RFI 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 RFI shall initiate customer password change:
7. Immediately after the first login using the initial password; and
8. At least every ninety (90) days or when a suspicious activity occurs.
9. The RFI shall revoke a customer's access to the EBP account 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 RFI suspects unauthorised use of the password;
    c. After several failed login attempts, as determined by the RFI but involving no more than five consecutive attempts; and
    d. After a period of six months of not accessing the specific system to which the password has been assigned.
10. An RFI may unblock a password so long as the customer has been duly identified using KYC and account related information.
11. The stipulations of paragraph 74(8) shall not apply to EBPs using biometric identifications or devices that generate OTPs.

# PART XII - EXTERNAL CONNECTIONS

This part addresses direct computerised communication for the purpose of conveying messages, such as trading orders between two different RFIs, an RFI and a stock market, an RFI and a financial institution and/or other organisations.

## 76. DIRECT CONNECTIVITY

1. Connection between two institutions shall be considered with respect to the risk estimate involving the contact between them.
2. Information security risk assessment 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. 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 incident shall be provided as required;
    f. Business information transferred between end-points shall be saved to an application-level log; and
    g. Event during 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 where the test environment of the RFIs need to be connected:
    a. Cyber and information security safeguards as detailed in paragraph 75 (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 anonymised 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; and

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

5. An RFI that seeks to connect to another institution shall first obtain BoG approval.

## 77. OTHER FINANCIAL AND NON-RFIs

This paragraph addresses connectivity between RFIs and other stakeholders.

1. The parties shall meet all requirements in this Directive prior to seeking approval for a connection.
2. The parties shall meet the Directives included in paragraph 77.
3. Information security risk assessments of the connectivity between the parties shall be conducted in the operational environment at least every six months. Equivalent assessments shall be conducted in the test environment.
4. The responsibility for conducting these assessments lies with each party.
5. The assessment findings of each party shall be presented to The Committee or highest level of management of each party. Any vulnerability identified shall be addressed or remediated immediately.
6. Assessment findings shall be sent to BoG, together with a schedule for remediation.

## 78. BUSINESS PARTNERS

This paragraph addresses connectivity between two business partners and related to an RFI.

1. Any connectivity between an RFI and its business partner shall be established in accordance with the RFI's approved third-party risk management framework and in compliance with this Directive.
2. The RFI shall conduct due diligence to ensure that its business partners implement effective risk management controls, including ICT, cyber, and information security measures consistent with the Directive's requirements.
3. The RFI shall ensure that its business partners meet at least the minimum cyber and information security requirements defined in this Directive.
4. The RFI shall perform periodic risk and information security assessments on the business partner and the connectivity environment between the two parties. These assessments may include risk and security assessments, penetration testing, and resilience assessments (for the required testing frequency, refer to Annexure H – Testing Frequency)., conducted at least annually or as determined by the RFI's risk management policy.
5. All identified gaps or weaknesses shall be documented and remediated within agreed timelines. Unremediated issues shall be escalated to the RFI's Senior Management for decision on whether to maintain, suspend, or terminate the connection.
6. A summary report of the assessments and remediation status shall be made available to Bank of Ghana upon request or as part of periodic regulatory reporting.

## 79. REMOTE ACCESS

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

1. Approving remote access to RFI 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 defined cases.
2. Clear criteria and procedures shall be laid down when Senior Management decide to enable remote access.

3. All remote access not covered by paragraph 78(2) shall be implemented using technology that meets the requirements of paragraphs 33 and 61 and is compatible with the following:
    a. The technology shall serve as the exclusive gateway to the RFI's ICT resources. Any ICT component capable of providing remote access shall be inspected; if such functionality exists, it must be disabled and the component must instead be connected to a dedicated RFI mechanism to ensure all remote access is controlled and supervised;
    b. Uses an authentication mechanism and one-time password 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, logging all traffic in a dedicated log and ensuring encryption;
    e. Any access shall require manual activation and intervention by the employee in charge; and
    f. The system shall support logging, including computerised management of the administrative process accompanying the communication.
4. The CISO shall determine requirements for remote access that consider 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, the session shall be logged or recorded and monitored.
    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.

## 80. EXTERNAL PARTIES

1. As a rule, any external communication performed over a Wide Area Network (WAN) shall meet the provisions of paragraphs 63 and 80.
2. Notwithstanding paragraph 79(1), an RFI shall place particular emphasis on the following:
    a. Encryption implemented shall be end-to-end;
    b. Intrusion detection and prevention systems (IDS/IPS), firewall, and traffic monitoring shall be implemented; and
    c. Any other measures as decided by the RFI.

## 81. DATA IN MOTION

1. The RFI 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 RFI 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 XIII - CLOUD SERVICES

## 82. CORPORATE GOVERNANCE

1. An RFI considering the use of cloud computing shall bring this 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. Senior Management shall formulate a policy 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 RFI 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;
    i. Data sovereignty; and
    j. Terms and conditions of contract termination.
3. The Board shall either reject or approve the RFI's use of cloud computing based on paragraph 81(2).
4. Senior Management and Board shall discuss the agreement prior to finalising its contract with a cloud service provider.
5. An RFI shall seek approval from BoG to transit to cloud services.
6. Senior Management shall ensure that any use of cloud computing complies with the policy provided for in paragraph 81(2), and that this use is subject to the terms of its general approval of the transition to the cloud.
7. The RFI shall ensure that its designated cloud technical and security personnel undergo continuous training and capacity-building programs to maintain the requisite skills, knowledge, and competencies for effective management and protection of cloud resources.

## 83. RISK MANAGEMENT

1. An RFI 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 with evidence documented.
2. During the contract period or at least every two years, the RFI shall conduct an additional due diligence with evidence documented.
3. An RFI 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 RFI and/or provider. The assessment shall focus on risks unique to cloud computing with evidence documented.

4. Senior Management shall discuss and approve transitioning to the cloud, any activity area or application not included in the original contract.
5. An RFI shall ensure that all controls are in place, including appropriate compensatory controls for the risks that have been mapped.
6. The RFI shall monitor cyber and information security incidents related to its use of cloud services. The RFI shall ensure it meets accepted standards and its own regulations when capabilities are provided by the provider. Moreover, it shall integrate these capabilities with existing monitoring systems within the RFI.
7. Data in motion between an RFI and the provider must be encrypted.
8. Data at rest stored at cloud service provider shall be encrypted. The data classified by an RFI as sensitive and whose exposure is liable to compromise the RFI and/or its customers shall be encrypted.
9. The encryption keys shall be stored with the RFI rather than the provider.

## 84. 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 RFI to conduct independent cyber and information security audit, including resilience and penetration tests and/or any other tests that substantiate and confirm the provider's compliance with this Directive;
    c. Enabling the RFI, under special circumstances, to require that the provider conduct an ad-hoc security audit of a specific issue;
    d. Allowing the RFI to unilaterally suspend use of the provider's services or switch to a different provider. The RFI 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 to an irreversible deletion of all data (including residual and backup copies) from its systems, confirmed through certification or attestation;
2. The contract shall also provide for implementation of all cyber and information security mechanisms and controls that the RFI requires to protect its data, including customers' data and ICT resources.
3. An RFI 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.

## 85. INSTITUTIONAL APPLICATION DEVELOPMENT

1. An RFI shall ensure its service provider maintains separate environments for development, testing, and operations.
2. The RFI shall ensure that secure development practices are implemented in line with this Directive and internationally accepted standards for secure software development.
3. The RFI shall ensure that cyber and information security testing can be performed on all environments, either by the RFI or by an authorised third party on its behalf.
4. The RFI shall ensure that relevant system and security logs from all environments are retained and relayed to the institutional SIEM for control, monitoring, and analysis.

## 86. PROMOTIONAL MATERIAL

1. The cloud service provider shall protect the integrity, reliability and availability of all the RFI'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.

## 87. CLOUD OPERATIONS, MONITORING AND RESILIENCE

1. The RFI shall deploy centralised logging, monitoring, and SIEM capabilities specifically tuned for cloud environments (e.g., aggregating logs from CSP, storage buckets, API gateways).
2. The RFI shall maintain metrics and dashboards for resource utilisation, anomalies, unauthorised changes, and capacity thresholds.
3. The RFI shall ensure that backup and snapshot capabilities provided by the CSP, or external tools are properly configured, tested, and aligned with the RFI's recovery requirements objectives.
4. The RFI shall coordinate periodic failover testing (e.g., across availability zones or regions) to validate resilience in the cloud (for the required testing frequency, refer to Annexure H – Testing Frequency).
5. The RFI shall ensure that functions or containers are limited in execution time, resource consumption, and have proper throttling, isolation, and controls observability where serverless or microservice architectures are used.
6. The RFI shall maintain a documented cloud incident response plan that is integrated with the RFI's overall incident management procedures, including roles, escalation protocols, forensic access, and coordination with the CSP.

## 88. CLOUD SECURITY CONTROLS AND ASSURANCE

1. The RFI shall implement defence-in-depth controls across Identity and Access Management (IAM), network segmentation (virtual networks, subnets), micro-segmentation, encryption, least privilege, and zero trust principles in the cloud context.
2. The RFI must ensure that CSP's native security controls (such as identity management, key management, firewall as a service, and virtual private cloud controls) are appropriately configured and supplemented with additional controls when necessary.
3. Sensitive workloads should be isolated to dedicated virtual private networks or "private endpoint" constructs instead of default public access paths.
4. The RFI shall implement strict, fine-grained IAM roles for its staff and services accessing cloud resources. Credentials (e.g., access keys, secrets) must be rotated regularly and stored in hardware-backed secret vaults.
5. All data in transit, including within the cloud backbone, must be encrypted using strong protocols such as Transport Layer Security (TLS) v1.3 or higher.
6. All data at rest must be encrypted. A CSP or third-party provider can supply a Key Management Service (KMS), but it must ensure that the RFI maintains control over key policies, rotation, and revocation.
7. The RFI shall ensure thorough logging and audit trails for privileged actions, configuration changes, and resource lifecycle events.

8. The RFI shall periodically review and correct misconfigurations (e.g., overly permissive buckets, firewall rules, open ports).
9. Where containerisation or serverless functions are used, the RFI shall implement runtime monitoring, integrity checks, vulnerability scanning, and restrict the use of privileged containers.
10. The RFI shall mandate vulnerability scanning of cloud components and generate a remediation plan subject to the Board's approval oversight.

# PART XIV - RFIs WITH INTERNATIONAL AFFILIATION

## 89. FOREIGN RFIs IN GHANA

1. This Directive shall apply to foreign RFIs as is, except for the following revisions:
    a. Whenever a directive refers to the RFI'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 RFI's ICT systems overseas; and
        ii. Other local institutional systems in Ghana, including their interfaces with the RFI's systems abroad.
    b. Whenever the Board's obligations are defined, they shall apply to the local management, that is, the foreign RFI's management in Ghana.
    c. Whenever a reporting duty to BoG is referred to, the duty to report to the foreign parent RFI Senior Management abroad shall be added.
2. A foreign RFI shall report to 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 RFI, including any changes therein.
3. Where a foreign parent RFI's regulation is less stringent than the comparative regulatory requirements in Ghana, the foreign branch in Ghana shall comply with this Directive.
4. Where the foreign parent RFI's regulation is more stringent, the RFI may apply those higher standards, provided it can demonstrate to BoG that such measures offer equal or greater protection.
5. In cases where differences exist between the parent regulation and this Directive, this Directive applies.

## 90. GHANAIAN RFIs OPERATING ABROAD

1. A Ghanaian RFI operating abroad shall comply with this Directive, including reporting to BoG and supervision by BoG.
2. A Ghanaian RFI operating abroad shall comply with the privacy protection and cyber and information security laws applicable both abroad and in Ghana.

# PART XV - PHYSICAL SECURITY

## 91. GENERAL

1. All the RFI's physical sites and facilities shall be mapped and classified to determine the access permission levels required of employees. Mapping shall include both manned and unmanned sites, facilities with IT equipment such as servers, information platforms, sites where RFI employees are employed such as offices, and sites or sites storing equipment such as generators and air-conditioners.
2. An RFI 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 at all times 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 RFI shall use technologies to ensure that all visual and auditory surveillance records are saved and analysed.
5. An RFI shall issue every employee with an identification and access device defining the authorised accessible physical environments.
6. The RFI shall ensure that access to sites with ICT equipment such as servers and information platforms, including sites where RFI employees work is controlled using trained guards and various technologies.
7. An RFI shall implement a system to correlate employees' attendance records with their identification and authentication to its ICT systems, including remote access through the RFI's secure environment.
8. The RFI shall conduct routine maintenance and periodic testing, at least once in a year, of all security systems to ensure their effectiveness, reliability, and optimal performance with evidence documented (for the required testing frequency, refer to Annexure H – Testing Frequency).

## 92. SECURED ZONES

1. Work areas shall be segmented into secured zones according to the sensitivity of the information contained, stored or accessed within them and the potential impact on the RFI in the event of a compromise.
2. Servers and communication equipment including storage devices 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 at all times.
5. All entries and exits to and from a secured zone shall be controlled using an MFA mechanism, depending on the zone's sensitivity level.
6. When an employee is transferred, the assigned access permissions shall be modified in line with the current role. All permissions granted an employee shall be revoked immediately upon termination or resignation.

## 93. SEGMENTATION

1. Each segment of a secured zone shall be physically protected in a manner that prevents entry into the secured zone and access to a segment not under the subzones or segments.
2. Secured zones that serve the entire RFI such as communication cable ducts shall be constructed so as to enable surveillance at all times.
3. Notwithstanding paragraph 92(1) when it proves impossible to divide a site/facility into separate secured zones and implement physical protection as provided under PART XV -PHYSICAL SECURITY, the RFI 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 RFI 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.

## 94. PHYSICAL SECURITY OF HARDWARE AND OTHER EQUIPMENT

1. ICT equipment requiring protection includes any unit that processes and retains 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, integrity or availability of the information stored over the equipment in question; or
    b. the business impact of a physical loss or unavailability of the equipment.
3. An RFI shall implement a “one-way-in/no-way-out” policy for any physical IT equipment placed on its premises.
4. Notwithstanding paragraph 93(3), an RFI 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 RFI’s premises, the provisions of paragraph 93(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 a destruction certificate shall be generated and filed.

# PART XVI - CONTRACTUAL ASPECTS

## 95. CYBER SECURITY CONTRACTS

This part addresses the cyber and information security requirements in contracts between an RFI, its employees, and Third Parties.

1. An RFI shall be allowed to contract with Third Parties only in line with the following conditions:
    a. Third Parties that meet international cyber and information security standards such as ISO/IEC 27000 family of standards.
    b. Third Parties shall comply with this Directive with regard to their mutual activity with the RFI (see also PART XIII).
    c. An RFI shall conduct a risk assessment of a Third Party at least annually.
    d. An RFI and a Third Party shall include in their contract 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 Third Parties. The RFI and the Third Party 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. Remediating and improving cyber and information security issues shall be prioritised and handled without any delay.
    e. The right to unilaterally suspend or terminate the contract; or take any other actions as it deems fit when Senior Management finds the Third Party is not compliant to a satisfactory degree thus creating a risk for the RFI.
2. In its contracts with software vendors, an RFI is required but not limited to include the following:
    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 RFI 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 RFI 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 RFI shall test the software. Other companies specialising in software tests and in cyber and information security tests may assist the RFI.
    d. The software maintenance provider shall meet the cyber and information security requirements stipulated in paragraphs 94(2)(a)-(c).
    e. An RFI shall include in the contract with the provider a systematic process of rapid and efficient treatment of any software vulnerability detected.
    f. The RFI and the provider shall agree on a process in order to resolve escalating incidents as quickly, efficiently, and effectively as possible.
    g. In its contracts with software vendors providing off-the-shelf programs, the RFI is required to include such aspects that include but are not limited to:
        i. The vendors' commitment to cyber and information security issues in their software;
        ii. Their assurance that their software has passed cyber and information security tests; and

iii. The option to suspend any purchase should the RFI find that a certain software product does not meet its cyber and information security requirements.

3. Whenever the RFI develops and/or purchases hardware/software, the contract shall include proprietary, intellectual property, and copyright clauses.
4. In every contract with Third Parties whose employees are required to enter the RFI's premises, the Third Party shall take full responsibility for their employees. The contract shall include the following, but not be limited to:
    a. The Third Party as well as its employees shall sign a confidentiality agreement or a Non-Disclosure Agreement (NDA) with the RFI.
    b. The RFI shall be entitled to examine the background of any Third Party's employee about to be assigned to its premises, as stipulated in Paragraph 55.
    c. An RFI is entitled to reject any candidate who fails to meet the requirements and tests provided for in paragraph 95(4)(b).
5. In every contract with Third Parties hired to provide remote support, the Third Party shall be required to accept full responsibility for its employees.

## 96. SUPPLY CHAIN CYBER AND INFORMATION SECURITY CONTRACTS OBLIGATIONS

Every contract or service level agreement (SLA) with a Third Party shall include comprehensive cyber and information security obligations. These obligations shall, at a minimum, address the following (See also paragraph 16(6)):

1. **Adherence to Security Standards and Directives:** A mandatory requirement for the Third Party to comply with the RFI's information security policies, relevant international standards (e.g. ISO/IEC 27001, NIST Cyber and information security Framework), and all applicable Bank of Ghana directives and regulations.
2. **Audit and Assessment Rights:** An unequivocal right for the RFI, to conduct, or appoint a representative to conduct, security assessments, audits, and reviews of the Third Party's information systems, security controls, and relevant facilities. Including the option for the RFI to commission and rely on independent third-party audit. All such assessments shall be subject to appropriate confidentiality protections to safeguard the Third Party's proprietary information.
3. **Cyber Incident Notification and Management:** There shall be a binding obligation for the Third Party to notify the RFI of any cyber and information security incident that could potentially impact the RFI's data, services, or operations within a timeframe, not exceeding an hour from the moment the incident is confirmed or reasonably suspected by the Third Party.
4. **Cooperation in Incident Response and Forensics:** A requirement for the Third Party to provide full access to relevant systems, logs, and personnel, and to offer all necessary technical support during incident response, containment, eradication, and subsequent forensic investigations.
5. **Business Continuity and Disaster Recovery:** Mandated requirements for the Third Party to maintain and regularly test robust backup, business continuity, and disaster recovery plans. These plans must be commensurate with the criticality of the service provided and ensure the timely resumption of operations in line with agreed-upon recovery objectives.
6. **Remediation and Termination for Security Failures:** There shall be express termination rights and the ability to invoke exit migration arrangements if the Third Party fails to meet the agreed security requirements, suffers a material security breach, or is unable to restore services within agreed-upon timelines. This includes the right to demand a secure and orderly transition of services.
7. **Subcontractor (Tier-n) Oversight and Flow-Down Clauses:** A strict obligation for the primary

Third Party to ensure that all subcontractors, at any tier, who are involved in the delivery of services to the RFI, are bound by equivalent or stricter cyber and information security and information security requirements. The primary Third Party must retain full responsibility for the acts and omissions of its subcontractors and provide the RFI with audit or oversight rights over critical sub-suppliers.

## 97. CONTRACTS INVOLVING AI, ML OR ALGORITHMIC SERVICES

1. **Scope**
   All contracts between RFI's and Third Parties involving the use, deployment, or management of AI, ML, or algorithmic decision-making systems shall include explicit provisions addressing transparency, accountability, and oversight in line with applicable standards such as ISO/IEC 42001.
2. **Mandatory Contractual Clauses**
   Contracts shall, at a minimum, contain provisions that ensure:
   a. **Model Transparency:** Clear disclosure of model purpose, data sources, training methods, performance metrics, and explainability level to allow supervisory and institutional understanding of algorithmic behaviour.
   b. **Audit Access:** Full audit rights for BoG and the RFI's to review model design, training data lineage, algorithmic logic, performance logs, and control mechanisms, ensuring compliance with regulatory and ethical standards.
   c. **Performance Guarantees:** Explicit SLAs and performance indicators addressing model accuracy, fairness, robustness, and operational reliability, including fallback and fail-safe procedures.
   d. **Liability and Accountability:** Defined liability provisions for errors, bias, misuse, or harm resulting from AI/ML system behaviour, including obligations for rectification and compensation mechanisms where applicable.
   e. **Retraining and Version Control:** Mandatory inclusion of clauses governing periodic model retraining, version management, documentation of updates, and notification obligations prior to significant algorithmic or data-related changes.
   f. **Dispute Resolution for Algorithmic Decisions:** Provisions for transparent, traceable, and fair dispute resolution mechanisms related to decisions made or influenced by AI/ML systems, ensuring human oversight and appeal rights for affected parties.
3. **AI/ML Awareness and Education**
   RFIs shall ensure that staff responsible for managing, overseeing or engaging with AI/ML service providers receive periodic education and awareness training on AI risk management, ethical implications and regulatory compliance obligations. Such training must be integrated into the institution's overall cyber and information security and operational risk training framework.
4. **Supervisory Rights**
   BoG reserves the right to review, approve, or require modification of any AI/ML-related contractual terms deemed inconsistent with national cyber and information security, data protection, or financial stability objectives.

# PART XVII - DIGITAL INNOVATIONS

Bank of Ghana recognises the transformative potential of digital innovations to enhance the efficiency and accessibility of financial services. This part of the directive is to provide a clear and comprehensive cyber security regulatory framework for RFIs seeking to engage in the use of digital innovations, ensuring financial stability and protecting the Ghanaian public interest in line with all relevant laws.

## 98. GENERAL

1. An RFI considering the adoption of digital innovations such as Blockchain, AI, Virtual Assets, Quantum Computing, and Robotics shall present the adoption to the Board prior to implementing the 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. Senior Management shall ensure cyber security policies governing the use of digital innovations which addresses but not limited to the following:
    a. **Information Security:** Protection of electronic systems and client data using encryption, secure protocols, and industry best practices.
    b. **Data Governance and Classification:** Categorisation of data based on sensitivity and application of appropriate controls.
    c. **Access Controls:** Role-based access, multi-factor authentication, and session management.
    d. System Operations and Availability: Ensuring uptime, performance planning, and disaster recovery.
    e. **Network and System Security:** Use of firewalls, IDS/IPS, and secure consensus protocols.
    f. Smart Contract and Code Validation: Regular audits and validation of blockchain code and smart contracts.
    g. **Authentication and Session Controls:** Password policies, timeouts, and verification for sensitive changes.
    h. **Transaction Security:** Monitoring and verification of virtual asset transactions, especially high-value or sensitive ones.
    i. **Client Data Privacy:** Secure data transfer, prevention of unauthorised access, and leakage.
    j. **Vendor and Third-Party Management:** Vetting and monitoring of service providers with cyber and information security clauses.
    k. **Physical and Environmental Security:** Protection of infrastructure and cold wallets from physical threats.
    l. **Incident Response and Reporting:** Defined procedures for breach detection, reporting, and recovery.
    m. **Cryptographic Key Management:** Use secure key generation algorithms and effective key handling procedures.
    n. **Policy Review and Updates:** Annual review by the CISO and updates based on evolving threats.

o. **Bias and Discrimination:** Risks of unfair outcomes due to biased training data or model design.
p. **Lack of Explainability:** Difficulty in understanding or justifying AI-driven decisions, which can undermine trust and accountability.

3. The Board shall either reject or approve the RFI's use of digital innovations based on paragraph 97(2).
4. An RFI shall seek prior written approval from BoG and all relevant regulators before implementation of a digital innovation.

## 99. DATA PRIVACY AND CONFIDENTIALITY REQUIREMENTS

1. RFIs adopting or operating digital innovations must ensure that all processing of customer, employee, or institutional data complies with the principles of lawfulness, fairness, transparency, non-repudiation, accuracy, storage limitation, integrity, availability, and confidentiality, in accordance with the Data Protection Act, 2012 (Act 843), and relevant international data protection standards.
2. RFIs shall conduct a Data Privacy Impact Assessment (DPIA) for all technology projects, especially those involving personal or sensitive information.
3. RFIs shall integrate privacy-by-design and privacy-by-default principles throughout system development, ensuring that privacy controls are built into technical and operational processes.
4. Each RFI shall maintain data retention and deletion schedules, ensuring personal data is stored as long as necessary and is securely disposed of.
5. RFIs shall ensure that all third-party service providers and technology partners implement data protection standards that are equal to or more stringent.
6. Each RFI shall appoint a Data Protection Officer (DPO) or designate a privacy lead to manage compliance, advise on DPIAs, and collaborate with the CISO and Board Risk Committee.
7. Privacy breaches shall be integrated into the incident response and breach notification framework, requiring prompt reporting to affected customers, the Data Protection Commission, and Bank of Ghana.

## 100. AI/ML GOVERNANCE AND SECURITY

1. RFIs that adopt, deploy, or operate artificial intelligence or machine learning models (collectively "AI/ML Models") in any core business process such as risk decision-making, customer interaction, fraud detection, credit scoring, predictive analytics, or system operations, must implement governance, security, and risk management controls in accordance with this Directive and the principles outlined in Annex E (AI/ML Governance & Control Guidelines).
2. The RFIs must ensure that AI/ML models are designed, developed, tested, validated, monitored, and maintained in a way that protects the confidentiality, integrity, and availability of systems and data, reduces bias, and guarantees explainability and auditability.
3. The RFIs must establish an AI/ML Oversight Committee (or designate it within the existing Cyber & Information Security Risk Committee) whose mandate includes the review of (see also Annexure E):
    a. Model risk assessments, including adversarial and robustness testing;
    b. Ethical and fairness assessments;
    c. Model change control, retraining schedules, versioning, and rollback procedures;
    d. Monitoring of model performance, drift, degradation, and anomaly detection; and
    e. Auditing and logging of model decisions and rationale, to enable post hoc review and regulatory scrutiny.

4. The RFI must document and maintain a model inventory of all AI/ML models in use or under development, including metadata such as owner, version, input data sources, business purpose, validation summaries, control status, risk ratings, and dependencies.
5. Before deploying to production, AI/ML models must undergo independent validation (internal or external), adversarial testing (such as stress tests and injection of edge cases), and counterfactual analysis. The validation report, including a residual risk assessment, must be submitted to Senior Management and the Board for approval.
6. The RFI should implement continuous monitoring of AI/ML models in production, including detecting drift, performance degradation, unexpected outputs, fairness violations, or anomalous behaviour. Alerts must be triggered when thresholds are breached, and the RFI must have a rollback or a kill switch capability.
7. In any incident or breach involving an AI/ML model (e.g. model evasion attack, data poisoning, incorrect outputs causing financial or reputational losses), the RFI must report it to Bank of Ghana following the same incident reporting obligations outlined in PART VIII - CYBER RESPONSE with additional details about the model, affected data and mitigation measures taken.
8. The RFI shall include AI/ML risks in their risk register, evaluate control effectiveness and mitigation in accordance with PART V - CYBER AND INFORMATION SECURITY RISK MANAGEMENT.
9. Senior Management and the Board must receive periodic (at least quarterly) reports on AI/ML Model performance, risk metrics (e.g. drift, error rates, bias assessments), incidents and planned model changes.
10. The RFI shall ensure that the institution has the appropriate skills, training and awareness for AI/ML governance, security, interpretability and audit.

# PART XVIII - DATA CENTRE MANAGEMENT

RFIs shall ensure that all data centre facilities they operate or engage comply with the baseline requirements specified in this Directive to ensure resilience, security, and continuity of critical financial operations.

## 101. GOVERNANCE AND OPERATIONS

1. The RFI shall maintain documented policies, procedures, and an information security framework covering asset management, access control, incident response, and supplier management.
2. A governance structure with clear roles and responsibilities for risk, security, and operations shall be established.
3. The RFI shall operate a monitoring and response function for critical facility systems at all times.

## 102. BUSINESS CONTINUITY AND DISASTER RECOVERY

1. A business continuity and disaster recovery framework shall be in place, including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
2. Annual continuity tests (including failover or recovery simulations) shall be conducted and results documented (for the required testing frequency, refer to Annexure H – Testing Frequency).

## 103. SITE AND EXTERNAL RISK

1. The data centre shall be located, constructed, and designed to mitigate environmental and man-made risks, including flooding, seismic activity, fire and crime.
2. The RFI shall maintain an up-to-date site risk assessment with documented mitigation measures.

## 104. POWER AND ENERGY

1. The RFI shall maintain redundant and independent power supply paths with sufficient backup capacity in the facility.
2. Alternate power supply shall be provided to sustain operations for a minimum of 12–24 hours.
3. Power distribution paths to equipment racks shall be dual-fed.

## 105. COOLING AND ENVIRONMENTAL CONTROL

1. Heating, Ventilation and Air-conditioning (HVAC) systems shall be implemented to address the protection of supporting utilities in the data centre to maintain optimal environmental conditions.

2. Redundant cooling systems shall be in place to avoid single points of failure.
3. Continuous monitoring of environmental conditions shall be implemented with alarms and alerts.

## 106. FIRE PROTECTION

1. The RFI shall implement early fire detection and automatic suppression systems suitable for IT environments.
2. Fire-rated construction shall separate critical areas.
3. Fire response and evacuation plans shall be documented and tested.

## 107. CABLING AND CONNECTIVITY

1. Structured and managed cabling systems shall be implemented with proper labelling and records.
2. Connectivity shall include diverse entry paths, meet-me rooms, and redundant telecommunications providers.
3. Cable management shall ensure capacity headroom to prevent congestion.

## 108. PHYSICAL SECURITY

1. Multi-layered security shall be put in place to enforce access control, including perimeter protection, mantraps, and Closed-Circuit Television (CCTV).
2. Visitors shall be escorted and their access logged and controlled.
3. Critical spaces may require multi-factor authentication for entry.

## 109. SEGREGATION

1. Racks, cages, and suites shall be physically segregated and locked.
2. Shared spaces shall have policies preventing unauthorised access.

## 110. MONITORING AND INCIDENT RESPONSE

1. All critical facility systems (power, cooling, fire, and security) shall be continuously monitored.
2. Incident management processes shall be documented, with clear escalation paths and defined recovery procedures.
3. The RFI shall prepare incident and post-mortem reports.

## 111. CONTRACTS AND SLAS

1. Contracts with service providers shall specify uptime commitments, incident notification timelines, recovery objectives, and audit rights.
2. Uptime commitments shall reflect high availability expectations for critical financial systems.

## 112. VULNERABILITY AND MAINTENANCE OF FACILITY SYSTEMS

1. All building management, Uninterruptible Power Supply (UPS), power, HVAC and security systems shall be maintained on a documented schedule.
2. Where systems are software-driven, patching and hardening procedures shall be implemented.
3. Changes and maintenance windows shall be planned, documented, and communicated to all relevant parties.

## 113. COLOCATION

In addition to paragraphs 101-112, for all colocation arrangements, an RFI shall comply with the following requirements:

1. Colocation contracts shall include secure decommissioning and data/media destruction procedures.
2. The RFI shall ensure an annual cyber security assessment report is provided.
3. The RFI shall be notified of incidents and outages without undue delay.
4. Shared spaces shall have policies preventing unauthorised cross-tenant access.

# PART XIX - CYBER AND INFORMATION SECURITY REQUIREMENTS FOR ARTIFICIAL INTELLIGENCE (AI) SYSTEMS

The objective of this Part is to establish a binding governance, risk management, and control framework for the adoption, development, deployment, and operation of Artificial Intelligence (AI) and Machine Learning (ML) systems by Regulated Financial Institutions (RFIs).

This Part shall apply to all AI/ML systems, whether developed in-house, procured from a third party, or embedded within a broader product or service, that materially impact:

a. Financial or risk decision-making (e.g., credit scoring, underwriting, fraud detection, trading algorithms),
b. Customer interactions and support (e.g., chatbots, personalised marketing),
c. Regulatory compliance and reporting (e.g., AML screening, transaction monitoring), or
d. Core system operations and cybersecurity (e.g., network intrusion detection, predictive maintenance).

## 114. GENERAL PRINCIPLES

1. An RFI shall establish, implement, and maintain a comprehensive AI/ML Governance and Control Framework that addresses, at a minimum, the areas of:
    a. Governance, Accountability, and Oversight;
    b. AI/ML Risk Management;
    c. Data Management for AI/ML;
    d. Model Lifecycle Management, including validation and testing;
    e. Security Hardening and Robustness;
    f. Third-Party and Vendor Risk Management for AI/ML;
    g. Interpretability, Explainability, and Auditability;
    h. Operational Resilience and Contingency Planning; and
    i. Ethics, Fairness, and Regulatory Compliance.
2. The specific controls, technical requirements, and implementation guidance for the areas listed in paragraph 114(1) are detailed in Annexure E – AI/ML Governance and Control Guidelines, which forms an integral part of this Directive. Compliance with the provisions of Annexure E is mandatory.
3. The Board and Senior Management shall ensure that the institution possesses the necessary skills, expertise, and resources to understand, govern, and oversee the AI/ML systems it deploys.

## 115. REPORTING AND NOTIFICATION

1. An RFI shall include in its quarterly cyber and information security report to the Bank of Ghana a summary of its AI/ML inventory, material changes to its AI/ML risk profile, and a high-level overview of any significant model incidents or failures.
2. In addition to the requirements of PART VIII - CYBER RESPONSE, an RFI shall notify the Bank of Ghana immediately of any AI/ML-specific incident that results in, or has the potential to result in:
    a. Material financial loss to the institution or its customers,

b. Systemic bias or widespread customer harm,
c. Compromise of the model's integrity through adversarial attack (e.g., data poisoning, model theft), or
d. Significant regulatory or legal action.

# PART XX - CYBER AND INFORMATION SECURITY TESTING AND EXERCISE REGIME

This Part of the CISD establishes a comprehensive and mandatory framework for the testing of cyber and information security controls, defences, and response capabilities. It consolidates all testing requirements from across this Directive to ensure a systematic, risk-based approach to validating the effectiveness, resilience, and maturity of an RFI's security posture. All testing frequencies are aligned with the provisions of Annexure H – Testing Frequency.

Vulnerability Management covers the proactive identification of technical weaknesses in an RFI's infrastructure and applications.

Information about technical vulnerabilities of an RFIs information systems in use shall be obtained, exposure to such vulnerabilities shall be evaluated and appropriate measures taken to remediate adverse findings.

## 116. VULNERABILITY ASSESSMENT

1. An RFI shall conduct regular automated vulnerability scanning of all ICT assets, including network devices, servers, workstations, and applications, to identify missing patches, misconfigurations, and known security flaws.
2. The minimum frequency for vulnerability assessments shall be in accordance with the RFI's tier classification as defined in Annexure H, ranging from monthly automated scans for Tier 1 & 2 institutions to semi-annual automated scans for Tier 4 & 5 institutions.
3. All critical and high-risk findings must be documented, prioritised based on risk, and remediated according to a timeline approved by the CISO, not exceeding the timelines specified in PART V - CYBER AND INFORMATION SECURITY RISK MANAGEMENT.

## 117. CONFIGURATION COMPLIANCE SCANNING

1. The RFI shall implement regular scanning to validate that systems are configured in line with the institution's approved hardening standards (e.g., CIS benchmarks, NIST guidelines).
2. Configuration compliance against a recognised baseline must be reviewed at least quarterly, as stipulated in Annexure H – Testing Frequency.

## 118. PATCH AND CONFIGURATION COMPLIANCE VALIDATION

1. The RFI shall maintain a formal patch management process and conduct periodic reviews to ensure patches and configuration changes have been successfully and securely applied across the environment.
2. The frequency for these validation reviews shall be monthly for Tier 1 & 2 RFIs, quarterly for Tier 3, and semi-annually for Tier 4 & 5, as detailed in Annexure H – Testing Frequency.

## 119. WEB APPLICATION AND API TESTING (DAST/SAST)

1. All web applications, mobile applications, and APIs developed, owned, or operated by the RFI must undergo regular security testing, including Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST).
2. The frequency of testing shall be risk-based. For Tier 1 & 2 RFIs, critical applications require continuous or monthly scanning, while all applications must be tested at least quarterly. Frequencies for other tiers are specified in Annexure H – Testing Frequency.
3. Applications must be re-tested after any significant modification and prior to deployment to a production environment.

## 120. PENETRATION TESTING

1. The RFI shall conduct controlled penetration tests to simulate real-world attacks and assess the potential for unauthorised access or system compromise. These tests must cover network infrastructure, external and internal perimeters, and critical applications.
2. The minimum frequency for comprehensive penetration testing is bi-annually for Tier 1 & 2 RFIs, annually for Tier 3, and annually (external only) for Tier 4 & 5, as defined in Annexure H – Testing Frequency. Additional tests are required following significant system changes.
3. All penetration test findings must be remediated in accordance with a risk-based schedule, and a report must be submitted to the Cyber and Information Security Risk Management Committee.

## 121. RED TEAM EXERCISES AND ADVERSARIAL SIMULATION

1. To assess the effectiveness of people, processes, and technology in a holistic manner, the RFI shall conduct advanced adversarial simulation exercises (Red Teaming). These exercises go beyond standard penetration tests to emulate the tactics, techniques, and procedures of real threat actors.
2. The frequency for Red Team exercises shall be annually for Tier 1 & 2 RFIs, every two years for Tier 3, and every three years (or as directed by BoG) for Tier 4 & 5, as stipulated in Annexure H – Testing Frequency.

## 122. AI AND ML MODEL-SPECIFIC TESTING

1. For institutions deploying Artificial Intelligence or Machine Learning systems, testing must include evaluations for adversarial robustness, model drift, bias, and data poisoning.
2. AI/ML models must undergo independent validation and security testing prior to deployment and at periodic intervals thereafter, in line with the institution's risk assessment.

## 123. INCIDENT RESPONSE PLAN TESTING AND DRILLS

1. The CISO shall conduct regular exercises to test the effectiveness of the cyber incident response plan and the capabilities of the Cyber Response Team.
2. Small-scale exercises involving the cyber response unit and relevant ICT/business units shall be conducted quarterly.

3. A comprehensive, institution-wide exercise involving Senior Management and relevant business functions shall be conducted annually. The lessons learned report must be submitted to Senior Management and the Board.

## 124. BUSINESS CONTINUITY AND DISASTER RECOVERY TESTING (INCLUDING CLOUD)

1. The RFI shall test its business continuity and disaster recovery plans, including failover mechanisms for critical systems, data restoration from backups, and the operability of alternate sites. This includes testing failover to alternate cloud availability zones or regions, where applicable.
2. Disaster recovery and failover testing for critical systems must be conducted at least annually, as specified in Annexure H – Testing Frequency. The results must be documented and any shortcomings addressed.

## 125. CALL CENTRE AND TELEPHONY SECURITY TESTING

1. The CISO shall ensure that security, risk, resilience, and penetration tests are conducted on the call centre environment, including the telephony equipment and associated systems.
2. These tests must be conducted at least annually.

## 126. USER ACCESS REVIEWS

1. The RFI shall conduct periodic reviews of all user accounts, access rights, and permissions to ensure adherence to the principle of least privilege and to identify and remove unnecessary or dormant accounts. (Ref: paragraph 36(8), 56(3))
2. Access reviews for critical systems must be conducted at least twice a year, as stipulated in Annexure H – Testing Frequency. Reviews for non-critical systems shall be conducted at least annually.

## 127. ASSET INVENTORY REVIEW

1. The CISO, in coordination with asset owners, shall ensure the accuracy and completeness of the ICT and information asset inventory is reviewed at least annually or upon significant changes or events to the environment.

## 128. THIRD-PARTY SECURITY ASSESSMENT

1. The RFI shall conduct formal security assessments of its third-party service providers, suppliers, and business partners, based on the criticality of the services they provide.
2. Assessments for critical vendors shall be conducted at least annually for Tier 1-3 RFIs and biennially for Tier 4 & 5, as outlined in Annexure H – Testing Frequency. This may include reviewing independent audit reports (e.g., SOC 2), conducting on-site audits, or performing technical tests.

## 129. PHYSICAL SECURITY CONTROL TESTING

1. The RFI shall conduct routine maintenance and periodic testing of all physical security systems, including access control systems, surveillance equipment, and intrusion detection systems, to ensure their effectiveness.
2. These tests must be conducted at least annually and the evidence documented.

# PART XXI - INTERPRETATION

In this Directive, unless the context otherwise requires, words used have the same meaning as assigned to them as follows:

“Access Control” means the process of granting, denying, or restricting logical or physical access to information, systems, assets, or facilities based on defined rules, roles, and permissions. Source: NIST SP 800-53; CNSSI 4009.

“Advanced Persistent Threat (APT)” means an adversary with significant capability and persistence that uses multiple attack vectors over an extended period to achieve strategic objectives, including compromise, espionage, disruption, or positioning for future attack. Source: NIST SP 800-39.

“API Gateway” means an intermediary service that manages, brokers, secures, and monitors API traffic between clients and backend services. Source: NIST SP 800-204A.

“Application Programming Interface (API)” means a set of rules, protocols, and interfaces that enables different software applications, services, or components to communicate and exchange data.Source: NIST SP 800-204.

“Artificial Intelligence (AI)” means a machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, content, or decisions influencing real or virtual environments. Source: NIST AI RMF 1.0; OECD AI Principles.
“Assessment” means the testing or evaluation of management, operational, or technical controls to determine whether they are correctly implemented, operating as intended, and producing the required security outcome. Source: NIST SP 800-37; NIST SP 800-53A.

“Assessment Findings” means results produced by the application of an assessment procedure to a control or control enhancement, including determinations of whether the control is satisfied or not satisfied. Source: NIST SP 800-53A.

“Asset” means anything that has value to the RFI, including information, systems, software, hardware, services, facilities, processes, and personnel. Source: ISO/IEC 27000; CNSSI 4009.

“Attack” means an attempt to gain unauthorised access to system services, resources, or information, or to compromise system confidentiality, integrity, or availability. Source: NIST SP 800-32; CNSSI 4009.

“Authentication” means the process of verifying the identity of a user, process, device, or other entity as a prerequisite to granting access to resources. Source: NIST SP 800-53; NIST SP 800-63; CNSSI 4009.

“Authentication Factors” means the categories of evidence used to verify identity, including something the user knows, something the user has, and something the user is. Source: NIST SP 800-63B.

“Availability” means the property that information, services, and systems are accessible and usable on demand by authorised entities in a timely and reliable manner. Source: NIST SP 800-53; CNSSI 4009.

“Availability Zone” means an isolated location within a cloud region designed to reduce correlated failure and support resilient deployment of services and workloads. Source: NIST SP 800-145.

“Awareness” means activities intended to focus attention on security issues and enable individuals to recognise and respond appropriately to cyber and information security concerns. Source: NIST SP 800-50.

“Backup” means a separate copy of data, software, configurations, or systems retained for restoration in the event of loss, corruption, compromise, or failure. Source: NIST SP 800-34.

“Baseline Security” means the minimum set of security controls required to safeguard a system based on its confidentiality, integrity, and availability needs. Source: NIST SP 800-16.

“Biometric Authentication” means authentication based on measurable biological or behavioural characteristics such as fingerprints, facial features, voice, or iris patterns. Source: NIST SP 800-63B.

“Blacklist” means a list of entities, such as hosts, users, applications, addresses, or senders, that have been identified as malicious, unauthorised, or not permitted. Source: NIST SP 800-94; NIST SP 800-114.

“Blockchain” means a distributed ledger technology that records transactions in cryptographically linked blocks across a network of participants. Source: NISTIR 8202.

“Bring Your Own Device (BYOD)” means a practice that permits employees or other authorised users to access organisational systems and data using personally owned devices. Source: NIST SP 800-124.

“Bring Your Own Key (BYOK)” means a cryptographic key management model under which the customer supplies and controls encryption keys used to protect data in a cloud or external service environment.
“Cloud Computing” means a model that enables on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Source: NIST SP 800-145; CNSSI 4009.

“Cloud Security Posture Management (CSPM)” means processes or technologies used to identify, assess, and remediate security misconfigurations and compliance gaps in cloud environments. Source: Cloud Security Alliance.

“Cloud Service Provider (CSP)” means an entity that offers one or more cloud computing services to customers, including infrastructure, platform, or software services. Source: NIST SP 800-145.

“Cold Wallet” means an offline method for storing private keys or virtual assets in a manner designed to reduce exposure to online attack. Source: Cloud Security Alliance

“Compartmentalisation” means the practice of segregating systems, networks, or data into distinct security domains to limit the potential impact of a security breach.  Source: CNSSI 4009

“Community Cloud” means a cloud deployment model in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers with shared concerns. Source: NIST SP 800-145.

“Computer Forensics” means the practice of gathering, preserving, retaining, analysing, and presenting computer-related data for investigative purposes while maintaining its integrity. Source: CNSSI 4009; NIST SP 800-86.

“Computer Security Incident Response Team (CSIRT)” means a capability or team established to assist in responding to computer security-related incidents. Source: NIST SP 800-61.

“Confidentiality” means the principle of protecting information from unauthorised access or disclosure, ensuring that sensitive data is only accessible to authorised individuals. Source: ISO/IEC 27001.

“Consensus Protocol” means the rules and mechanisms by which participants in a distributed ledger or blockchain network agree on the validity and ordering of transactions. Source: NISTIR 8202.

“Container Escape” means a security failure or exploit by which a process running inside a container breaks isolation and gains unauthorised access to the host or other containers. Source: NIST SP 800-190.

“Containment” means the actions taken to limit, isolate, or control a security incident in order to prevent escalation, spread, or further damage. Source: NIST SP 800-61.

“Continuous Monitoring” means maintaining ongoing awareness of security controls, vulnerabilities, threats, events, and risks to support risk-based decision making. Source: CNSSI 4009.

“Controlled Access Area/Zone” means a physical area to which only authorised personnel are granted unrestricted access and all other persons are escorted or placed under continuous surveillance. Source: CNSSI 4009.

“Controlled Access Protection” means a minimum set of security functionalities that enforces access control, accountability, auditing, and resource isolation for individual users. Source: CNSSI 4009.

“Controlled Area/Zone” means an area or space for which the organisation has sufficient physical and procedural protections to meet information protection requirements. Source: NIST SP 800-53.

“Controlled Space” means the three-dimensional space surrounding information system equipment within which unauthorised individuals are denied unrestricted access. Source: CNSSI 4009.

“Countermeasure” means an action, device, procedure, technique, or control used to prevent, reduce, detect, respond to, or recover from a threat, vulnerability, or attack. Source: CNSSI 4009; NIST SP 800-53.

“Credential Compromise” means the disclosure, theft, loss, misuse, or unauthorised acquisition of authentication credentials such that they may be used by an unauthorised party. Source: NIST SP 800-63B.

“Cross-Tenant Attack” means an attack in a multi-tenant environment in which one tenant attempts to access, interfere with, or compromise another tenant’s data, workloads, or resources. Source: NIST SP 800-125A; Cloud Security Alliance.

“Cyber Attack” means an attack via cyberspace targeting the use of cyberspace for the purpose of disrupting, disabling, destroying, maliciously controlling computing resources, or compromising information integrity or confidentiality. Source: CNSSI 4009.

“Cyber Incident” means an actual or potentially adverse event or action affecting an information system or the information it processes, stores, or transmits, including attempted cyber attacks. Source: CNSSI 4009; NIST SP 800-61.

“Cyber Infrastructure” means electronic information and communications systems and services, and the information contained in them, including hardware, software, networks, control systems, and cyber services. Source: NISTIR 7628.

“Cyber Intelligence” means information relating to cyber threats, vulnerabilities, attack methods, indicators, or malicious activity that is gathered and analysed to support defence and risk management. Source: NIST SP 800-150.

“Cyber Response Team” means the RFI’s frontline function responsible for preparing for, detecting, analysing, responding to, and recovering from cyber and information security incidents. Source: ISO/IEC 27035-1; NIST SP 800-61.

“Cyber Risk” means the potential for damage, loss, disruption, or other adverse impact resulting from the occurrence of a cyber incident, taking into account probability and impact. Source: ISO/IEC 27005.

“Cyber Security” means the ability to protect or defend the use of cyberspace, information systems, networks, and data from cyber attacks and other malicious activities. Source: CNSSI 4009.

“Cyber Threat” means the threat of occurrence of a cyber incident or any circumstance indicating the potential for a cyber incident. Source: CNSSI 4009.

“Data Asset” means an information-based resource or any entity comprised of data, such as a database, file, document, output, service, or webpage. Source: CNSSI 4009.

“Data Classification” means the process of categorising data according to its sensitivity, value, criticality, or regulatory importance to determine the level of protection required. Source: ISO/IEC 27001; NIST SP 800-60.

“Data Integrity” means the property that data has not been altered, destroyed, or corrupted in an unauthorised manner while in storage, processing, or transit. Source: NIST SP 800-27.

“Data Lineage” means the record of the origin, movement, transformation, and use of data over its lifecycle. Source: NIST AI RMF 1.0; ISO/IEC 5259.

“Data Loss Prevention (DLP)” means measures or technologies used to detect and prevent the unauthorised disclosure, exfiltration, or loss of sensitive data. Source: NIST SP 800-53.

“Database Activity Monitoring (DAM)” means the monitoring and analysis of database activity to detect suspicious behaviour, misuse, or policy violations. Source: NIST SP 800-53.

“Database Firewall (DBF)” means a security mechanism that monitors, filters, and controls database access and queries based on defined security rules.Source: NIST SP 800-53.

“Demilitarised Zone (DMZ)” means a host, network segment, or perimeter zone logically placed between internal and external networks to provide controlled external access while shielding internal systems. Source: NIST SP 800-41; NIST SP 800-45; CNSSI 4009.

“Denial of Service (DoS)” means the prevention of authorised access to resources or the delaying of time-critical operations by exhausting or obstructing system capacity. Source: CNSSI 4009; NIST SP 800-61.

“Disaster Recovery Plan (DRP)” means management policy and procedures used to guide enterprise response and recovery following major loss of capability or damage to facilities or systems. Source: CNSSI 4009; NIST SP 800-34.

“Disruption” means an unplanned event that causes an information system, service, or major application to become inoperable or materially impaired for a period of time. Source: NIST SP 800-34; CNSSI 4009.

“Distributed Denial of Service (DDoS)” means a denial-of-service technique that uses numerous hosts or distributed resources to conduct the attack. Source: CNSSI 4009.

“Encryption” means the cryptographic transformation of data into a form that conceals its original meaning and protects confidentiality. Source: NIST SP 800-175B.

“Endpoint” means a computing device or node that communicates with a network and serves as a point of entry, exit, or access for data or services. Source: NIST SP 800-53.

“Endpoint Detection and Response (EDR)” means technology that continuously monitors endpoint devices to detect, investigate, contain, and respond to suspicious activity or threats. Source: NIST SP 800-61; NIST Cyber and information security Framework.

“End-to-End Encryption” means encryption in which information is encrypted at its origin and decrypted only at its intended destination, without intermediate decryption. Source: NIST SP 800-12; CNSSI 4009.

“End-to-End Security” means the safeguarding of information and communications from point of origin to point of destination. Source: CNSSI 4009.

““Event” means any observable occurrence within a system, network, or environment, such as a change of state, system action, or network activity. NIST SP 800 61 Rev.2/3 CNSSI 4009 2015”

“External Network” a network that is outside the organisation’s control and typically not governed by organisational security policies. Source: NIST SP 800 53 Rev.5;CNSSI 4009 2015”

“Failover” means the automatic or manual switching to a redundant or alternate system, site, zone, or component when the primary one fails or is impaired. Source: NIST SP 800-34.

“Firewall” means a hardware, software, or virtual capability that limits access between networks or systems according to a defined security policy. Source: NIST SP 800-32; CNSSI 4009.

“Forensics” means the gathering, preservation, retention, analysis, and presentation of computer-related data for investigative purposes while maintaining data integrity. Source: CNSSI 4009; NIST SP 800-86.

“Guard” means a mechanism that limits or mediates the exchange of information between systems or subsystems. Source: CNSSI 4009.

“Hacker” means an unauthorised user who attempts to gain, or gains, access to an information system. Source: CNSSI 4009.

“Hardening” means the process of reducing system vulnerabilities by securely configuring hardware, software, operating systems, network devices, or applications and disabling unnecessary functions. Source: NIST SP 800-123; CIS Benchmarks.

“Hardware-Backed Secret Vault” means a system or module that stores secrets or cryptographic material using hardware-based protection and controlled access mechanisms. Source: NIST SP 800-57; NIST SP 800-152.

“Hybrid Cloud” means a cloud deployment model composed of two or more distinct cloud infrastructures that remain unique entities but are bound together to enable portability or interoperability. Source: NIST SP 800-145.

“Hypervisor” means software, firmware, or hardware that creates and runs virtual machines and enables multiple operating systems or workloads to share a physical host. Source: NIST SP 800-125.

“Identification” means the process of claiming or establishing the identity of a user, process, or device, usually as a prerequisite to granting access. Source: NIST SP 800-47.

“Identity” means a set of attributes that uniquely describes a person, service, device, or other entity within a given context. Source: NIST SP 800-63.

“Identity and Access Management (IAM)” means the policies, processes, and technologies used to manage identities and control access to systems, applications, and data. Source: NIST SP 800-63; NIST SP 800-53.

“Incident” means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, or an event that actually or potentially jeopardises confidentiality, integrity, or availability. Source: NIST SP 800-61; CNSSI 4009.

“Incident Handling” means the mitigation, response, and management of security policy violations and related incidents. Source: NIST SP 800-61.

“Incident Preparedness” means the state of planning, capability, resources, and readiness necessary to detect, respond to, contain, eradicate, and recover from security incidents. Source: NIST SP 800-61; ISO/IEC 27035-1.

“Indicator” means a sign or observable artefact suggesting that an incident may have occurred or may currently be occurring. Source: NIST SP 800-61.

“Information Asset” means data, information, systems, information processing facilities, documents, and knowledge that support asset management and organisational objectives and require governance and lifecycle management. Source: NIST SP 800-37 and ISO/IEC 27000.

“Information Security” means the protection of information and information systems against unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Source: NIST SP 800-37; NIST SP 800-53; CNSSI 4009.

“Information Security Continuous Monitoring (ISCM)” means maintaining ongoing awareness of information security, vulnerabilities, threats, and control effectiveness to support organisational risk decisions. Source: NIST SP 800-137.

“Information Security Management System (ISMS)” means a systematic approach to establishing, implementing, maintaining, and continually improving information security. Source: ISO/IEC 27001.

“Information Security Policy” means the aggregate of directives, rules, regulations, and practices prescribing how an organisation manages, protects, and distributes information. Source: NIST SP 800-53; NIST SP 800-18; CNSSI 4009.

“Information Security Risk” means the risk to operations, assets, individuals, other organisations, or the nation due to the potential for unauthorised access, use, disclosure, disruption, modification, or destruction of information or information systems. Source: NIST SP 800-30.

“Information System” means a discrete set of information resources organised for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Source: NIST SP 800-53.

“Infrastructure as a Service (IaaS)” means a cloud service model that provides processing, storage, networks, and other fundamental computing resources on which the consumer can deploy and run arbitrary software. Source: NIST SP 800-145.

“Intrusion” means an unauthorised act of bypassing the security mechanisms of a system. Source: CNSSI 4009.

“Intrusion Detection and Prevention System (IDPS)” means software or a system that monitors computer or network events for signs of possible incidents and attempts to stop detected incidents. Source: NIST SP 800-61.

“Intrusion Detection System (IDS)” means hardware or software that gathers and analyses information from systems or networks to identify possible security breaches or misuse. Source: CNSSI 4009.

“Intrusion Prevention System (IPS)” means a system able to detect intrusive activity and attempt to stop the activity, ideally before it reaches its target. Source: NIST SP 800-36; CNSSI 4009.

“JSON” means JavaScript Object Notation, a lightweight structured data-interchange format commonly used in APIs and digital services. Source: RFC 8259.

“Key Management Service (KMS)” means a system or service used to generate, store, protect, rotate, distribute, and manage cryptographic keys. Source: NIST SP 800-57.

“Least Privilege” means the principle that each user, process, or entity is granted only the minimum system resources and authorisations needed to perform its function. Source: NIST SP 800-12; CNSSI 4009.

“Logging” means the process of recording events occurring within an information system for monitoring, investigation, auditing, and accountability. Source: NIST SP 800-92.

“Machine Learning (ML)” means a type of artificial intelligence in which systems learn patterns, relationships, or decision rules from data to improve performance on tasks. Source: NIST AI RMF 1.0; ISO/IEC 22989.

“Malicious Code” means software or firmware intended to perform an unauthorised process that adversely affects the confidentiality, integrity, or availability of an information system. Source: NIST SP 800-53; CNSSI 4009.

“Malware” means a program or code-based malicious entity inserted into a system, usually covertly, to compromise confidentiality, integrity, availability, or otherwise disrupt operations. Source: NIST SP 800-83; NIST SP 800-61.

“Managed Security Service Provider (MSSP)” means a third-party provider engaged to deliver managed cyber and information security services such as monitoring, incident response, threat intelligence, SIEM, DFIR, or related security operations. Source: NIST SP 800-160.

“Micro-segmentation” means the use of granular segmentation policies to isolate workloads, applications, or network paths and restrict east-west traffic within an environment. Source: NIST SP 800-207.

“Microservice Architecture” means an architectural approach in which an application is composed of small, independently deployable services that communicate over defined interfaces. Source: NIST SP 800-204.

“Migration and Exit Plan” means a documented strategy and set of procedures for moving services, workloads, or data into, out of, or between service environments while maintaining business continuity and data control. Source: DORA (Digital Operational Resilience Act; ISO/IEC 27017)

“Model Drift” means degradation or change in model performance or behaviour over time due to changes in data, environment, or underlying conditions. Source: NIST AI RMF 1.0.

“Monitoring” means the ongoing observation and review of systems, services, users, events, and security conditions for operational, risk, and security purposes. Source: NIST SP 800-137.

“Multi-Factor Authentication (MFA)” means an authentication method that requires two or more different factors to verify the identity of a user or entity. Source: NIST SP 800-63B.

“Multi-Tenancy” means a cloud architecture in which a single instance of software or infrastructure serves multiple customers while maintaining logical separation of their data and operations. Source: NIST SP 800-145.

“Mutual Authentication” means a process in which parties at both ends of a communication authenticate each other. Source: NIST SP 800-32.

“Need-To-Know” means a method of isolating information resources based on a user’s need to access the resource in order to perform assigned duties and no more. Source: NIST SP 800-192.

“Network Segmentation” means splitting a network into sub-networks, for example, by creating separate areas on the network which are protected by firewalls configured to reject unnecessary traffic for that section. Source: NIST SP 800-125B.

“Non-repudiation” means assurance that the sender of information cannot deny having sent it and the recipient cannot deny having received or processed it. Source: CNSSI 4009; NIST SP 800-60; FIPS 186.

“Outsourcing” means the use of an external service provider to perform a function, activity, or service that would otherwise be undertaken by the RFI itself. Source: Basel outsourcing principles; ISO/IEC 27036.

“Password Management” means the policies, processes, and technical controls used to create, protect, rotate, store, reset, and retire passwords or related authenticators. Source: NIST SP 800-63B.

“Penetration Testing” means security testing in which evaluators mimic real-world attacks to identify ways to circumvent the security features of an application, system, or network. Source: NIST SP 800-115; NIST SP 800-53A.

“Perimeter” means the boundary encompassing all components of a system or network subject to a defined security policy or accreditation scope. Source: CNSSI 4009.

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information. Source: NIST SP 800-122.

“Platform as a Service (PaaS)” means a cloud service model that provides the capability to deploy consumer-created or acquired applications using programming languages, libraries, services, and tools supported by the provider. Source: NIST SP 800-145.

“Privacy” means the protection of personal or subscriber information and the restriction of access, processing, or disclosure in accordance with law and regulation. Source: NIST SP 800-32.

“Private Cloud” means a cloud deployment model provisioned for exclusive use by a single organisation comprising multiple consumers. Source: NIST SP 800-145.

“Private Endpoint” means a cloud networking construct that enables access to a service over a private network path rather than public internet exposure. Source: Cloud Security Alliance guidance.

“Privilege Escalation” means the exploitation of a flaw, weakness, or misconfiguration to obtain higher access rights or privileges than those originally authorised. Source: NIST SP 800-61; NIST SP 800-53.

“Privileged Access Management (PAM)” means policies, processes, and technologies used to control, monitor, and secure access for users or accounts with elevated privileges. Source: NIST SP 800-53.

“Proxy” means an application that intermediates a connection between client and server by receiving, processing, and forwarding traffic. Source: NIST SP 800-44.

“Public Cloud” means a cloud deployment model provisioned for open use by the general public. Source: NIST SP 800-145.

“Quantum Computing” means a computing paradigm that uses quantum-mechanical phenomena, such as superposition and entanglement, to perform certain computations. Source: NIST quantum terminology; ISO/IEC 4879.

“Recovery” means the restoration of systems, services, and operations to normal or acceptable functionality after an incident or disruption. Source: NIST SP 800-61; NIST SP 800-34.

“Recovery Point Objective (RPO)” means the maximum tolerable period in which data might be lost due to a major incident before recovery takes place. Source: NIST SP 800-34.

“Recovery Time Objective (RTO)” means the maximum tolerable length of time that a system, service, or process can be unavailable after a disruption. Source: NIST SP 800-34.

“Regulated Financial Institution (RFI)” means Regulated Financial Institution. For definition refer to Applicability, paragraph(2).

“Related Party” means any person or entity that has a direct or indirect relationship with a regulated financial institution that enables the exercise of control or significant influence over the institution’s management or policies. This includes Directors and key management personnel of the institution, significant shareholders (e.g., persons with substantial interest), close family members of directors or key management, entities in which the institution or its key persons have significant ownership or control, affiliates, subsidiaries, and parent companies.

“Remediation” means the act of correcting a vulnerability, eliminating a threat, or otherwise resolving a weakness through measures such as patching, reconfiguration, or removal. Source: NIST SP 800-40.

“Remediation Plan” means a plan to perform remediation of one or more threats or vulnerabilities, including treatment options and priorities. Source: NIST SP 800-40.

“Residual Risk” means the remaining risk after all planned and implemented security measures, controls, or mitigation actions have been applied. Source: NIST SP 800-33; ISO/IEC 27005.

“Resilience” means the ability to continue operating under adverse conditions while maintaining essential capabilities and to recover to an effective operational posture within a required timeframe. Source: NIST SP 800-137.

“Risk” means a measure of the extent to which an entity is threatened by a potential circumstance or event, typically as a function of likelihood and adverse impact. Source: NIST SP 800-37; NIST SP 800-60.

“Risk Analysis” means the process of identifying risks and determining their likelihood, impact, and the safeguards that can reduce or manage them. Source: NIST SP 800-27.

“Risk Assessment” means the process of identifying, prioritising, and estimating risks by considering threats, vulnerabilities, likelihood, and impact. Source: CNSSI 4009; NIST SP 800-30.

“Risk Management” means the process of managing risks to operations, assets, individuals, and systems, including risk assessment, mitigation, and continuous monitoring. Source: NIST SP 800-53; NIST SP 800-37.

“Risk Management Framework (RMF)” means a structured approach used to manage and oversee risk throughout the lifecycle of systems and services. Source: CNSSI 4009; NIST SP 800-37.

“Risk Mitigation” means the prioritisation, evaluation, and implementation of controls or countermeasures to reduce risk. Source: CNSSI 4009; NIST SP 800-30; NIST SP 800-39.

“Risk Monitoring” means maintaining ongoing awareness of the risk environment, risk management programme, and associated activities to support risk decisions. Source: NIST SP 800-30; NIST SP 800-39.

“Robotics” means programmable systems or machines capable of carrying out physical or cognitive tasks, often autonomously or semi-autonomously. Source: ISO 8373.

“Role-Based Access Control (RBAC)” means an access control approach in which permissions are assigned to roles and users receive permissions through role assignment. Source: NIST RBAC model; INCITS 359.

“Rollback Strategy” means a predefined method for restoring systems, data, and configurations to a previously known stable state after a failed migration, deployment, or update. Source: NIST SP 800-34.

“Safeguards” means protective measures prescribed to meet confidentiality, integrity, and availability requirements for an information system. Source: NIST SP 800-53; FIPS 200; CNSSI 4009.

“Sandboxing” means a method of isolating code, applications, or modules into distinct domains so that untrusted or risky processes can execute with restricted access. Source: NIST SP 800-19.

“Secure Development Life Cycle (SDLC)” means a development process that integrates security activities and controls into each stage of system or software development. Source: NIST SP 800-64; NIST SP 800-218.

“Secure Relay” means a controlled intermediary mechanism used to transfer information or communications securely between parties or environments.

“Security Architecture” means the strategic and technical design of security controls, principles, patterns, and mechanisms across systems, networks, and services. Source: NIST SP 800-160 Vol. 2.

“Security Association” means a relationship established between two or more entities to enable protection of data they exchange. Source: CNSSI 4009.

“Security Control Assessment” means the testing or evaluation of management, operational, and technical controls to determine whether they are correctly implemented and effective. Source: NIST SP 800-37; NIST SP 800-53A.

“Security Control Effectiveness” means the measure of how correctly a control is implemented and how well it meets organisational needs in accordance with current risk tolerance. Source: NIST SP 800-137.

“Security Controls” means management, operational, and technical safeguards or countermeasures prescribed for a system to protect its confidentiality, integrity, and availability. Source: NIST SP 800-53; FIPS 200; CNSSI 4009.

“Security Information and Event Management (SIEM)” means a capability or set of tools for centralised collection, aggregation, correlation, analysis, and monitoring of security event and log data from multiple sources. Source: NIST SP 800-137; NIST SP 800-92.

“Security Operations Centre (SOC)” means the centralised function or facility responsible for monitoring, detecting, analysing, and responding to cyber and information security events and incidents.
Source: NIST Cyber and information security Framework; derived from the Directive.

“Security Perimeter” means a physical or logical boundary within which a particular security policy or architecture is applied. Source: CNSSI 4009.

“Security Policy” means the statement of required protection for information, systems, and services, and the criteria for the provision of security services. Source: NIST SP 800-27; FIPS 188.

“Security Requirements” means requirements derived from laws, directives, policies, standards, regulations, procedures, or mission needs to ensure confidentiality, integrity, and availability. Source: FIPS 200; NIST SP 800-53; CNSSI 4009.

“Security Safeguards” means protective measures and controls prescribed to meet defined security requirements for systems, assets, facilities, and information. Source: CNSSI 4009.

“Senior Management” means the highest level of managers in the RFI, 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.

“Sensitive Position” means a role within the RFI where the employee’s access, responsibilities, or decisions could significantly affect financial integrity, information security, or operational stability. Source: NIST SP 800-53 Rev. 5; ISO/IEC 27001.

“Serverless Architecture” means an architecture in which the underlying infrastructure and server management are abstracted from the consumer, typically through event-driven execution models. Source: NIST SP 800-204A.

“Service Level Agreement (SLA)” means a documented agreement that defines service expectations, responsibilities, performance targets, and remedies between service parties. Source: ISO/IEC 20000-1;

“Shared Responsibility Matrix” means a documented allocation of security and control responsibilities between the CSP, the RFI, and any shared parties for each control domain. Source: CSA CCM; ISO/IEC 27017.

“Shared Responsibility Model” means a cloud governance model under which the cloud provider and the customer each bear defined responsibilities for implementing and operating security controls. Source: NIST SP 800-145;.

“Simple Mail Transfer Protocol (SMTP)” means a protocol used to send and relay electronic mail messages between systems. Source: RFC 5321.

“Social Engineering” means the use of deception or manipulation to trick people into revealing sensitive information or performing actions that compromise security. Source: NIST SP 800-114.

“Software as a Service (SaaS)” means a cloud service model in which the consumer uses the provider’s applications running on a cloud infrastructure. Source: NIST SP 800-145.

“Storage Bucket” means a logical cloud storage container used to hold objects, files, or data within an object storage service.

“Supply Chain” means the system of organisations, people, activities, information, and resources that provides products or services to consumers. Source: NIST SP 800-53; CNSSI 4009.

“Survivability” means the capability of a system, service, or organisation to continue operating and delivering essential functions while under attack, failure, or adverse conditions, and to recover after the event. Source: NIST SP 800-160 Vol. 2; CNSSI 4009.

“System Integrity” means the quality that a system has when it performs its intended function in an unimpaired manner and remains free from unauthorised manipulation. Source: NIST SP 800-27.

“Technical Controls” means security controls implemented and executed primarily through hardware, software, or firmware mechanisms. Source: NIST SP 800-53; FIPS 200.

“Tenant Isolation” means the logical, and where applicable physical, separation of one tenant’s data, workloads, and control plane from another tenant’s within a shared environment. Source: NIST SP 800-125A; CSA guidance.

“Test” means an assessment method characterised by exercising one or more assessment objects under specified conditions and comparing actual with expected behaviour. Source: NIST SP 800-53A.

“Third Party” means any person or entity that is independent of the regulated financial institution and does not qualify as a related party, but provides goods, services, or support to the institution or otherwise interacts with it on a contractual or business basis. This includes vendors and suppliers, IT and cloud service providers, consultants and contractors, outsourced service providers, business partners without ownership/control relationships, sub-suppliers, sub-contractors etc.

“Threat” means any circumstance or event with the potential to adversely impact operations, assets, or individuals through unauthorised access, destruction, disclosure, modification, or denial of service. Source: FIPS 200.

“Threat Analysis” means the examination of threat sources against system vulnerabilities to determine relevant threats in a specific operational environment. Source: NIST SP 800-27.

“Threat Assessment” means the formal evaluation of the degree and nature of threat to an information system or enterprise. Source: CNSSI 4009; NIST SP 800-53A.

“Threat Intelligence” means evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging threat or hazard. Source: NIST SP 800-150.

“Threat Monitoring” means the analysis, assessment, and review of audit trails and other information for the purpose of identifying events that may constitute security violations. Source: CNSSI 4009.

“Tier-n Supplier” means an indirect supplier or subcontractor beyond the first tier in the supply chain whose products or services may affect the RFI’s operations or security posture. Source: NIST SP 800-161 Rev. 1.

“Transport Layer Security (TLS)” means a cryptographic protocol used to provide confidentiality, integrity, and authenticity for communications over a network. Source: RFC 8446.

“Unauthorised Access” means access by a user or entity to a resource that the user or entity is not permitted to use. Source: FIPS 191.

“User and Entity Behaviour Analytics (UEBA)” means techniques or technologies that analyse user and entity behaviour patterns to detect anomalies indicative of compromise, insider threat, or misuse. Source: NIST Cyber and information security Framework; industry practice.

“Vendor Lock-In” means a condition in which a customer becomes dependent on a provider’s proprietary products, formats, interfaces, or services, making migration or substitution difficult or costly. Source: NIST cloud computing guidance; CSA guidance.

“Virtual Asset” means a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes, but does not include digital representations of fiat currency, securities, or other financial assets where excluded by law. Source: FATF guidance.

“Virtual Private Network (VPN)” means a virtual network that provides protected communications over untrusted networks through tunnelling, encryption, and authentication. Source: NIST SP 800-77.

“Vulnerability” means a weakness in an information system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-53; FIPS 200.

“Vulnerability Assessment” means the systematic examination of a system, product, or environment to determine the adequacy of security measures and identify security deficiencies. Source: NIST SP 800-53A; CNSSI 4009.

“Web Application Firewall (WAF)” means a security capability that monitors, filters, and blocks malicious traffic to or from web applications and can provide protection against web application attacks, including some zero-day attacks. Source: NIST SP 800-44.

“Wide Area Network (WAN)” means a communications network that spans a broad geographic area and interconnects multiple smaller networks or sites. Source: NIST SP 800-82.

“Zero Trust Architecture” means an enterprise cyber and information security architecture in which no implicit trust is granted to assets or user accounts based solely on physical or network location, and access decisions are continuously verified. Source: NIST SP 800-207.

“Zero-Day Attack” means an attack that exploits a previously unknown or unpatched vulnerability before a fix, signature, or effective mitigation is available. Source: NIST SP 800-61; CNSSI 4009.

# ANNEXURES

The annexures contained in this Directive are provided as guidance to support the implementation of the requirements set out herein. Their application shall be determined based on the outcome of an information security risk assessment and the specific circumstances of the relevant arrangement or engagement. Where clarification is required, or where uncertainties arise in the application of these annexures, the RFIs shall consult Bank of Ghana for appropriate guidance.

# ANNEXURE A – PROPORTIONALITY FRAMEWORK

| | | TIER ONE (1) | | TIER TWO (2) | | TIER THREE (3) | | TIER FOUR (4) | | TIER FIVE (5) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions | | Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers | | Community Banks (RCBs), Digital Credit Service Providers | | Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs | | PSP Medium, PSPs Standards. PFTSP | |
| | **PARAGRAPH** | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments |
| | | | | | | | | | | | |
| | **PART I - PRELIMINARY MATTERS** | | | | | | | | | | |
| 1 | Objective | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 2 | Applicability | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 3 | Proportionality and Case-by-Case Assessment | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 4 | Obligations of Regulated Entities | ✓ | | ! | An RFI may apply for exemption for 4(9) | ! | An RFI may apply for exemption for 4(9) | ✗ | | ! | An RFI may apply for exemption for 4(9) and 4(10). |
| | **PART II - GOVERNANCE** | | | | | | | | | | |
| 5 | The Board | ✓ | | ✓ | | ✓ | 5 (3) Board Cyber and Information Security responsibilities shall be included in the Board Risk Committee charter. | ✓ | 5 (3) Board Cyber and Information Security responsibilities shall be included in the Board charter. | ✓ | 5 (3) Board Cyber and Information Security responsibilities shall be included in the Board charter. |
| 6 | The Senior Management | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 7 | Internal Audits | ✓ | | ✓ | | ✓ | | ! | An RFI may outsource Cyber and Information Security internal audit responsibilities on case by case basis. | ! | An RFI may outsource Cyber and Information Security internal audit responsibilities on case by case basis. |
| 8 | Information Security Department | ✓ | | ✓ | | ! | An RFI may assign Information Security Department responsibilities to Risk Office/ Department or outsource on case by case basis. | ! | An RFI may assign Information Security Department responsibilities to Risk Office/ Department or outsource on case by case basis. | ! | An RFI may assign Information Security Department responsibilities to Risk Office/ Department or outsource on case by case basis. |
| 9 | Information Security Budget Management | ✓ | | ✓ | | ! | An RFI may have a dedicated Information Security Budget on case by case basis. | ! | An RFI may have a dedicated Information Security Budget on case by case basis. | ! | An RFI may have a dedicated Information Security Budget on case by case basis. |
| | **PART III - THE CHIEF INFORMATION SECURITY OFFICER** | | | | | | | | | | |

| | | TIER ONE (1) | | TIER TWO (2) | | TIER THREE (3) | | TIER FOUR (4) | | TIER FIVE (5) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions | | Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers | | Community Banks (RCBs), Digital Credit Service Providers | | Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs | | PSP Medium, PSPs Standards. PFTSP | |
| | **PARAGRAPH** | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments |
| 10 | Appointment | ✓ | | ✓ | | ! | An RFI may assign CISO responsibilities to Risk Manager or outsource CISO function on case by case basis. | ! | An RFI may outsource CISO function on case by case basis or apply for exemption. | ! | An RFI may outsource CISO function on case by case basis or apply for exemption. |
| 11 | Status in the institutional Hierarchy | ✓ | | ✓ | | ! | An RFI may assign CISO responsibilities to Risk Manager or outsource CISO function on case by case basis. | ! | An RFI may outsource CISO function on case by case basis or apply for exemption. | ! | An RFI may outsource CISO function on case by case basis or apply for exemption. |
| 12 | Responsibilities | ✓ | | ✓ | | ! | An RFI may assign CISO responsibilities to Risk Manager or outsource CISO function on case by case basis. | ! | An RFI may outsource CISO responsibilities on case by case basis or apply for exemption. | ! | An RFI may outsource CISO responsibilities on case by case basis or apply for exemption. |
| **PART IV - CYBER AND INFORMATION SECURITY POLICY AND PROCEDURES** | | | | | | | | | | | |
| 13 | Policy | ✓ | | ✓ | | ! | RFIs shall develop broad policies to cover the requirements of cyber security risk management. | ! | RFIs shall develop broad policies to cover the requirements of cyber security risk management. | ! | RFIs shall develop broad policies to cover the requirements of cyber security risk management. |
| 14 | Procedures | ✓ | | ✓ | | ! | RFIs shall develop broad procedures to cover the requirements of cyber security risk management. | ! | RFIs shall develop broad procedures to cover the requirements of cyber security risk management. | ! | RFIs shall develop broad procedures to cover the requirements of cyber security risk management. |
| 15 | The Cyber and Information Security Risk Management Committee | ✓ | | ✓ | | ! | 13 (3) The Committee member shall include MD, Risk Manager (CISO), IT Manager and any senior management member. | ✗ | | ! | 13(3) The Committee resposibilities may be assigned to the MD on case by case basis |
| **PART V - CYBER AND INFORMATION SECURITY RISK MANAGEMENT** | | | | | | | | | | | |
| 16 | Risk Management | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 17 | Risk Identification | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 18 | Risk Analysis | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |

| | | TIER ONE (1) | | TIER TWO (2) | | TIER THREE (3) | | TIER FOUR (4) | | TIER FIVE (5) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions | | Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers | | Community Banks (RCBs), Digital Credit Service Providers | | Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs | | PSP Medium, PSPs Standards. PFTSP | |
| | **PARAGRAPH** | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments |
| 19 | Risk Assessments in Cloud Environment | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 20 | Risk Mitigation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 21 | Risk Evaluation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 22 | Risk Monitoring and Reporting | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| | **PART VI - ASSET MANAGEMENT** | | | | | | | | | | |
| 23 | Inventory | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 24 | Ownership | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 25 | Acceptable Use | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 26 | Asset Mapping and Classification | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| | **PART VII - CYBER DEFENCE** | | | | | | | | | | |
| 27 | Security Infrastructure | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 28 | Architecture | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 29 | Network Elements | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 30 | Network Management | ✓ | | ✓ | | ! | An RFI may implement Network Management based on risk profile | ! | An RFI may implement Network Management based on risk profile | ! | An RFI may implement Network Management based on risk profile |
| 31 | Encryption | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 32 | Media Encryption | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 33 | Remote Access | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 34 | Internet Access | ✓ | | ✓ | | ✓ | | ! | An RFI may apply for exemption from 2 (a) (i), (ii), (iii) and 2 (b) | ✓ | |
| 35 | Websites and Web Applications Protection | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 36 | Access Control and Authentication | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 37 | Biometric Authentication | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 38 | Compartmentalisation and Permissions | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 39 | Servers and Workstations | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 40 | Databases | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 41 | Software Information Security | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 42 | Application Programming Interface (API) | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |

| | | TIER ONE (1) | | TIER TWO (2) | | TIER THREE (3) | | TIER FOUR (4) | | TIER FIVE (5) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions | | Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers | | Community Banks (RCBs), Digital Credit Service Providers | | Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs | | PSP Medium, PSPs Standards. PFTSP | |
| | **PARAGRAPH** | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments |
| 43 | Auditing | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 44 | Incident Preparedness | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 45 | Cyber Intelligence and Research | ✓ | | ✓ | | ✓ | | ✗ | | ✓ | |
| **PART VIII - CYBER RESPONSE** | | | | | | | | | | | |
| 46 | Structure and Hierarchy | ✓ | | ✓ | | ! | In addition to the proportionality provisons for the CISO, an RFI shall include the cyber response function in the CISO's terms of reference. | ✗ | | ! | In addition to the proportionality provisons for the CISO, an RFI shall include the cyber response function in the CISO's terms of reference. |
| 47 | Security Information and Event Management (SIEM) | ✓ | | ✓ | | ✓ | | ! | An RFI shall implement alternate mechanisms to monitor system | ✓ | |
| 48 | Security Operations Centre (SOC) | ✓ | | ✓ | | ✓ | | ! | An RFI shall implement mechanisms for monitoring cyber and information security alerts and incidents. | ✓ | |
| 49 | Methodology | ✓ | | ✓ | | ✓ | | ✗ | | ✓ | |
| 50 | Incident Handling | ✓ | | ✓ | | ✓ | | ✗ | | ✓ | |
| 51 | Reporting to the BoG | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 52 | Managed Security Service Provider (MSSP) | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| **PART IX - HUMAN RESOURCE SECURITY, ACCESS CONTROL AND CYBER COMPETENCY FRAMEWORK** | | | | | | | | | | | |
| 53 | Access Control | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 54 | Hiring and Onboarding | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 55 | New Employee | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 56 | Sensitive Positions | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 57 | Employee Lifecycle | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 58 | Termination | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 59 | Cyber Education | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 60 | Cyber Exercise | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |

| | | TIER ONE (1) | | TIER TWO (2) | | TIER THREE (3) | | TIER FOUR (4) | | TIER FIVE (5) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions | | Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers | | Community Banks (RCBs), Digital Credit Service Providers | | Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs | | PSP Medium, PSPs Standards. PFTSP | |
| | **PARAGRAPH** | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments |
| 61 | Artificial Intelligence (AI) and Machine Learning (ML) | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| **PART X - CHANNELS OF COMMUNICATION WITH EXTERNAL ENTITIES** | | | | | | | | | | | |
| 62 | Data Transfer between Sites and Organisations | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 63 | Email | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 64 | Web Access | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 65 | Bring Your Own Device (BYOD) | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 66 | Institutional mobile device | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| **PART XI - ELECTRONIC BANKING PLATFORMS** | | | | | | | | | | | |
| 67 | General Controls | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 68 | Subscribing to Electronic Banking Platforms | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 69 | Identification and Authentication | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 70 | Website | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 71 | Mobile Applications | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 72 | Email | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 73 | Telephony Services | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 74 | Customer Security | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 75 | Passwords and Password Management | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| **PART XII - EXTERNAL CONNECTIONS** | | | | | | | | | | | |
| 76 | Direct Connectivity | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 77 | Other Financial and non-RFIs | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 78 | Business Partners | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 79 | Remote Access | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 80 | External Parties | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 81 | Data in Motion | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| **PART XIII - CLOUD SERVICES** | | | | | | | | | | | |
| 82 | Corporate Governance | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 83 | Risk Management | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 84 | The Cloud Computing Service Contract | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |

| | | TIER ONE (1) | | TIER TWO (2) | | TIER THREE (3) | | TIER FOUR (4) | | TIER FIVE (5) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions | | Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers | | Community Banks (RCBs), Digital Credit Service Providers | | Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs | | PSP Medium, PSPs Standards. PFTSP | |
| | **PARAGRAPH** | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments |
| 85 | Institutional Application Development | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 86 | Promotional Material | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 87 | Cloud Operations, Monitoring and Resilience | ✓ | | ✓ | | ! | An RFI may apply for exemption on a case by case basis | ! | An RFI may apply for exemption on a case by case basis | ! | An RFI may apply for exemption on a case by case basis |
| 88 | Cloud Security Controls and Assurance | ✓ | | ✓ | | ! | An RFI may apply for exemption on a case by case basis | ! | An RFI may apply for exemption on a case by case basis | ! | An RFI may apply for exemption on a case by case basis |
| | **PART XIV - RFIs WITH INTERNATIONAL AFFILIATION** | | | | | | | | | | |
| 89 | Foreign RFIs in Ghana | ✓ | | ✓ | | ✗ | | ✗ | | ✗ | |
| 90 | Ghanaian RFIs Operating Abroad | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| | **PART XV - PHYSICAL SECURITY** | | | | | | | | | | |
| 91 | General | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 92 | Secured Zones | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 93 | Segmentation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 94 | Physical Security of Hardware and Other Equipment | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| | **PART XVI - CONTRACTUAL ASPECTS** | | | | | | | | | | |
| 95 | Cyber Security Contracts | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 96 | Supply Chain Cyber Security Contracts Obligation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 97 | Contracts Involving AI, ML or Algorithmic Services | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| | **PART XVII - DIGITAL INNOVATIONS** | | | | | | | | | | |
| 98 | General | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 99 | Data Privacy and Confidentiality Requirements | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 100 | AI/ML Governance and Security | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| | **PART XVIII - DATA CENTRE MANAGEMENT** | | | | | | | | | | |
| 101 | Governance & Operations | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 102 | Business Continuity & Recovery | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 103 | Site & External Risk | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 104 | Power & Energy | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |

| | | TIER ONE (1) | | TIER TWO (2) | | TIER THREE (3) | | TIER FOUR (4) | | TIER FIVE (5) | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Banks, ARB Apex Bank, Apex Bank, DEMIs, PSP Scheme & Development Finance Institutions | | Microfinance Banks (S&L, Finance Houses, MFCs, MCCs, Credit Union), Leasing Companies, PSP Enhanced, Virtual Asset Service Providers | | Community Banks (RCBs), Digital Credit Service Providers | | Last Mile Providers eg. (Cooperative Susu, Financial Co-operative Societies, MC Ent, FNGOs), FEBs | | PSP Medium, PSPs Standards. PFTSP | |
| | **PARAGRAPH** | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments | Key | Alternative/Comments |
| 105 | Cooling & Environmental Control | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 106 | Fire Protection | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 107 | Cabling & Connectivity | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 108 | Physical Security | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 109 | Segregation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 110 | Monitoring & Incident Response | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 111 | Contracts & SLAs | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 112 | Vulnerability & Maintenance of Facility Systems | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 113 | Colocation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| **PART XIX - CYBERSECURITY REQUIREMENTS FOR ARTIFICIAL INTELLIGENCE (AI) SYSTEMS** | | | | | | | | | | | |
| 114 | General Principles | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 115 | Reporting and Notification | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| **PART XX - CYBER AND INFORMATION SECURITY TESTING AND EXERCISE REGIME** | | | | | | | | | | | |
| 116 | Vulnerability Assessment | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 117 | Configuration Compliance Scanning | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 118 | Patch and Configuration Compliance Validation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 119 | Web Application and API Testing (DAST/SAST) | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 120 | Penetration Testing | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 121 | Red Team Exercises and Adversarial Simulation | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 122 | AI and ML Model-Specific Testing | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 123 | Incident Response Plan Testing and Drills | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 124 | Business Continuity and Disaster Recovery Testing (Including Cloud) | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 125 | Call Centre and Telephony Security Testing | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 126 | User Access Reviews | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 127 | Asset Inventory Review | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 128 | Third-Party Security Assessment | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |
| 129 | Physical Security Control Testing | ✓ | | ✓ | | ✓ | | ✓ | | ✓ | |

| Legend | |
|---|---|
| **Key** | **Description** |
| ✔ | **Full Implementation:** RFI ahall fully comply with all provisions in the paragraph |
| ! | **Partial Implementation:** RFI shall fully comply with the alternative controls or apply for an exemption |
| ✖ | **Not Applicable** |

## ANNEXURE B – MANAGED SECURITY SERVICE PROVIDER GUIDELINES

RFIs that opt to engage a Managed Security Service Provider (MSSP) shall be guided by the MSSP Guidelines in this Directive.

| Category | Criteria / Requirement | Key Reference / Standard |
|---|---|---|
| 1. Legal & Regulatory Compliance | An MSSP shall comply with Ghana's Data Protection Act, 2012 (Act 843). | Data Protection Act, GDPR, ISO/IEC 27001, SOC 2 Type II |
| | An MSSP shall be accredited by Cyber Security Authority (CSA). | |
| | An MSSP shall be registered with the Data Protection Commission. | |
| | An MSSP shall be subjected to independent oversight or audits (SOC 2 Type II, ISO/IEC 27001). | |
| 2. Technical Capability & Expertise | An MSSP may be required to operate a Security Operations Centre (SOC) at all times. | ISO 31000, ISO 22301 |
| | An MSSP may be required to demonstrate experience in cyber and information security operations. | |
| | An MSSP may be required to provide advanced services: Threat Intelligence, SIEM, Network Traffic Analysis, DFIR (Digital Forensics and Incident Response). | |
| | An MSSP may be required to integrate with RFI's existing systems (SIEM, EDR, sensors, etc.). | |
| | An MSSP must maintain business continuity management framework (ISO 22301). | |
| | An MSSP must be certified by Ghana's Cyber Security Authority (CSA). | |
| 3. Security Posture & Certifications | An MSSP must be certified by Ghana's Cyber Security Authority (CSA). | ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, PCI DSS |
| | An MSSP must hold 2 certifications: ISO/IEC 27001, ISO/IEC 27017/27018, SOC 2 Type II. | |
| | An MSSP must maintain tested Incident Response and Business Continuity Plans. | |
| | An MSSP must provide penetration test and security posture reports. | |
| 4. Contractual & Service Level Agreements (SLAs) | An MSSP must define roles/responsibilities (RACI matrix). | ISO/IEC 27036 (Outsourcing Security), BoG Outsourcing Directive |
| | An MSSP must have SLAs which includes but not limited to:<br>→ **Time to Detect**<br>→ **Time to Respond**<br>→ **Escalation** | |
| | An MSSP must ensure data sovereignty, ownership, and destruction procedures. | |
| 5. Reporting & Transparency | An MSSP must provide real-time security dashboards and customised reports for RFI Management, RFI Technical Teams, and RFI Boards. | ISO/IEC 27004 (Metrics & Monitoring) |
| | An MSSP must participate in quarterly and annual reviews. | |

| Category | Criteria / Requirement | Key Reference / Standard |
|---|---|---|
| 6.Governance & Oversight | An MSSP shall report to the CISO of the RFI. | BoG Cyber and Information Security Directive, ISO/IEC 27035 |
| | An MSSP must provide quarterly SLA reviews and annual MSSP reassessments. | |
| | An MSSP must have incident response simulation exercises at least twice in a year. | |
| | An MSSP must share notifications of breaches with the respective entities. | |
| 7. Incident Response & Coordination | An MSSP must align its Incident Response (IR) process with Regulated Financial Institution's plan. | ISO/IEC 27035 (Incident Management) |
| | An MSSP must support containment, investigation, and recovery. | |
| | An MSSP shall be mandated to notify BoG of any major incidents through the RFI. | |
| 8. Business Continuity & Resilience | An MSSP shall maintain a tested Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). | ISO 22301 (Business Continuity) |
| | An MSSP must align with RFI's BCP/DRP and ensure service availability. | |
| 9. Documentation & Record Keeping | An MSSP must keep evidence of due diligence, contracts, risk assessments, incidents and audits. | ISO/IEC 27001 (A.5–A.10 Controls) |
| | An MSSP shall maintain documentation for regulatory inspections. | |

# ANNEXURE C - ENHANCED COMPETENCY FRAMEWORK

## Guide to Enhanced Competency Framework (ECF) on Cyber Security

1. All RFIs are encouraged to use this ECF to raise and maintain professional competence of their cyber and information security practitioners. The framework is not a mandatory licensing regime, however, it is expected that RFIs will adopt it to enable cyber and information security talent and build the professional competencies and capabilities of staff involved in cyber and information security responsibilities.
2. An RFI shall prepare and implement an enhanced cyber and information security competency framework to ensure that cyber and information security personnel meet the specified competency levels. Progress in implementing the ECF shall be considered during The Committee meetings.
3. The ECF is aimed at a new entrant or an existing practitioner engaged by an RFI to perform in roles ensuring operational cyber resilience. For the ECF, RFIs may have key roles based on the three lines of defence concept under cyber risk governance.
4. Employees performing key roles solely in the information technology operating function of the RFI, such as system developers, system operators, helpdesk operators, and IT support are excluded.
5. 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 cyber and information security function.
    b. Professional Level - This level is applicable for staff with 5 and above years of relevant work experience in the cyber and information security function.
6. Cyber and information security professionals, cyber and information security establishments and licensed cyber and information security service providers operating in the financial industry shall obtain certification per sections 57 and 59 of Cyber and Information Security Act, 2020 (Act 1038). Additionally, cyber and information security professionals who operate in the financial industry are also required to obtain accreditation from the Cyber Security Authority.
7. Under the qualification structure, at minimum, the following list of recognised certificates are encouraged:

| RECOGNISED CERTIFICATES | IT Security Operations and Delivery | IT Risk Management and Control | IT Audit |
|---|---|---|---|
| ***Core Level*** | | | |
| CSX Fundamentals Certificate | ✓ | ✓ | ✓ |
| CSX Practitioner Certificate (CSX-P) | ✓ | ✓ | ✓ |
| Cyber and information security Audit Certificate | | ✓ | ✓ |
| GIAC Information Security Professional (GIAC GISP) | ✓ | ✓ | |
| GIAC Security Essentials (GSEC) | ✓ | ✓ | ✓ |
| ISC² Systems Security Certified Practitioner (SSCP) | ✓ | | |

| RECOGNISED CERTIFICATES | IT Security Operations and Delivery | IT Risk Management and Control | IT Audit |
|---|---|---|---|
| ***Core 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) | ✓ | ✓ | |
| Certified Chief Information Security Officer (C\|CISO) | ✓ | ✓ | |
| Certified Ethical Hacker (CEH) | ✓ | ✓ | |
| Computer Hacking and Forensic Investigation (CHFI) | ✓ | ✓ | |
| Lead Information Security Auditor | ✓ | ✓ | ✓ |
| Lead Information Security Implementor | ✓ | ✓ | |

8. Where the qualifications held by staff are different from the qualifications above, the RFI may apply judgement in evaluating such qualifications and see if those qualifications are equivalent qualifications. The RFI 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.
9. Staff who have successfully obtained the qualifications listed under Section 7 should fulfil the Continuing Professional Development (CPD)/Continuing Professional Education (CPE) requirement of the relevant certification scheme.

# ANNEXURE D – SUPPLY CHAIN CYBER RESILIENCE FRAMEWORK

This Annexure serves as the structured and practical implementation guide for paragraph 96 of this Directive. It translates the seven mandatory contractual obligations into actionable tools, including templates, clauses, and checklists, to ensure consistency, enforceability, and regulatory compliance across all RFI third-party engagements.

## 1. Adherence to Security Standards and Directives

Implementation Checklist for RFIs:

a. Verify that the Third Party's certifications (e.g., ISO/IEC 27001) are current and within scope for the services provided.
b. For vendors without formal certification, require a completed Self-Assessment Questionnaire mapping their controls to the NIST Cyber and information security Framework.

As part of the contract:

The supplier must agree that it shall, throughout the terms of the agreement, maintain security controls such as ISO/IEC 27001 or an equivalent standard acceptable by the RFI. The supplier shall provide copies of its certificates and most recent audit reports upon request. Furthermore, the supplier shall comply with all applicable laws and regulations of Ghana as well as Bank of Ghana directives, including any updates thereto, within thirty (30) days.

## 2. Audit and Assessment Rights

Practical Guidance:

a. Tier 1 (Critical) Suppliers: Mandate an independent third-party audit (e.g., SOC 2 Type II or its most recent version) annually, paid for by the supplier.
b. Tier 2 (Medium) Suppliers: RFI-led desk audits or reviews of existing certifications annually.
c. Tier 3 (Low) Suppliers: Self-certification or light-touch questionnaires.

As part of the contract:

The RFI, or its appointed qualified independent third-party, shall have the right to audit the supplier's facilities, systems, and relevant records upon thirty (30) days' notice, or immediately in the event of a security incident. The supplier shall cooperate fully and bear the reasonable costs of such audits where findings reveal material non-compliance. The RFI reserves the right to rely on a SOC 2 Type II or ISO/IEC 27001 audit report from an independent auditor in lieu of conducting its own on-site audit.

## 3. Cyber Incident Notification and Management

Incident Notification Template (To be used by Third Party):

| Field | Instruction |
|---|---|
| Supplier Name | Legal name of the reporting entity. |
| Date & Time of Incident (GMT) | When the incident was first suspected/confirmed. |
| RFI Contact Person | Name and contact details of the supplier's primary contact. |
| Nature of Incident | (e.g., Ransomware, Data Breach, Service Outage, Unauthorised Access). |
| Systems/Data Affected | Specify which RFI systems or data types are potentially impacted. |
| Current Impact | Describe the current operational impact on services provided to the RFI. |
| Actions Taken | Immediate containment or mitigation steps already taken. |
| Expected Time to Next Update | e.g., "Within 2 hours." |

There shall be a requirement for the supplier to notify the RFI's CISO and or designated cyber and information security contact immediately, and in any case no later than one (1) hour, upon becoming aware of any actual or suspected security incident impacting RFI data or services. The initial notification may be verbal or via email and must be followed by a written report using an approved template.

## 4. Cooperation in Incident Response and Forensics

In the unlikely event of an active incident, the supplier shall grant the RFI's incident response team, or its designated third-party forensic investigators, remote or on-site access to relevant systems and logs. The supplier shall provide a designated point of contact to coordinate response activities and shall not destroy any relevant evidence without the prior written consent of the RFI.

## 5. Business Continuity and Disaster Recovery

Minimum BCP/DR Requirements by Tier:

| Tier | Recovery Time Objective (RTO) | Recovery Point Objective (RPO) |
|---|---|---|
| Tier 1 (Critical) | < 4 hours | < 15 minutes |
| Tier 2 (Medium) | < 24 hours | < 4 hours |
| Tier 3 (Low) | < 72 hours | < 24 hours |

The Supplier shall maintain, and test at least annually, a Business Continuity and Disaster Recovery Plan specific to the services provided to the RFI. The plan must meet defined minimum RTO and RPO thresholds defined in the Service Level Agreement. The Supplier shall provide a summary of test results to the RFI upon request."

## 6. Remediation and Termination for Security Failures

Where the supplier fails to remediate a critical security finding identified during an audit within thirty (30) days, or suffers a material breach of security resulting in significant impact to the RFI, the RFI reserves the right to:

a. Suspend the supplier's access to RFI systems until remediation is complete; or
b. Terminate the agreement for cause and invoke the migration and exit plan.

Upon termination, the supplier shall securely transfer all RFI data to the RFI or a new provider within seven (7) days and provide a certificate of data destruction upon completion.

## 7. Subcontractor (Tier-n) Oversight and Flow-Down Clauses

The supplier shall remain fully liable for all acts and omissions of its subcontractors. The supplier warrants that any subcontractor involved in delivering services to the RFI is bound by contractual terms no less protective than those contained in the agreement. The supplier shall maintain an up-to-date list of all subcontractors and provide the RFI with audit rights over critical sub-suppliers upon request.

*Vendor Risk Tiering Matrix*

| Tier | Definition | Data Access | Example Vendors | Due Diligence Level | Monitoring Frequency |
|---|---|---|---|---|---|
| Tier 1 | Critical to daily operations; high impact if unavailable. | Sensitive customer/PII data. | Core Banking Provider, Cloud Hyperscaler, Payment Switch. | Full independent audit (e.g., SOC 2). | Continuous / Quarterly |
| Tier 2 | Important but not immediately critical. | Non-public operational data. | HR Platform, Marketing Agencies. | RFI-led assessment. | Annually |
| Tier 3 | Low impact services. | Public data or no access. | Office Supply, Cleaning Services. | Self-certification. | Upon Renewal |

*Supplier Cyber Risk Register*

| Supplier Name | Tier | Service Provided | Data Classification | Last Assessment Date | Key Findings | Remediation Due Date | Status |
|---|---|---|---|---|---|---|---|
| Example: CloudSys Ltd | 1 | Cloud Hosting | Confidential | 45672 | MFA not enforced on admin accounts | 45703 | In Progress |

# ANNEXURE E – AI/ML GOVERNANCE AND CONTROL GUIDELINES

This Annexure outlines mandatory guidance and expectations for RFIs applying AI and ML systems within their operations, risk management, decision-making processes, or service delivery. It defines the minimum required controls, documentation, and oversight mechanisms required to ensure security, reliability, fairness, explainability, and regulatory compliance throughout the AI/ML models lifecycle.

## 1. Introduction/ Scope

1. This Annex provides the mandatory requirements and control objectives for the governance, risk management, and security of Artificial Intelligence (AI) and Machine Learning (ML) systems used by Regulated Financial Institutions (RFIs).
2. The controls defined herein apply to all AI/ML systems covered under Part XXI, paragraph 118(2), regardless of their development origin or deployment model. The rigor of implementation must be commensurate with the model's risk classification as determined by the RFI's risk assessment.

## 2. Governance, Accountability, and Oversight

a. **AI Governance Committee:** The RFI shall establish a formal AI Governance Committee (or assign these responsibilities to an existing committee, such as the Cyber and Information Security Risk Management Committee) with a defined charter. This Committee shall be responsible for:
   i. Approving the institution's AI/ML strategy and risk appetite;
   ii. Overseeing the AI/ML risk management framework;
   iii. Reviewing and approving high-risk AI/ML models before deployment; and
   iv. Ensuring appropriate resources, skills, and training are available for AI/ML governance.

b. **Roles and Responsibilities:** The RFI shall clearly define and document the roles and responsibilities for all parties involved in the AI/ML lifecycle, including model developers, data scientists, risk managers, the CISO, the DPO, and internal audit.

c. **Board-Level Oversight:** The Board of Directors (or its designated Committee) shall receive and review regular reports on the performance, risks, and incidents related to the institution's AI/ML systems at least annually.

d. **AI Inventory:** The RFI shall maintain a comprehensive, up-to-date inventory of all AI/ML models in use, development, or pilot, including metadata such as model owner, version, purpose, data sources, risk rating, and deployment status.

e. **AI/ML Risk Management**
   i. ***Risk Identification:*** The RFI's enterprise risk management framework shall explicitly include AI/ML-specific risks. At a minimum, the following risk categories must be assessed:
      1. Adversarial Threats: Risks from data poisoning, model evasion, model inversion, and extraction attacks.
      2. Model Integrity: Risks from model drift, concept shift, performance degradation, and cascading failures due to interconnected models.
      3. Fairness and Ethics: Risks of bias, discrimination, and unfair outcomes based on protected or proxy attributes.
      4. Explainability and Transparency: Risks arising from the inability to interpret or justify model decisions ("black box" risk).
      5. Regulatory and Legal: Risks of non-compliance with data protection, consumer protection, and financial services laws.
      6. Dependency Risk: Risks associated with third-party AI models, including lack of transparency and vendor lock-in.
   ii. ***Risk Assessment:*** A formal AI/ML risk assessment shall be conducted prior to the deployment

of any new model and at least annually thereafter. The assessment must be documented and approved by the AI Governance Committee.

f. Data Management for AI/ML
   i. Data Lineage and Provenance: The RFI must document the source, ownership, and all transformations applied to data used for training, validation, and testing of AI/ML models to ensure traceability and auditability.
   ii. Data Quality: Processes shall be implemented to ensure that data used for AI/ML is accurate, complete, and representative of the intended use case. Data quality metrics must be defined and monitored.
   iii. Privacy Safeguards: The RFI shall implement privacy-preserving techniques, including anonymisation, pseudonymisation, and differential privacy, where personal data is used, in full compliance with the Data Protection Act, 2012 (Act 843). Re-identification of anonymised data must be strictly prohibited and technically prevented.

g. Model Lifecycle Management
   i. Design and Development: AI/ML systems shall be developed following a secure development lifecycle that incorporates security and privacy by design principles. This includes secure coding practices, code reviews, and the removal of features that could introduce bias or leak sensitive data.
   ii. Versioning and Change Management: Strict version control and change management processes must be in place for all AI/ML models. All changes, including retraining events, parameter adjustments, and code updates, must be documented, approved, and auditable.
   iii. Testing and Validation: Prior to deployment, all AI/ML models must undergo rigorous testing, including:
      1. Functional and performance testing against defined business requirements;
      2. Adversarial testing to evaluate resilience against manipulation;
      3. Fairness testing to detect and measure bias across relevant demographic groups; and
      4. Back-testing using historical data to validate predictive accuracy and financial impact.
   iv. Independent Validation: High-risk AI/ML models must be subject to independent validation by a function or party not involved in their development. Validation reports must be reviewed and approved by the AI Governance Committee before deployment.

h. Security Hardening and Robustness
   i. Adversarial Defence: The RFI shall implement controls to protect AI/ML models from adversarial attacks. This includes input sanitisation, adversarial training, and monitoring for anomalous queries or data manipulation attempts.
   ii. Protection of Model Artifacts: Model weights, parameters, and training data shall be treated as critical information assets. They must be encrypted at rest and in transit, and access shall be restricted based on the principle of least privilege, enforced with multi-factor authentication.
   iii. Robustness Testing: Models shall be regularly stress-tested under scenarios involving data perturbations, missing inputs, or simulated attacks to ensure they behave reliably and safely under adverse conditions.

i. Third-Party and Vendor AI Models
   i. Vendor Due Diligence: Before procuring or integrating any third-party AI/ML system, the RFI shall conduct a comprehensive due diligence assessment of the vendor's AI governance, security practices, data handling procedures, and model transparency.
   ii. Contractual Requirements: Contracts with AI/ML vendors must explicitly include:
      1. The right for the RFI and the Bank of Ghana to audit the vendor's controls, model development processes, and relevant documentation;
      2. Clear definitions of model ownership, intellectual property, and liability for errors, bias, or security breaches;

3. Performance guarantees and SLAs covering model accuracy, fairness, and availability; and
4. The RFI's right to independently validate, retrain, or replace the vendor's model.

iii. Ongoing Oversight: The RFI shall maintain ongoing oversight of third-party AI models, including regular reviews of vendor-provided reports and independent monitoring of model performance.

j. Interpretability, Explainability, and Audit
   i. Minimum Explainability: RFIs must ensure that decisions generated by AI/ML systems that materially affect customers can be explained in a clear, meaningful, and justifiable manner. For complex models, this shall be achieved through the use of post-hoc explainability techniques (e.g., SHAP, LIME) to identify key influencing variables.
   ii. Comprehensive Logging: AI/ML systems must be configured to generate tamper-proof logs that record, at a minimum:
      1. Model inputs and outputs for all significant transactions or decisions;
      2. Version identifiers and timestamps for the model used;
      3. Any manual overrides and the rationale for them; and
      4. Events indicating model drift, retraining, or performance alerts.
   iii. Audit Trails: Logs and audit trails must be retained securely for a minimum period of seven (7) years, or longer if required by other regulations, and must be readily accessible for regulatory inspection and forensic investigation.

k. Operational Resilience and Contingency Planning
   i. Backup and Failover: For critical AI/ML systems, the RFI shall maintain documented and tested backup, failover, and fallback procedures. This includes the ability to quickly switch to a secondary model or a manual, rule-based process if the primary AI system fails or produces unreliable outputs.
   ii. Kill-Switch Capability: The RFI shall implement a technical capability ("kill-switch") to immediately halt the operation of an AI/ML system if it is found to be malfunctioning, compromised, or producing demonstrably harmful outcomes.
   iii. AI-Specific Incident Response: The RFI's incident response plan shall be updated to include specific procedures for AI/ML-related incidents, such as data poisoning attacks, model drift leading to widespread errors, or adversarial manipulation.

l. Ethics, Fairness, and Regulatory Compliance
   i. Bias Mitigation: The RFI shall proactively implement processes to detect, measure, and mitigate bias in AI/ML models. Fairness metrics must be defined, monitored, and reported to the AI Governance Committee. If material bias is detected, the model's use must be suspended until effective mitigation is applied.
   ii. Customer Recourse: The RFI must establish and communicate clear mechanisms for customers to seek recourse and appeal decisions that were made or significantly informed by an AI/ML system.
   iii. Compliance: The RFI shall demonstrate, through its documentation and controls, that all AI/ML systems are in full compliance with the Data Protection Act (Act 843), applicable consumer protection laws, anti-discrimination legislation, and all relevant provisions of this Directive.

# ANNEXURE F – CLOUD SECURITY STANDARDS, CONTROLS AND BENCHMARKING

This Annexure offers guidance and minimum expectations for RFIs using cloud services in line with the BoG's cyber and information security and operational resilience standards. It provides definitions, control frameworks, and standard templates to support secure, compliant, and resilient deployment of cloud resources across Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models.

This Annexure serves as a reference for RFIs; compliance with its provisions indicates adherence to the BoG's cyber and information security standards for cloud adoption, governance, and oversight.
Key sources include:

- ENISA (2021) Cloud Security for Financial Institutions
- ISO/IEC 19941:2017 Information technology — Cloud computing — Interoperability and portability
- ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- ISO/IEC 27018:2019 - Protection of personally identifiable information (PII) in public clouds.
- ISO/IEC 22123-1 - Information technology — Cloud computing — Part 1: Vocabulary
- ISO/IEC TS 23167 - Information technology - Cloud computing - Common technologies and techniques
- NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organisations.
- NIST SP 800-144 — Guidelines on Security and Privacy in Public Cloud Computing
- NIST SP 800-145 - The NIST Definition of Cloud Computing
- NIST SP 500-292 - NIST Cloud Computing Reference Architecture.
  Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v4.0.

## 1. Definition and Terminology

To ensure consistency across RFIs, cloud service providers (CSPs), and auditors, the following definitions apply:

| Term | Definition (aligned with ISO/NIST/CSA) |
|---|---|
| Cloud computing | A model enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications) that can be rapidly provisioned and released with minimal management effort (NIST SP 800-145). |
| IaaS (Infrastructure-as-a-Service) | A cloud service model that offers virtualised computing resources, including servers, storage, and networking, where the consumer controls the operating systems and applications (NIST SP 800-145). |
| PaaS (Platform-as-a-Service) | A service model providing runtime environments and development tools managed by the CSP, enabling consumers to deploy applications without managing infrastructure (NIST SP 800-145). |
| SaaS (Software-as-a-Service) | A model delivering software applications over the internet, managed entirely by the CSP, where the consumer controls only configuration settings (NIST SP 800-145). |
| Shared Responsibility Model | A security and compliance framework dividing control and accountability between the CSP and the customer, as outlined in ISO/IEC 27017. |
| Multi-tenancy | An architectural feature where multiple customers share the same computing resources, isolated logically but not necessarily physically (ISO/IEC 27017). |
| Tenant Isolation | Security mechanisms ensure that one tenant's data, processes, and operations are segregated and protected from other tenants (ISO/IEC 27017). |
| Hypervisor | Software that creates and manages virtual machines (VMs) by abstracting physical hardware resources (ISO/IEC 22123). |
| Containerisation | Lightweight virtualisation enables applications to run in isolated environments that share the same kernel. |

| | |
|---|---|
| Serverless Computing | A cloud model in which the CSP dynamically manages the allocation of machine resources, executing code in response to events (NIST SP 500-322). |
| API Gateway | A managed service that acts as a single-entry point for APIs, handling authentication, routing, throttling, and logging (ISO/IEC TS 23167, NIST SP 800-228, NIST SP 800-207A). |
| Data Sovereignty | The concept that digital information is subject to the laws of the country in which it is located. |
| Portability and Interoperability | The ability to migrate data or services between CSPs or on-premises environments without vendor lock-in, as per ISO/IEC 19941. |

## 2. Cloud Readiness Assessment Checklist

Before engaging in any CSP, the RFI must complete a formal Cloud Readiness Assessment covering the following areas:

1. **Governance and Strategy**
    a. Cloud strategy alignment - Verify that the proposed cloud usage aligns with the institution's ICT, risk, and outsourcing strategies.
    b. Shared responsibility model - Clearly document delineation of responsibilities between the CSP and RFI for security, privacy, and compliance obligations.
    c. Third-party management - Ensure CSPs are included in the RFI's vendor risk management framework, following ISO/IEC 27036 and BoG outsourcing directives.
2. **Regulatory and Compliance Alignment**
    a. Jurisdiction and data residency - Verify that data storage and processing adhere to Ghanaian data protection and financial sector regulations, including approvals for cross-border transfers.
    b. Regulatory access - Ensure the Bank of Ghana and other authorised authorities have the right to access relevant data, audit reports, and premises if necessary.
    c. Certification and assurance - Verify current certifications (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II, CSA STAR, PCI DSS, where applicable).
    d. Legal review - Perform legal due diligence on contractual clauses, SLAs, and applicable governing laws.
3. **Security and Risk Management**
    a. Access control and IAM - Assess CSP capabilities for identity federation, MFA enforcement, least privilege, and role-based access.
    b. Encryption - Verify encryption at rest, in transit, and key management ownership (BYOK, HYOK options).
    c. Network and perimeter security - Assess segmentation, DDoS mitigation, and secure connectivity options (VPN/private link).
    d. Vulnerability and patch management - Verify consistent patching, setup standards, and RFI notification procedures.
    e. Logging and monitoring - Ensure the CSP includes audit logging, SIEM integration, and event retention features.
    f. Data classification and lifecycle - Confirm data classification, retention, deletion, and secure disposal procedures.
4. **Operational Resilience and Incident Response**
    a. Business continuity and DR - Validate the CSP's BCP/DR plans, backup frequency, RTO/RPO, and geographic distribution redundancy.
    b. Incident management - Define the escalation matrix, notification timelines (e.g., within 24 hours of breach), and access to forensic data.
    c. Service-level management - Review uptime commitments, monitoring transparency, and penalty clauses for SLA violations.

5. **Audit, Oversight, and Transparency**
    a. Right to audit - Confirm the contractual right for BoG and/or RFI-appointed auditors to review controls, processes, and facilities.
    b. Independent assurance - Require annual independent assurance reports (SOC 2 Type II, ISO surveillance audits).
    c. Continuous monitoring - Ensure the RFI maintains ongoing oversight and control validation processes.
6. **Portability, Interoperability, and Exit Readiness**
    a. Exit strategy - Outline exit procedures, notice periods, and handover schedules.
    b. Data portability - Verify data extraction tools, supported formats, and completeness assurances.
    c. Data deletion verification - Ensure CSP provides verifiable certificates for deletion and sanitisation.
    d. Dependency risk assessment - Evaluate risks associated with vendor lock-in and the feasibility of migration.
7. **Advanced and Emerging Considerations (Optional)**
    a. Cloud-native security posture management (CSPM/CWPP) - Assess the use of continuous compliance monitoring tools.
    b. AI/ML workload protection - Assess CSP's governance regarding AI model data, training pipelines, and bias control (if applicable).
    c. Zero Trust and Confidential Computing readiness - Assess support for confidential VMs, secure enclaves, and ongoing authentication.

## 3. Shared Responsibility Matrix

A shared responsibility matrix specifies which party (CSP or RFI) is responsible for each security domain. This clarity helps prevent gaps or overlaps in implementing controls. An example is provided below for clarity (based on ISO/IEC 27017, CSA CCM v4.0, NIST SP 800-53).

| Control Domain | CSP Responsibility | Shared | RFI Responsibility |
|---|---|---|---|
| Physical security | √ | | |
| Hypervisor patching and maintenance | √ | | |
| Network segmentation and perimeter defense | | √ | |
| Identity and Access Management (IAM) | | √ | √ |
| Application security and logic validation | | | √ |
| Encryption (at rest/in transit) | √ (infrastructure level) | √ (key management) | √ (application level) |
| Monitoring and logging | | √ | √ |
| Incident response coordination | | √ | √ |
| Compliance with local data laws | | √ | √ |

## 4. Migration and Exit Plan

RFIs shall maintain a documented migration and exit strategy that ensures business continuity and data control. This includes but is not limited to the following:

### 1. Data Extraction Procedures

This subsection outlines the methods, tools, and governance mechanisms that enable an RFI to securely and efficiently extract its data from a third-party or CSP during migration or exit. The procedures must guarantee the completeness, integrity, and confidentiality of the extracted data throughout the process. RFIs are expected to:

a. Define standardised extraction formats (e.g., CSV, JSON, XML, or other interoperable structures) that preserve metadata, timestamps, and data lineage.
b. Set up secure transfer methods (e.g., encrypted channels, verified delivery) to prevent data loss or unauthorised access.
c. Verify data accuracy using checksum validation, reconciliation reports, audit trails, or other integrity check methods.
d. Demand that the provider facilitate prompt and comprehensive data export without unnecessary delay or reliance on proprietary systems.
e. Outline roles, responsibilities, and approval processes for initiating and validating data extraction.

The procedures should be tested regularly as part of exit-plan drills to ensure operational readiness and compliance with data protection, privacy, and business continuity obligations.

### 2. Rollback and Fallback Strategies

Rollback and fallback strategies outline how a financial institution can safely revert to a previous system state or switch to an alternative processing environment if a migration or deployment fails or poses unacceptable risks. These strategies maintain operational continuity and data integrity during migration to or from cloud or on-premises environments.

***A rollback strategy*** involves restoring systems, configurations, and data to their most recent stable version using verified backups or snapshots to undo failed migrations or updates. It requires version control, automated restore processes, and pre-verified rollback checkpoints.

***A fallback strategy*** provides alternative operational options when rollback isn't possible, such as switching to a replicated environment, a disaster recovery site, or a manual processing mode, to maintain critical business functions during remediation.
The RFIs are expected to:

a. Document, test, and regularly validate both rollback and fallback procedures as part of their migration and exit plans, ensuring they are aligned with business continuity and incident response frameworks, and coordinated with third-party service providers where applicable.

### 3. Staging and Testing

Before any production migration or system exit occurs, the RFIs are expected to:

a. Conduct a staging and testing phase to verify all technical, operational, and security aspects of the planned transition. This phase confirms that migration procedures, rollback plans, and exit strategies function as intended, without disrupting business continuity or compromising data integrity.
b. Establish a staging environment that closely resembles the production setup, including infrastructure, connectivity, access controls, and data handling configurations, to conduct thorough testing of migration tools, data transfer processes, and application performance. Security and resilience

assessments, such as penetration testing and failover simulations, must also be performed to ensure that systems comply with regulatory, contractual, and security standards after migration.

c. Comprehensive documentation of test cases, results, deviations, and corrective actions shall be maintained, and a final go-live decision should only be approved once all acceptance criteria have been met and independently validated by relevant assurance functions (e.g., risk, compliance, or internal audit).

**4. Contractual Exit Rights**

Contractual exit rights ensure that the RFI maintains the legal and operational ability to disengage from a CSP or third-party arrangement in a controlled and secure manner. The RFIs are expected to establish a contract that:

a. Clearly specify the RFI's rights to terminate the agreement, whether due to performance issues, security breaches or violations, regulatory non-compliance, or strategic reasons, without causing unnecessary disruption to critical services or data integrity of the RFI.
b. Such provisions should include clear terms for data retrieval, deletion, and secure transfer to alternative environments, as well as ongoing support from the provider during the transition period.
c. The clause should also require the provider to cooperate fully during offboarding, ensure service continuity for a specified period, and avoid imposing excessive termination fees or technical charges barriers.
d. These rights are essential for maintaining operational resilience, regulatory compliance, and data sovereignty in accordance with the BoG expectations for prudent cloud and outsourcing governance.

**5. Source Deletion**

After completing a cloud or service migration, or upon contract termination, RFIs are expected to:

a. Ensure thorough and verifiable removal of its data, code, configurations, parameters, and backups from the provider's environment.
b. Performing a secure and irreversible removal of all copies of institutional data, including primary sources, replicas, and cached instances, in accordance with data retention and destruction policies, i.e., source deletion.
c. The RFI should specify that the service provider must:
    i. Apply certified data erasure methods (e.g., NIST SP 800-88 Rev. 1 or ISO/IEC 27040).
    ii. Provide written attestation or audit evidence confirming deletion.
    iii. Ensure deletion extends across production, backup, and disaster - recovery sites.

This control prevents the exposure of residual data after migration or contract termination, ensuring compliance with confidentiality, privacy, and data minimisation requirements under the BoG framework.

# ANNEXURE G – PRIVACY AND DATA PROTECTION CONTROLS

## Privacy and Data Protection Controls

### 1. Introduction

This Annexure outlines the framework and mandatory controls for RFIs to ensure the protection, lawful processing, and confidentiality of personal and institutional data, in line with the Data Protection Act, 2012 (Act 843), and applicable BoG directives.

### 2. Regulatory Alignment

a. Ghana Data Protection Act, 2012 (Act 843)
b. NIST SP 800-53 Rev. 5, Appendix J (Privacy Controls)
c. ISO/IEC 27701:2025 (Privacy Information Management)
d. OECD Privacy Guidelines (2023 revision)

### 3. Core Principles and Controls

a. Lawful and Fair Processing: Data shall be processed legally, fairly, and transparently, with clear communication to the data subject.
b. Purpose Limitation: Data shall be collected for specific, explicit, and legitimate purposes and not processed further in ways incompatible with those purposes.
c. Data Minimisation: Only the essential data required for the specific business purpose shall be collected.
d. Accuracy: RFIs shall take reasonable steps to ensure that personal data is accurate and current.
e. Storage Limitation: Data shall not be kept longer than necessary for its lawful purpose.
f. Integrity and Confidentiality: RFIs shall secure data through encryption, access control, and continuous monitoring to prevent loss, unauthorised access, or disclosure.
g. Data Subject Rights: RFIs shall establish mechanisms to enable access, correction, erasure, restriction, portability, and objection rights for data subjects.
h. Third-Party Data Sharing: No personal data shall be shared externally without documented consent and assurance of equivalent protection.
i. Cross-Border Transfers: Data transfers outside Ghana must only happen with proper safeguards and approval from the BoG.
j. Breach Notification: RFIs must notify the BoG and the Data Protection Commission within the required timeframe after a privacy or data protection incident.

### 4. Governance and Oversight

The Board and Senior Management shall consider data privacy a key risk area within the RFI's cyber and information security and operational resilience frameworks. The DPO will work with the CISO to incorporate privacy controls into the broader cyber and information security programme.

### 5. Privacy Audit and Reporting

Each RFI shall conduct an annual privacy audit to evaluate compliance with Act 843 and this Directive. The results shall be documented and made accessible to the Bank of Ghana and the Data Protection Commission upon request.

## ANNEXURE H – TESTING FREQUENCY

This Annexure outlines the minimum requirements for key cyber and information security tests and reviews to ensure controls remain effective and risks are proactively managed across all RFIs.

| Component | Tier 1 & 2 RFI | Tier 3 RFI | Tier 4 & 5 RFI |
|---|---|---|---|
| Vulnerability Assessment | Monthly automated scanning with quarterly manual validation | Quarterly automated scanning with semi-annual manual validation | Semi-annual automated scanning |
| Web Application Testing (DAST/SAST) | Continuous for critical applications; quarterly for others | Quarterly for critical applications; semi-annual for others | Semi-annual for all applications |
| Penetration Testing (Network and Application) | Bi-annually (internal and external) | Annually (internal and external) | Annually (external only) |
| Red Team or Adversary Simulation Exercise | Annually | Every 2 years | Every 3 years or as directed |
| Control Effectiveness and Configuration Review | Semi-annually | Annually | Annually |
| Third-Party Security Assessment | Annually for critical vendors | Annually for critical vendors | Biennially for key vendors |
| Patch and Configuration Compliance Validation | Monthly review cycles | Quarterly review cycles | Semi-annual review cycles |
| Configuration Compliance Scanning (CIS/NIST aligned) | Quarterly review cycles | Quarterly review cycles | Quarterly review cycles |
| Disaster Recovery / Failover Testing | Annually | Annually | Annually |
| User Access Review (Critical Systems) | At least twice a year | At least twice a year | At least twice a year |
| Asset Register Review | Annually | Annually | Annually |

Designed by Communications Department
Bank of Ghana