The Sierra Leone Gazette

(Extraordinary)

Published by Authority

Vol. CXLXII | FRIDAY 31ST DECEMBER, 2021 | No. 80

FREETOWN. 31st December, 2021

Govt. Notice No. 429

BANK OF SIERRA LEONE CYBER SECURITY

AND

IT RISK MANAGEMENT GUIDELINES FOR COMMERCIAL BANKS

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTING DEPARTMENT, SIERRA LEONE
Annual Subscription:–Inland–Le350,000.00, Overseas–Le2,750,000.00
To be purchased from the Government Bookshop, Wallace Johnson Street, Freetown. Price:–Le5,000.00G.P. O/208/21/700/1.21.

TABLE OF CONTENTS

Section One

SECTION ONE

1.0 INTRODUCTION

These Guidelines are developed to ensure the benefits derived from technological inventions can be fully enhanced without conceding financial stability, consumer protection and cyber resilience. It provides a risk-based methodology for managing Cyber and Information Technology risks. This document comprises nine Sections:

* Introduction, objective, scope and compliance, authority, applicability, review and commitments of Commercial Banks
* Cyber and Information Technology Security Governance and Oversight
* Cyber and Information Technology Security Risk Management System
* Cyber and Information Technology Controls
* Cyber and Information Technology Defense
* Cyber and Information Technology Response and Recovery
* Cyber Threat Intelligence
* Information Sharing and Collaboration
* Monitoring and Reporting to the Bank of Sierra Leone

1.1 OBJECTIVE

(a) In line with the growing technology innovation usage, reliance on a dynamic operating and cyber threat environment, commercial banks shall establish robust and effective Information technology risk management processes, governance structures and cyber security controls.

(b) The specific objectives of these Guidelines are listed below:

i. To establish an effective mechanism that can identify, measure, monitor, and control the risks of Commercial Banks information system, ensure data integrity, availability, confidentiality and consistency,

ii. Provide the relevant early warnings, thereby enabling Commercial Banks to improve their competency in utilizing information technology to promote financial system stability.

iii. Build a safe surrounding within the data superhighway (cyber space) for the financial services industry and create adequate trust and confidence in Information systems as well as transactions in the cyber space.

iv. Solidifying the Regulatory framework to ensure a secure environment within cyberspace.

v. Continuous enhancement of cyber and information security risk assessments.

vi. Improving Commercial Banks core competitiveness and capacity for sustainable development.

vii. To foster cross border cooperation and consistency in regulatory and supervisory approaches in order to enhance cyber and operational resilience in Commercial Banks.

viii. Enhance Cyber Security Information Sharing among Commercial Banks that will help to defend Commercial Banks against emerging cyber threats.

ix. Preservation of Public Confidence in the financial system

1.2 SCOPE AND COMPLIANCE

i. These Guidelines set the minimum standards that Commercial banks shall adopt in order to develop effective Cyber Security Governance and Information Technology Risk management frameworks.

ii. All Commercial Banks licensed by the Bank of Sierra Leone shall comply with these Guidelines.

iii. Noncompliance shall attract the appropriate penalties and sanctions from the Bank of Sierra Leone

1.3 AUTHORITY

These Guidelines on Cyber Security and the Risk Management of Commercial Banks Information Technology are developed in accordance with Section 53 (1) of the Banking Act 2019, which empowers the Bank of Sierra Leone to issue Directives and Guidelines.

1.4 APPLICABILITY

These Guidelines apply to all Commercial Banks licensed under Section eight (8) of the Banking Act 2019.

1.5 REVIEW OF THE CYBER SECURITY AND INFORMATION TECHNOLOGY RISK MANAGEMENT GUIDELINES

This document shall be reviewed annually or when significant changes occurs within the cyber and Information Technology realm to ensure its continuing, suitability, adequacy and effectiveness.

1.6 Commercial Banks regulated by the Bank of Sierra Leone shall comply with the following:

1. Place distinctive importance on cyber and information security and take all necessary steps to safeguard and manage their systems and data well.

   Commercial banks shall, recruit or appoint a Chief Information Security Officer.

   He/she shall report to the Board and copy the CEO. Foreign Subsidiaries can use CISO of their parent/group for a period of twenty four (24) months to enable them develop local capacity.

2. All Commercial Banks shall establish a Cyber and Information Systems Security function headed by a Chief Information Security Officer.

3. The Cyber Security Policy and Strategy shall be separated from the broader IT Policy and Strategy of the Commercial Banks.

6. Individuals hired as IT Risk Manager shall have the required IT skill set.

   All Commercial banks shall establish a Cyber and Information Security Steering Committee chaired by the Chief Information Security Officer.

   All Commercial banks shall put in place a Cyber Incidence Response Team (this team shall also serve as members of Inter- Financial Institution Cyber Incidence Response Team) to enable information sharing and collaboration amongst Commercial Banks in fighting Cyber Crime.

Commercial Banks shall ensure that resources are dedicated towards developing their cyber and information security skills.

All Commercial banks shall have a Cyber-Crisis Management Plan (CCMP) to improve the institution's cyber resilience to operational disruptions due to the dynamic nature of cyber risks.

7. The CCMP shall address protection, detection, response and recovery as the traditional Business Contingency Plan and Disaster Recovery arrangements may not be adequate and hence may need to be revisited keeping in view the dynamic of the cyber risks, to reduce damage to its Information Technology assets and customers information.

8. Commercial Banks shall manage their cyber and information security risks subject to Guidelines pertaining to operational risks, business continuity, and Information Technology Management.

9. In managing operational risks, the bank shall report and document all cyber and information risks pertinent to its operations as well as the measures taken to mitigate them.

14. Commercial Banks shall address all cyber and information security matters which may affect its own activities and those of customers, suppliers and service providers.

15. Understand the scope of cyber and information security threats and assess the security skills required for meeting this challenge.

16. All licensed Commercial Banks supervised by the Bank of Sierra Leone shall implement international best practice and technical standards such as ISO, COBIT and NIST etc.

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

18. Commercial Banks that handle, process, store or transmit debit card, credit card, prepaid card, e-purse, ATM cards and /or POS and related Information shall be PCI-DSS certified.

19. Commercial banks shall conduct regular reviews of the operating environment with a view to identifying new emerging cyber and information security threats.

20. Reports of such review shall be produced and filed with the Bank of Sierra Leone.

1.7 IMPLEMENTATION/TRANSITIONAL PERIOD

Commercial banks shall have 180 days from the effective date of these Guidelines to comply with the requirements set forth herein.

SECTION 2

2.0 CYBER AND INFORMATION TECHNOLOGY SECURITY GOVERNANCE

2.1 Responsibilities of Board of Directors

The Board of Directors of a regulated commercial bank shall have the following responsibilities with respect to the management of information systems:

1. The Board shall be responsible for all IT and cyber strategies, cyber and information security risk management framework and policies.

2. Specifically, the board shall approve cyber and IT risk management strategies and policies, understand the major IT risks involved, set acceptable levels for these risks, and ensure the implementation of the measures necessary to identify, measure, monitor and control these risks.

3. Approve policies on outsourcing, backup and recovery from cyber-attacks and disaster management events.

4. Approve the annual and other work plans relating to cyber and information security, business continuity and disaster recovery.

5. Establish a culture within the bank that emphasizes and demonstrates to all levels of personnel the importance of cyber and IT risk management.

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

7. Establish a Cyber and Information Security steering committee, with a well-defined charter.

8. Appoint a Board Sub-Committee on Cyber and Information security risks and counter measures with a clear Charter.

9. Receive quarterly and or immediate reports about important cyber and information security incidents.

10. Dedicate at least two meetings each year to cyber and information security risks and countermeasures.

11. Review the adequacy of cyber and information security policies and strategies.

12. Extend support towards inter-institutional collaboration on cyber and information security defense

13. Implement and comply with the regulations and technical standards pertaining to the management of information systems.

14. Establish cyber and IT governance structure, proper segregation of duty, clear role and responsibility, maintain checks and balances and clear reporting relationship.

15. Build and strengthen the capacity of IT professional staff by developing an incentive program.

16. Submit an annual report to the Bank of Sierra Leone on cyber and information system risk management that has been reviewed and approved by the Board of Directors.

17. Report in a timely manner to the Bank of Sierra Leone any serious incident relating to information systems or any unexpected event, and quickly respond to it in accordance with the contingency plan.

18. Cooperate with the Bank of Sierra Leone in the supervisory Examination of the risk management of information systems and ensure that supervisory opinions are followed up.

2.2 RESPONSIBILITIES OF SENIOR MANAGEMENT

The Senior Management's duties are listed below:

1. Formulate Cyber and IT Strategies which aligns with the overall business plan of the bank.

2. Develop an institutional framework for Cyber and Information Security Risk Management and oversee its implementation and maintenance.

3. Develop institutional policies on cyber and information security, outsourcing, backup and recovery from cyber incidents and disaster events.

4. Senior Management shall decide as to whether the policies referred to in (3) above should be revised yearly.

5. Allocate the necessary resources towards the institutional cyber and information security framework and policies.

6. Hold meetings twice-a-year to monitor and control the implementation and effectiveness of the institution's cyber and information security activities and measures.

7. Obtain quarterly and ad-hoc reports, as required, about cyber and information security threats and countermeasures with reference to the risk estimate stipulated in this guideline.

8. Collect and discuss monthly reports on significant cyber and information security incidents and analyze their corporate implications.

9. Select the types of cyber and information security incidents necessitating immediate attention of Senior Management.

10. Ensure that the Cyber and Information Security Steering Committee is chaired by the Chief Information Security Officer.

11. Immediately report to the Board any important violation(s) of cyber and information security which may occur.

12. Promote inter-institutional collaboration on cyber and information security defense.

13. Report all major and suspected cyber and information security incidents to the Bank of Sierra Leone.

14. Senior Management shall fully understand risks related with Information Technology Outsourcing. Due diligence reports shall be prepared before a service provider is appointed.

15. Collaborate with other Commercial Banks to share information on the latest cyber threats/attacks encountered by the institution.

2.3 RESPONSIBILITIES OF INTERNAL AUDIT

1. Commercial Banks shall establish a special Cyber and IT Security audit role, within the Internal Audit function, which should put in place IT audit policies and procedures, develop and execute IT Audit Plan.

2. The unit shall be responsible for auditing Information Technology, Cyber and Information Security.

3. The Senior Management shall deploy the necessary resources for implementing the auditing processes, and to ensure that adequate training is provided for the unit to increase its capabilities.

4. All aspects of cyber and information security management shall be audited at least once yearly or in line with the risk-based audit approach of the bank.

5. The IT auditor shall review the institution's, backup and recovery processes at least once a year.

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

7. The Board and Senior Management shall deliberate the Cyber and IT Audit Reports.

8. Whenever internal cyber and information security audits make use of outsourcing services, evaluation of audit findings shall remain the exclusive purview of the bank's internal audit unit.

9. The Internal Audit should establish follow-up process for tracking and monitoring cyber and information security audit recommendations.

2.4 COMPLIANCE FUNCTION

This shall be the responsibility of the Compliance Manager who shall ensure that:

1. The bank's complies with IT security issues.

2. The bank is compliant with its own Cyber Security and IT Risk Management Policies, and the Bank of Sierra Leone Cyber Security and Information Technology. Risk Management Guildelines for Commercial Banks.

3. The bank's Cyber Security and or IT Risk Management Policies are in line with best practices and applicable international standards.

4. The relevant Cyber and IT Risk Management compliance information are provided to Board and Management.

5. Monitoring changes in cyber laws and regulations and ensuring bank's compliance

6. Prepare quarterly reports on cyber and information Technology compliance issues which should be submitted to the Board.

2.5 RISK MANAGEMENT CONTROL FUNCTIONS

Commercial banks shall designate a specific individual for Cyber Security and IT Risk Management. He/she shall

1. Reports directly to the Chief Information Security Officer and copying the Head Risk Management, and Enterprise Risk Management committee.

2. Serves as a member of the Cyber Security incident response team.

3. coordinating the establishment of policies regarding Cyber and IT risk management, especially the areas of information security

4. Maintain comprehensive cyber risk registers.

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

6. List of servers, functions and operating systems installed on them.

7. Network inventory (switches, routers, modem, hub, bridges, gateway, firewall, repeater etc.

8. Network topology diagram.

9. A list of computer inventory, owners and the operating system installed on them.

10. Accountable for ensuring that cyber and IT security risks within the institution are identify, analyze, control, monitor and escalated to Chief information security Officer.

2.6 APPOINTMENT OF CHIEF INFORMATION SECURITY OFFICER

The Board of Directors of commercial banks shall appoint or designate a qualified individual as the Chief Information Security Officer (CISO) who should report directly to the CEO and copy the Board. The CISO shall possess a master's in Information Technology and any form of certification in Cyber/Information Security.

Roles and responsibilities of the CISO shall include the following:

1. Playing a direct role in key decisions for the business development involving the use of IT in the bank.

2. Guide the Senior Management and Board on cyber and Information Security Management.

3. Formulate an approach for managing cyber and information security risks.

4. Develop the bank's Cyber and Information Security Policies and submit it to Senior Management and Board for approval.

5. The CISO shall ensure that information systems meet the needs of the bank, and IT strategies are in line with the overall business strategies.

6. Responsible for the bank's Information Security.

7. Supervising and implementing the institutional cyber related programme and enforcing cyber security policies.

8. Draw up annual work plan, including budget for cyber and IT security.

9. Designing cyber security controls for management staff, contractors, consultants, business partners and service providers.

10. Ensuing that adequate processes are in place for monitoring IT systems to detect cyber security events and incidents in a timely manner.

11. Reporting to the Board on a quarterly basis detailed exception to the approved cyber security policies and procedures, all substantial cyber security events that affected the bank during the period and the budget required to enhance cyber defenses.

12. Ensure timely update of the incidence response mechanism and business contingency plan based on the latest cyber threat intelligence gathered.

13. Ensure frequent data backups of changes made to critical IT systems are carried out to a separate storage location.

14. Ensure the roles and responsibilities of managing cyber risks including in emergency or crisis are clearly defined, documented and communicated to the relevant staff.

15. Continuous testing of disaster recovery and business contingency arrangement to ensure that Commercial Banks can continue to function and meet its regulatory obligations in the event of an unforeseen attack through cyber-crime.

16. Organizing cyber and professional Information Technology trainings to improve its technical proficiency of staff.

17. Promote cyber and information security awareness and training of suppliers, service providers and customers.

18. Form a Cyber incident Response Team.

19. Collaborating with relevant institutions on cyber and information security issues.

20. Continuously learning and monitoring cyber and information security issues by identifying trends, methods and advanced developments in cyber and emerging attacks and ways of mitigating the risks associated with such attacks.

21. Prepare reports on major cyber and information security incidents to Bank of Sierra Leone.

22. Performing other related cyber and IT risk management tasks.

23. Supervising the work of the IT Risk Manager and serves as a liaison to Enterprise Risk Management committee.

SECTION THREE - CYBER AND INFORMATION TECHNOLOGY RISK MANAGEMENT

3.1. CYBER AND INFORMATION SECURITY STRATEGY

i. The Board of Directors shall approve a Commercial bank's cyber and information security strategies, which shall provide direction on how to achieve its cyber and Information security objectives.

ii. The strategies shall address and mitigate cyber and information security-risk while providing compliance with the legal, statutory and regulatory requirements.

iii. The strategies shall align with the Commercial bank's Information Security Management System (ISMS), and the overall corporate strategy.

3.2 CYBER AND INFORMATION TECHNOLOGY SECURITY POLICIES AND PROCEDURES

1. A financial institution shall also put in place a Cyber and Information Security Framework consisting of policies, standards and procedures in support of its strategy, which aligns policies, business and technological approaches to address cyber and Information security risks, which shall be presented to and approved by the Board.

2. The Cyber and IT Risk management policies should include the following areas:

i. Asset Management Policy

ii. System Configuration Management

iii. Cyber and IT Security Awareness Training

iv. Data Security (Data Loss Prevention)

v. System Development, Testing and Maintenance Policy (systems life cycle management

vi. Vulnerability Management (malware prevention)

vii. Access Control Policy, privileged user account access policy

viii. Physical Security Policy

ix. Personnel Security Policy (Human Resource Management)

x. Incident Response and Business Contingency Management

xi. Information security Event Management

xii. Third party Management

xiii. Removable Media Controls

3.3 PROCEDURES

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

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

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

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

5. IT risk policies, technical standards, and operational procedures shall be communicated to the staff frequently and updated on a timely basis.

3.4 ESTABLISHMENT OF CYBER AND INFORMATION SECURITY RISK MANAGEMENT STEERING COMMITTEE

1. The Senior Management shall appoint a Cyber and Information Security Risk Management Steering Committee.

2. The composition of the Steering Committee are as follows:

i. The Steering Committee shall include at least three members appointed by the Senior Management with the Certified Information Security Officer as Chair, the Heads of the Risk Management, Information Technology and major business units.

ii. The Board shall approve the Committee's structure.

3. The responsibilities of the Cyber and Information Security Risk Management Steering Committee are to help Senior Management to make judgments and to accomplish its duties in the arena of cyber and information security, including, backup and recovery issues.

4. The Steering Committee shall discuss and supervise:

i. The implementation of plans and activities to reduce cyber and information security risks, including backup and recovery issues.

ii. prospective risks involved in activating institutional systems in a cloud environment; and

iii. Potential risks involved in outsourcing institutional activities.

iv. the effectiveness of strategic IT planning, the IT budget and actual expenditure

5. The Steering Committee shall meet at least once a month and document its discussions.

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

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

3.5 CYBER AND INFORMATION SECURITY RISK MANAGEMENT SYSTEMS

The Risk Management programme shall be based on an understanding of threats, vulnerabilities, risk profile and level of risk tolerance of the institution. The process shall also be dynamic in view of the constantly changing risk landscape. The Risks management system consists of six stages:

* Risks Management
* Identification of all Information and IT assets
* Risks Survey
* Risks Assessments
* Risks mitigation
* Risk monitoring and Reporting

(1) RISKS MANAGEMENT

i. Risks shall be managed from a cross functional perspective.

ii. The Cyber and Information Security Risk Management Steering Committee shall be involved in this process and report to Senior Management and the Board of Directors.

iii. The Board and Senior Management shall support and be involved in the cyber information Technology-risk management process by ensuring that resources and capabilities are available, and roles of staff properly defined in management of risks.

iv. The Cyber and Information Security Risk Management Steering Committee shall report to the Senior Management on the following area:

(a) Managing cyber and information security risks is part of the overall risk management in Commercial Banks.

(b) Commercial Banks shall manage the cyber and information security risks together with operational and business continuity risks.

(c) When addressing matters related to business continuity, Commercial Banks shall also appraise cyber and information security risks that may affect its own operations and those of its suppliers and service providers.

(d) The Commercial bank risk management process shall rely on renowned methodologies and include surveys and tests as well as other useful risk assessment and mitigation processes.

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

a) cyber and information security risks;

b) new threats discovered globally or in Sierra Leone and their implications on the bank.

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

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

(2) Identification of all Information and IT assets.

i. Commercial banks shall identify all information and IT assets define their function, purpose and criticality.

ii. Their resources (time, people and money) are focused on the highest priority asset versus the lower priority and less critical assets.

iii. Commercial banks shall;

a) Keep a current record of all authorized devices such as workstations, laptops, printers, their owners and the operating system installed on them.

b) Maintain a list of scanner, photocopiers and owners.

c) List of servers, functions and operating systems Installed on them.

d) Network Inventory (routers, switches, hubs, bridges, gateway, modem, repeaters, Access points, firewalls)

e) Ensure that all identified devices are labelled according to the criticality and sensitivity of the data/information they store, process or transmit

f) Ensure that all identified devices are branded by their location and keep track of their movement.

g) Automate the detection of unauthorized devices as they connect to the Commercial Banks' network and ensure that only authorized devices are granted access to the network.

h) Ensure that all legacy systems but still-in-use (both critical and non-critical) shall be classified. Weaknesses connected with them shall be promptly identified and controls applied and must be upgraded.

(3) Risk survey

i. Commercial banks shall determine the cyber and information security threats and vulnerabilities to its environment, which comprise internal and external networks, hardware, software applications, systems interfaces, operations procedures and people.

ii. The computer surveys and cyber and information security defense tests shall be done frequently on Commercial Banks's IT systems and processes shall also be performed on any new or modified systems.

iii. The surveys are designed to ensure that the systems and infrastructure are resilient; assess the efficacy of protective measures with reference to the risk assessment; and suggest ways of correcting any issues discovered.

iv. The Chief Information Security Officer is responsible for determining the annual and multi-annual work plans for conducting cyber and information security surveys and tests, types of tests and the timetable and scope of tests.

v. The CISO shall budget and select the surveys as part of his annual work plan.

vi. Senior Management shall deliberate and approve any changes in the budgets allocated for surveys.

vii. The changes shall be brought to the Board's knowledge.

viii. The CISO shall ensure that the systems of all Commercial Banks, business and technological processes are surveyed regularly, at least once a year.

ix. The CISO shall initiate controlled penetration and robustness tests for Commercial Banks' various systems to assess their resilience to both internal and external risks.

x. This activity shall be performed at an interval appropriate to the specific risks of each system.

xi. Systems defined by Commercial Banks as high risk and/or connected directly to the internet and/or communicating outside Commercial Banks and/or using Wide-Area Network (WAN) shall be surveyed at least quarterly.

xii. The survey shall include, among other matters, the various systems' technological infrastructures and their security and communication links.

xiii. Survey findings and recommendations shall be submitted to the Cyber and Information Security Risk Management Steering Committee, which shall discuss them and set a schedule for implementing the corrective measures.

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

xv. Substantial survey and penetration test findings shall be reported to Senior Management and the Board's Cyber Committee.

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

(4) Risk Assessments

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

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

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

   i. the findings of audits and surveys, and any other regularly

   ii. available information that may suggest a vulnerability or breach;

   iii. external data, including information from third-party research

   iv. and notification from entities able to suggest a potential weakness or lead to the discovery of exposures or risks not yet identified;

   v. lessons learned from cyber and information security incidents in the institution or elsewhere;

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

   vii. Qualitative and/or quantitative indicators to assess risk exposure.

3. The risk assessment shall refer to the various activity areas of Commercial Banks's operations.

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

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

6. External companies with expertise in risk assessment may be authorized to conduct the risk survey

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

8. The annual risk assessment shall be discussed by the Senior Management and Board.

9. The monthly updates shall be discussed by Senior Management on a monthly basis.

10. Assessments pointing to significant risks shall be brought before the Board.

(5) Risk Mitigation

a) Commercial Banks shall develop and implement risk mitigation and control strategies.

b) These shall include determining the residual risk and the likelihood of new incidents.

c) Mitigation and control measures include but are not limited to the following:

i. Commercial Banks shall examine the effectiveness of existing controls and assess the residual risks using qualitative and/or quantitative methodologies and indicators.

ii. The process and its outcomes, including methodologies and indicators used, shall be documented.

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

iv. The CISO shall formulate a work plan to be implemented when controls are lacking and/or when controls need to be replaced or enhanced.

v. The work plan, including timetable and budget, shall be formulated based on the degree of risk to the institution on account of the non-implementation of the activity required.

vi. The plan shall be submitted to the Steering Committee for approval.

vii. The CISO should review and update Commercial Banks Cyber and Information risk Controls and Mitigation approach takin ng into account changing circumstances and variations in Commercial Banks risk profile.

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

(6) Risk Monitoring and Reporting

i. Commercial Banks shall maintain a risk register to facilitate the monitoring and reporting of risks.

ii. 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.

iii. The institution shall review the risk register periodically and put in place a monitoring and review process for continuous assessment and treatment of risks.

iv. The CISO is responsible for cyber and information risk monitoring and reporting.

v. Commercial Banks are required to develop cyber and information risk matrix to highlight systems, processes or infrastructure that have the highest risk exposure.

vi. An overall cyber and information risk profile of the institution shall be provided to the Board and Senior Management.

vii. In determining the risk matrix, the institution shall consider risk events, regulatory requirements and audit observations.

4.0 CYBER AND INFORMATION TECHNOLOGY CONTROLS

Commercial banks shall ensure that the following controls are instituted:

a. Malware protection- systems are protected from malicious attacks by using anti malware, web and email filtering techniques.

b. Commercial banks shall have the capacity to employ encryption technologies to mitigate the risk of losing confidential information in the information systems or during its transmission.

c. Appropriate management processes of the encryption facilities shall be put in place to ensure that;

   i. Encryption facilities in use meet international best practice security standards or requirements.

   ii. Staff in charge of encryption facilities are well trained and screened.

   iii. Encryption strength is adequate to protect the confidentiality of the information; and

   iv. Effective and efficient key management procedures, especially key lifecycle management and certificate lifecycle management, are in place.

d. Configuration Management

Configurations of firewalls, routers, network segmentation are instituted to protect Commercial Banks' networks from unauthorized traffic.

e. Logical Access Controls

1. Commercial banks shall have an effective process to manage user authentication and access control. Access to data and system shall be strictly limited to authorize individuals:

   i. Whose identity is clearly established, and their activities in the information systems should be limited to the minimum required for their legitimate business use (Need-to-know and least privilege principle) and Segregation of duties.

   ii. Password and systems authentication controls- Appropriate user authentication mechanism commensurate with the classification of information to be accessed should be selected.

   iii. Timely review and removal of user identity from the system shall be implemented when a user transfers to a new job or leaves a Commercial Bank.

2. Commercial banks shall secure the operating system and system software of all computer systems by

   I. Clearly defining a set of access privileges for different groups of users, namely, end-users, system development staff, computer operators, and system administrators and user administrators.

   II. Setting up a system of approval, verification, and monitoring procedures for using the highest privileged system accounts.

f. Physical and Environmental Security

i. Commercial banks - shall consider fully the environmental threats (e.g. proximity to natural disaster zones, dangerous or hazardous facilities or busy/major roads) when selecting the locations of their data centers.

ii. Physical and environmental controls shall be implemented to monitor environmental conditions that could adversely affect the operations of information processing facilities.

iii. Equipment facilities shall be protected from power failures and electrical supply interference.

iv. Physical security zones, such as computer centers or data centers, network closets, areas containing confidential information or critical IT equipment, and respective accountabilities are clearly defined, and appropriate preventive, detective, and restorative controls are put in place.

v. Physical access to ICT systems shall be permitted to only authorize individuals.

vi. Authorization shall be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored.

vii. Physical access shall be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.

4.7 Network Management

i. Commercial banks shall divide their networks into logical security domains (hereinafter referred to as the "domain") with different levels of security.

ii. The following security factors have to be assessed in order to define and implement effective security controls, such as physical or logical segregation of network, network filtering, logical access control, traffic encryption, network monitoring, activity log, etc. for each domain and the whole network.

a) Criticality of the applications and user groups within the domain;

b) Access points to the domain through various communication channels;

c) Network protocols and ports used by the applications and network equipment deployed within the domain.

d) Connectivity between various domains; and Trustworthiness of the domain.

e) Keep an approved up-to-date network topology of their wired and wireless networks regardless of their location.

f) Maintain a directory of all dedicated/frequently used network connection(s) to regulatory authorities, switches, vendors/contractors, and wholesale customers with details of the objectives of such connections.

g) Formulate a mechanism to maintain an up-to-date register of all other authorized network devices - ATMs, IP Phones and surveillance cameras etc. - connected to its network.

h) Unauthorized network devices shall not be granted access to the network; and make sure that risks related with these devices are regularly evaluated, documented and mitigated promptly.

4.8 Patch Management

Requires technical staff to review available security patches and report the patch status periodically.

4.9 Systems Software Security

Commercial banks shall ensure the security of all the application systems by: -

i. Creating a mechanism to maintain a current register of all applications/software (authorized and unauthorized) installed and/or running on all its systems. Unauthorized software/applications identified shall be considered for removal.

ii. Ensuring that the installation of applications/software including patches and hotfixes to approved workstations/laptops, server and mobile devices are centrally coordinated and managed by the systems administrator.

iii. Ensuring that all legacy but still-in-use software and applications are classified. Weaknesses related with them shall be quickly identified and upgraded.

iv. Instituting controls to discontinue unauthorized amendments or removal of its authorized software/applications while preventing the installation of unauthorized software/applications on its network.

v. Clearly defining the roles and responsibilities of end-users and IT staff regarding the application security;

vi. Implementing a robust authentication method commensurate with the criticality and sensitivity of the application system;

vii. Enforcing segregation of duties and dual controls over critical or sensitive functions; and

viii. Maintaining an audit trail in electronic format.

4.10 Events Management

1. Commercial banks shall have a set of policies and procedures controlling the login activities in all production systems to support effective auditing, security forensic analysis, and fraud prevention.

2. Commercial banks shall use automated software solution that aggregates and analyzes activity from many different resources across bank's entire IT infrastructure. Examples include Data dog Security Monitoring, Solar Winds Security Event Manager and McAfee Enterprise Security Manager etc.

4.11 Routine Maintenance on Computers and IT equipment

i. Commercial banks shall put in place an effective and efficient system for securing all end-user computing equipment, which include desktop personal computers (PCs), portable PCs, teller terminals, automatic teller machines (ATMs), debit or credit card readers, point of sale (POS) terminals, etc. and conduct periodic security checks on all equipment.

ii. Commercial banks shall ensure the continued availability of technology related services with timely maintenance and appropriate system upgrades.

iii. Proper record keeping (including suspected and actual faults and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance.

4.12 Protection of Customer Information.

Commercial banks shall put in place a set of policies and procedures to govern the collection, processing, storage, transmission, dissemination, and disposal of customer information.

4.13 Cyber Security Awareness Training

1. Commercial banks shall implement cyber and IT security awareness training programs to provide information on good IT security practices, common threat types and the institution's policies and procedures.

2. Training shall be provided to all employees including Senior Management and the Board.
3. Staff should fully understand the consequences of violating Cyber Security and Risk Management policies and procedures.

4. Commercial banks shall adopt a zero-tolerance policy against security violation.

5. Cyber security awareness and information should be provided to the institution's customers, clients, suppliers, partners, outsourced service providers and other third parties, who have links to the bank's IT infrastructure.

6. Commercial banks shall ensure that the training programme provides training for all staff members on a quarterly basis and contractors at least annually.

4.14 Application System Development, Testing and Maintenance

Commercial banks shall have the capability to identify, plan, acquire, develop, test, deploy, maintain, upgrade, and retire information systems.

4.15 Systems Upgrade

i. Commercial banks shall have a set of policies and procedures for controlling the process of system upgrade.

ii. The system upgrade shall be treated as a project and managed by all pertinent project management controls including user acceptance testing.

4.16 IT Project Planning Management

i. Policies and procedures shall be in place to govern the initiation, prioritization, approval, and control of IT projects.

ii. Commercial banks shall recognize the risks associated with IT projects, which include the possibilities of incurring various kinds of operational risks, financial losses, and opportunity costs stemming from ineffective project planning or inadequate project management controls of the bank.

iii. Appropriate project management methodologies shall be adopted and implemented to control the risks associated with IT projects.

iv. Progress reports of major IT projects shall be submitted to and reviewed by the Cyber and Information Security Steering Committee periodically.

4.17 Acquirement, development and maintenance of information system

1. Commercial banks shall adopt and implement a system development methodology to control the life cycle of Information systems.

2. The typical phases of system life cycle include system analysis, design, development or acquisition, testing, trial run, deployment, maintenance, and retirement.

3. The system development methodology to be used should be commensurate with the size, nature, and complexity of the IT project.

4. Commercial banks shall ensure system reliability, integrity, and maintainability by controlling system changes with a set of policies and procedures, which should include the following elements.

    i. Ensure that production systems are separated from development or testing systems;

    ii. Separating the duties of managing production systems and managing development or testing systems;

    iii. Prohibiting application development and maintenance staff from accessing production system under normal circumstances unless management approval is granted to perform emergency repair, and all emergency repair activities should be recorded and reviewed promptly;

    iv. Promoting changes of program or system configuration from development and testing systems to production systems should be jointly approved by IT Department and business departments, properly documented, and reviewed periodically.

4.18 Problem Management and Incidence Reporting

1. Commercial banks shall have in place a problem management and processing system to respond promptly to IT operation incidents, to escalate reported incidents to relevant IT management staff and to record, analyze and keep tracks of all these incidents until rectification of the incidents with root cause analysis is completed.

2. A help desk function shall be set up to provide front-line support to users on all technology-related problems and to direct the problems to relevant IT functions for investigation and resolution.

3. Support services or technical assistance from vendors, if necessary, shall also be documented.

4. Contacts and relevant contract information shall be made readily available to the employees concerned.

5. Accountability and line of command shall be delineated clearly and communicated to all employees concerned, which is of utmost importance for performing emergency repair.

4.19 Information Technology Operations

1. Commercial banks shall separate IT operations or computer center operations from system development and maintenance, to ensure segregation of duties within the IT Department.

2. Commercial banks shall detail operational instructions such as computer operator tasks, job scheduling and execution in the IT Operations Manual.

3. The IT Operations Manual shall also cover the procedures and requirements for on-site and off-site backup of data and software in both the production and development environments (i.e. frequency, scope and retention periods of back-up).

4. Commercial banks shall implement a process to ensure that the performance of application systems is continuously monitored, and exceptions are reported in a timely and comprehensive manner.

4.20 Change Management

a) Commercial banks shall have an effective change management process in place to ensure integrity and reliability of the production environment.

b) Commercial banks shall develop a formal change management process.

4.21 Business Continuity Management

4.21.1 Commercial banks shall:

1. Establish formal business continuity plans that outline arrangements to reduce the impact of a short, medium and long-term disruption, including:

   (a) Resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;

   (b) The recovery priorities for Commercial Banks's operations;

   (c) Communication arrangements for internal and external stakeholders.

2. Formulate escalation and evacuation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;

3. Possess processes to validate the integrity of information affected by the disruption.

4. Possess processes to review and update (1) to (3) following changes to Commercial Banks's operations or risk profile.

4.21.2 Business Impact Analysis

As part of sound business continuity management,

1. Commercial banks shall conduct Business Impact Analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis.

2. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies.

3. Commercial banks shall ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.

4.21.3 Business Continuity Planning

Based on their Business Impact Analysis,

1. Commercial banks shall establish plans to ensure business continuity (business continuity plans, BCPs), which shall be documented and approved by their management bodies.

2. The plans shall specifically consider risks that could adversely impact ICT systems and ICT services.

3. The plans shall support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets.

4. Commercial banks shall coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.

5. Commercial banks shall put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident).

6. In cases of severe business disruption that trigger specific business continuity plans, commercial banks shall prioritize business continuity actions using risk-based approach, which can be based on the risk assessments carried out. For Payment Service Providers this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.

7. Commercial banks shall consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it shall assess the potential impact that such scenarios might have.

8. Based on these scenarios, a commercial bank shall describe how the continuity of ICT systems and services, as well as the commercial bank's information security, are ensured.

4.21.4 Response and Recovery Plans

1. Based on the Business Impact Analysis and plausible scenarios, commercial banks shall develop response and recovery plans.

2. These plans shall specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, commercial banks' critical ICT systems and ICT services.

3. The response and recovery plans shall aim to meet the recovery objectives of commercial banks' operations.

4. The response and recovery plans should consider both short-term and long-term recovery options. The plans should:

    a) focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of commercial banks and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;

    b) be documented and made available to the business and support units and readily accessible in the event of an emergency;

    c) be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.

5. The plans should also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.

6. As part of the response and recovery plans, commercial banks shall consider and implement continuity measures to mitigate failures of third party providers, which are of key importance for a commercial bank's ICT service continuity.

4.21.5 Testing of Plans

1. Commercial banks shall test their BCPs periodically. They shall ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually.

2. BCPs shall be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events.

3. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, should also be considered, where relevant, as a basis for updating the BCPs.

4. Commercial banks' testing of their BCPs should demonstrate that they are able to sustain the viability of their businesses until critical operations are re-established. They shall:

    a) include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as testing of services provided by third parties, where applicable); this should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;

    b) be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans.

    c) include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the defined scenarios.

5. Test results shall be documented and any identified deficiencies resulting from the tests shall be analysed, addressed and reported to the management body.

4.21.6 Crisis Communications

a) In the event of a disruption or emergency, and during the implementation of the BCPs, commercial banks shall ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authorities when required by national regulations, and also relevant providers (outsourcing providers, group entities, or third party providers) are informed in a timely and appropriate manner.

b) A final BCP plan and an annual drill result must be signed off by the IT Risk Management, or internal auditor and Cyber and Information Security Steering Committee.

4.22 Outsourcing

1. In controlling access by third-party personnel (e.g. service providers) to secured areas, proper approval of access should be enforced, and their activities should be closely monitored. It is important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for permanent and temporary technical staff and contractors.

2. Commercial banks shall establish service level agreement and assess the IT service level standard attained.

3. Commercial Banks cannot contract out its regulatory obligations and should take reasonable care to supervise the discharge of outsourcing functions.

4. Commercial Banks also should take particular care to manage material outsourcing arrangement (such as outsourcing of data center, IT infrastructure, etc.) and shall notify BSL, when it intends to enter a material outsourcing arrangement.

5. Before entering, or significantly changing, an outsourcing arrangement, Commercial banks shall:

    i. Analyze how the arrangement will fit with the bank's reporting structure, business strategy, overall risk profile; and ability to meet its regulatory obligations.

    ii. Consider whether the arrangements will allow it to monitor and control its operational risk exposure relating to the outsourcing.

    iii. Conduct appropriate due diligence of the service provider's financial stability, expertise and risk assessment of the service provider, facilities, and ability to cover the potential liabilities.

    iv. Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract); and

    v. Consider any concentration risk implication such as the business continuity implication that may arise if a single service provider is used by several firms or ceases to exist.

6. In negotiating its contract with a service provider, Commercial banks shall consider (but not limited to) the following:

    i. Reporting and negotiation requirements, it may wish to impose on the service provider.

    ii. Whether enough access will be available to its internal auditors, external auditors and banking regulators.

    iii. Information ownership rights, confidentiality agreements and firewalls to protect client and other information (including arrangements at the termination of contract);

    iv. The extent to which the service provider must comply with Commercial Banks's policies and procedures covering IT Risk.

    v. The extent to which the service provider will provide business continuity for outsourced operations, and whether exclusive access to its resources is agreed.

    vi. The need for continued availability of software following difficulty at a third-party supplier.

7. The processes for making changes to the outsourcing arrangement and the conditions under which Commercial Banks or service provider can choose to change or terminate the outsourcing arrangement, such as where there is:

I. A change of ownership or control of the service provider or Commercial bank; or

II. Significant change in the business operations of the service provider or Commercial bank; or

III. Inadequate provision of services that may lead to Commercial Banks being unable to meet its regulatory obligations.

8. In implementing a relationship management framework, and drafting the service level agreement with the service provider, Commercial banks shall consider (but not limited to) the following:

   i. The identification of qualitative and quantitative performance targets to assess the adequacy of service provision, to both Commercial Banks and its customers, where appropriate.

   ii. The evaluation of performance through service delivery reports and periodic self-assessment and independent review by internal or external auditors; and

   iii. Remediation action and escalation process for dealing with inadequate performance.

9. Commercial banks shall enhance IT related outsourcing management in place to ensure data security of sensitive information such as:

   i. Bank's customer information; effectively separated from other customer information of the service provider.

   ii. The related staff of service provider should be authorized on "need to know" and "minimum authorization" basis.

   iii. Ensure service providers guarantee its staff for meeting the confidential requests.

   iv. All outsourcing arrangements related to customer information should be identified as material outsourcing arrangements and the customers should be notified.

   v. Strictly monitor re-outsourcing actions of the service provider and implement adequate control measures to ensure information security of the bank.

   vi. Ensure all related sensitive information be refunded or deleted from the service provider's storage when terminating the outsourcing arrangement.

10. Commercial banks shall ensure that it has appropriate contingency in the event of a significant loss of services from the service provider. Issues to consider include a significant loss of resources, turnover of key staff, or financial failure of, the service provider, and unexpected termination of the outsourcing agreement.

11. All outsourcing contracts shall be reviewed or signed off by IT Risk Management, internal IT auditors, Legal Department, and Cyber security and Cyber and Information Security Steering Committee. There shall be a process to periodically review and refine the service level agreements.

4.23 External Audit

1. The external information technology audit of Commercial Banks shall be carried out by certified service providers in accordance with laws, rules and regulations.

2. Commercial banks shall ensure there is an IT audit service provider to review and examine bank's hardware, software, documentation, and data to identify cyber and IT risks when they are commissioned to perform the audit.

3. Commercial banks shall communicate with the service provider in depth before the audit to determine audit scope and should not withhold the truth or do not cooperate with the service provider intentionally.

4. Commercial banks shall ensure the service providers strictly comply with laws and regulations to keep confidential and data security of any commercial secrets, private information learnt and cyber and IT risk information, when conducting the audit.

5. The service provider shall not modify, copy or take away any document provided by Commercial Banks.

4.24 .0 Electronic Banking Services

1. Commercial Banks shall be required to modify their risk management framework to the changing technological environment and modernize it on an ongoing and dynamic basis to deal with these risks.

2. Commercial Banks shall strictly observe information security principles to protect customer confidential information, information integrity of the bank and the availability of electronic banking services.

3. Commercial Banks shall also be required to improve on methods to detect misappropriation and fraud, perpetrated via remote transactions.

4.24.1 General

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

2. Commercial Banks shall put in place a procedure for obtaining customer approval on account transactions with reference to such aspects as type, nature and amount requested.

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

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

5. Commercial Banks shall provide customers with information about the precautions required when operating in an online environment at least once yearly.

6. Every new service shall be approved in advance by Bank of Sierra Leone.

4.25 Subscribing to Electronic Banking Services

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

2. 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.

3. Prior to obtaining the customer's approval for an agreement, Commercial Banks shall present to the customer the EBSs what each channel provides and the risks they involve.

4. Commercial Banks shall also inform the customer about cyber information security and recommended privacy protection principles for minimizing these risks to the customer.

4.26 Identification and Authentication

1. Commercial Banks shall determine individual identification and authentication factors for online and other remote transactions based on risk assessments and policies approved by the Board.
2. Commercial Banks 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.

3. Rules shall be put in place to determine password length and complexity re-use limitations, the frequency of password change, and password blocking and unblocking.

4. Identification and authentication factors shall be delivered to the customer securely and on separate channels.

5. Commercial Banks may make certain services and transactions depending on the use of additional factors such as a one-time code delivered on a different channel or generated by a dedicated component, biometric and identifications.

4.27.0 Online Services

4.27.1 Website

1. Commercial Banks shall utilize the means under its control to protect the computer or devices the customer uses for banking communications against unauthorized use and exposure of information about the customer's accounts.

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

3. Customer information shall be stored in the innermost zone of the server farm.

4. Customer information shall not be stored on a public cloud. Customer authentication method shall be based on a two-factor authentication.

5. Commercial Banks that operate a transactional website or web application shall also operate a technical support service and channels for reporting unusual incidents and other relevant issues. This service shall be available daily.

6. Commercial Banks shall conduct the following to assess the effectiveness of the existing safeguards:

    i. Website penetration tests at least half yearly and/or following any significant modification;

    ii. Penetration tests for the internal servers every six months and/or following any significant modification.

4.28 Mobile Applications

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

2. A user shall provide his expressed agreement to use the bank's mobile application.

3. A record of this agreement shall be saved to the bank's network.

4. Notification of receipt of the user's agreement to use the mobile application shall be sent to the user utilizing a channel such as SMS.

5. Mobile application shall be tested and examined by commercial bank regarding its cyber and information security prior to its release to customers.

6. Any mobile application update shall require a re-examination same.

7. Applications shall not store sensitive information on the mobile device.

8. Data shall be stored in encrypted form using the devices mechanisms when required.

9. Sensitive personal information shall be erased upon quitting the application.

10. Commercial Banks shall have in place an identification and authentication mechanism to verify the identity of mobile application users.

11. It shall for example use multi-factor authentication, such as fingerprints, as an additional layer of user authentication assuming the device supports such a capability.

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

13. Commercial Banks shall examine at least once every 24 hours whether the third-party applications used, indeed match those it has distributed to the store when a third party is used to distribute the application.

4.29 Email

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

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

3. Information shall be emailed from the commercial bank to the customer by adhering to the following:

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

ii. protected by a digital signature allowing senders authentication

iii. Commercial banks should be notified using electronic means that the customer has received and opened the email, downloaded it to his personal computer and/or printed it; and Information on customer activities is securely saved in the bank's network.

4.30 Text Messages (SMS)

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

4.31.0 Cloud services

4.31.1 Corporate Governance

a) Commercial Banks considering the use of cloud computing shall bring this issue to the Board prior to implementing this technology.

b) The Board shall discuss the risks involved and decide whether to grant its preliminary approval and direct Senior Management on steps required accordingly.

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

i. 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 risks;

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

iii. controls and auditing entities; type and scope of cloud services; legal aspects;

4.31.2 Terms and conditions of contract termination.

I. The Board shall either reject or approve the commercial bank's use of cloud computing based on the terms and conditions of contract.

II. The Senior Management and Board shall discuss the agreement prior to finalizing its contract with a cloud service provider.

III. Commercial Banks shall seek approval from BSL to transit to cloud services.

4.31.3 Risk Management

i. Commercial Banks shall conduct due diligence on the provider's financial strength, professionalism, and experience in providing similar services to other institutions prior to contracting with any cloud service provider.

ii. During the contract period or at least every two years, the commercial bank shall conduct additional due diligence.

iii. Commercial Banks shall conduct risks assessment prior to contracting with a cloud service provider.

iv. The assessment shall be updated on a yearly basis throughout the contract period or when technological, business changes (e.g. transitioning a new activity area or application to the cloud), institutional and regulatory changes in the bank and/or provider.

v. Senior Management shall discuss and approve transitioning to the cloud, any activity area or application not included in the original contract.

vi. Commercial Banks shall ensure that all controls are in place, including appropriate compensatory controls for the risks that have been identified and recorded.

vii. Commercial bank shall ensure that it is able to monitor cyber and information security incidents related to its use of cloud services.

viii. Data in motion between Commercial Banks and the provider shall be encrypted.

ix. Data stored with cloud service providers shall be encrypted.

x. The data classified by Commercial Banks as sensitive shall be encrypted.

xi. The encryption keys shall be stored with commercial banks rather than the providers.

4.31.4 The Cloud Computing Service Contract

The contract with the provider shall provide for, but not be limited to.

i. Receipts of the provider's internal and external cyber and information security auditing reports about its activity;

ii. Enabling the commercial bank to conduct independent cyber and information security audit surveys, including resilience and penetration tests and/or any other tests that substantiate and confirm the provider's compliance with this guideline;

iii. Enabling the bank, under special circumstances, to require that the provider conduct an ad-hoc security audit of a specific issue;

iv. Allowing the bank to unilaterally suspend use of the provider's services or switch to a different provider.

v. The commercial bank 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 its data from the provider's systems when it switches to another provider.

vi. The provider shall undertake that the data transfer including backups shall no longer be restorable from its systems;

vii. Commercial banks shall ensure that the service provider conducts cyber and information security audits in the provider's premises.

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

5.0 CYBER AND INFORMATION TECHNOLOGY DEFENSE

Commercial banks shall continuously monitor the network and information systems to detect anomalies and potential cyber security incidents before they can cause any significant damage. This shall cover the following:

I. Security Information and Event Management (SIEM)

II. Security Cameras

III. Intrusion Detection Solutions- Vulnerability assessment and penetration testing

6.0 CYBER AND INFORMATION TECHNOLOGY RESPONSE AND RECOVERY

1. Commercial banks shall implement an incident response management programme and measures to ensure business continuity.

2. Commercial banks shall ensure that they have in place the following:

i. Incident response management plan,

ii. Business and Disaster Continuity Management.

7.0 CYBER THREAT INTELLIGENCE

1. Commercial banks are required to possess an objective knowledge - based on facts on all emerging threats, cyber-attacks, attack vector, mechanisms and indicators of attack/ compromise to its information technology assets, which shall be used to make informed decisions.

2. Commercial Banks are required to:

I. Institute a Cyber-Threat Intelligence (CTI) program, which shall proactively identify, detect and mitigate potential cyber-threats and risks.

II. Create a Cyber-Threat Intelligence (CTI) policy (as part of the cyber security policy) approved by the Board of Directors to aid proactive identification of emerging cyber threats, trends, patterns, risks, and possible impact.

III. Take informed decisions based on the Cyber Threat Intelligence (CTI) program as it offers valuable information on areas susceptible to cyber-attacks, latest threats, attack vector etc. conducting emergency awareness training, vulnerability assessment, and penetration testing; review of vendor source codes, cyber-incident response plans, BCP/DR plans, Service Providers SLA; and increased system logging etc.

IV. Commercial Banks are required to promptly report all impending and challenging cyber-threats to their information assets to the Director, Banking Supervision Department, Bank of Sierra Leone.

8.0 INFORMATION SHARING AND COLLABORATION

All Commercial banks shall establish a Cyber-security Information Sharing and Collaboration Platform to facilitate sharing of cyber Security information and communication within the bank and among Commercial Banks, regulators and external parties to defend themselves against emerging cyber threats and fight cybercrime.

9.0 REPORTING

1. Bank of Sierra Leone directs all Commercial Banks to review their cyber security and Information Technology Risk Management strategies, policies, and frameworks regularly based on each institution's threat and vulnerability assessment.

2. Commercial Banks are required to submit their Cyber security and IT Risk Management Policies, strategies and frameworks to the Bank of Sierra Leone by 31st December, 2021.

3. The essential elements of a cyber-security policy charter are outlined in Appendix I to these Guidelines.

4. Commercial banks shall inform the BSL within 24 hours of any Cyber security incident(s) in the specified format set out as Appendix II.

5. On a quarterly basis, Commercial Banks shall provide BSL with a report in the format set out as Appendix III (Quarterly), concerning occurrences and its handling of Cyber security incidents via the email address bsup@bsl.gov.sl

In the event of any query or clarification, please contact:

The Director,
Banking Supervision Department
Bank of Sierra Leone
Gloucester Street
Freetown

10.0 Effective Date
These Guidelines shall come into effect on the day it is published in the Gazette.

APPENDIX 1

BANK OF SIERRA LEONE

THE ESSENTIAL ELEMENTS OF A CYBER SECURITY CHARTER

CYBER SECURITY CHARTER

1. The governance structure and processes-

Includes activities for the Board and senior managers to ensure that cyber security is overseen and validated from the top of Commercial Banks. Commercial banks shall have clear governance structures and defined lines of responsibility and accountability to oversee its cyber security and resilience processes. This might include establishing different elements of the framework into functions overseen by an accountable Director or governance committee. (Risk Management, Internal Audit, CISO, Compliance, Effective Risk Management programme etc.)

2. Board level commitment and involvement.

The Board shall endorse, support and participate?in the cyber security strategy, and receive regular updates on security issues, risks and compliance.

3. Board should also institute a continual improvement process?

A process to continually review and improve Commercial Banks's security measures, and to adapt to the changing threat landscape

4. Defense

Cyber resilience hinges on effective security controls that protect the confidentiality, integrity and availability of its assets and services.

5. Monitoring

i. Security monitoring

Commercial Banks systems, networks and security measures should be continually observed and logged, both through automated means and through less frequent activities such as vulnerability scanning and penetration testing. Any identified anomalies and weaknesses should be acted upon.

ii. Active detection

Commercial banks shall also actively seek to detect incidents (for example, by manually reviewing audit logs and gathering intelligence from outside the institution). Measures shall be put in place to help detect malicious activity that might otherwise be difficult to identify.

iii. Information security reviews

Commercial banks may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the bank should consider good practices such as source code reviews.

6. Response and Recovery

Commercial banks shall address the need to manage incidents quickly and effectively, to stop business disruption and return to full functionality.

i. Incident response management
There should be plans, defined roles, training, communications and management oversight for quickly discovering an incident and effectively containing the damage, eradicating the threat, and restoring the integrity of affected network and systems.

ii. Business continuity management
Commercial banks shall have measures in place for identifying the risk of exposure to internal and external threats, and for dealing with major disruptions like cyber-attacks, floods and supply failures.

7. Testing the element of cyber resilience
The- elements of a cyber-resilience framework shall be tested to determine its total effectiveness.

8. Cyber threat intelligence
Create a Cyber-Threat Intelligence (CTI) policy (as part of the cyber security policy) approved by the Board of Directors to aid proactive identification of emerging cyber threats, trends, patterns, risks, and possible impact.

9. Cyber security Training

i. Security team competence and training

The CISO and IT professional teams shall be suitably qualified and regularly trained on how to respond to cyber security incidents. There shall also be processes for developing security teams and identifying the necessary skills.

ii. Staff awareness training

Employees shall receive regular cyber security awareness training and be aware of security threats and procedures. This may include supplementary aids such as posters, briefings, etc.

10. Information Sharing and Collaboration

Threat and vulnerability information shall be shared among Commercial Banks, regulators, suppliers, to enhance the collective ability to proactively detect, prevent, mitigate, respond to and recover from cyber security incidents.

11. Resources

Commercial banks shall allocate enough cyber security budget based on the structure and size of its cyber risk function.

APPENDIX 2

BANK OF SIERRA LEONE

CYBER SECURITY INCIDENT REPORT FORM

Name of Commercial bank……

Reporting Period: Date…… Time…… of Reporting

Date of Incident	Time of Incident	Nature of Incident (Chronological order of events)	Impact Assessment	Number of Systems affected and details	Action already taken	Current Status

Commercial bank shall submit the cyber security incident report within 24 hours after a cyber-security incident(s) to the Banking Supervision Department at bsup@bsl.gov.sl

Signed for and behalf of ……
By the duly authorized Signatories

Name: ……

Designation: ……

Signature: ……

Name: ……

Designation: ……

Signature: ……

APPENDIX THREE
BANK OF SIERRA LEONE
QUARTERLY CYBER SECURITY INCIDENT REPORT FORM

Name of Commercial bank……

Reporting Period: …… Quarter: ……

No.	Date of Incident	Time of Incident	Nature of Incident	Action taken	Time of resolution	Action taken to mitigate future incidents	Root Cause
1.							
2.							
3.							
4.							
5.							

Submit this report on the 10th day after the end of every quarter to the Banking Supervision Department at Bank of Sierra Leone. 30 Siaka Stevens Street, Freetown or via the email address bsup@bsl.gov.sl.

Signed for and behalf of …….

By the duly authorized Signatories

Name: ……

Designation: ……

Signature: ……

Name: ……

Designation: ……

Signature: ……

Decisions involving significant change of schedule, change of key personnel, change of vendors, and major expenditures should be included in the progress report.

Annex: Cyber Lexicon

Annex: Cyber Lexicon

Term	Definition
Access Control	Means to ensure that access to *assets* is authorised and restricted based on business and security requirements. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Authenticity	Property that an entity is what it claims to be. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Availability	Property of being accessible and usable on demand by an authorised entity. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and *information systems*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber Advisory	Notification of new trends or developments regarding a *cyber threat* to, or *vulnerability* of, *information systems*. This notification may include analytical insights into trends, intentions, technologies or tactics used to target *information systems*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber Alert	Notification that a specific *cyber incident* has occurred or a *cyber threat* has been directed at an organisation's *information systems*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber Event	Any observable occurrence in an *information system*. *Cyber events* sometimes provide indication that a *cyber incident* is occurring. Source: https://www.fsb.org /2018/11/cyber-lexicon/

Term	Definition
Cyber Incident	A *cyber event* that: i. jeopardizes the *cyber security* of an *information system* or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. Source: https://www.fsb.org /2018/11/cyber-lexicon/ /2018/11/cyber-
Cyber Incident Response Plan	The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a *cyber incident*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber Resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to *cyber threat*s and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incident*s. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber Risk	The combination of the probability of *cyber incidents* occurring and their impact. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber Security	Preservation of *confidentiality*, *integrity* and *availability* of information and/or *information systems* through the *cyber* medium. In addition, other properties, such as *authenticity*, *accountability*, *non-repudiation* and *reliability* can also be involved. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Cyber Threat	A circumstance with the potential to exploit one or more *vulnerabilities* that adversely affects *cyber security*. Source: https://www.fsb.org /2018/11/cyber-lexicon/

Term	Definition
Denial of Service (DoS)	Prevention of authorised access to information or *information systems*; or the delaying of *information system* operations and functions, with resultant loss of *availability* to authorised users. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a *cyber event*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Distributed Denial of Service (DDoS)	A *denial of service* that is carried out using numerous sources simultaneously. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Exploit	Defined way to breach the security of *information systems* through *vulnerability*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Identify (function)	Develop the organisational understanding to manage *cyber risk* to *assets* and capabilities. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Identity and Access Management (IAM)	Encapsulates people, processes and technology to identify and manage the data used in an *information system* to authenticate users and grant or deny access rights to data and system resources. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Incident Response Team (IRT) [also known as CERT or CSIRT]	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events. Source: https://www.fsb.org /2018/11/cyber-lexicon/

Term	Definition
Information System	Set of applications, services, information technology *assets* or other information-handling components, which includes the operating environment. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Integrity	Property of accuracy and completeness. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their *information systems*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Multi-Factor Authentication	The use of two or more of the following factors to verify a user's identity: -- knowledge factor, "something an individual knows"; -- possession factor, "something an individual has"; -- biometric factor, "something that is a biological and behavioural characteristic of an individual". Source: https://www.fsb.org /2018/11/cyber-lexicon/
Patch Management	The systematic notification, identification, deployment, installation and *verification* of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an *information system*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of *cyber incidents*. Source: https://www.fsb.org /2018/11/cyber-lexicon/

Term	Definition
Recover (function)	Develop and implement the appropriate activities to maintain plans for *cyber resilience* and to restore any capabilities or services that were impaired due to a *cyber incident*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected *cyber event*. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Social Engineering	A general term for trying to deceive people into revealing information or performing certain actions. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Threat Actor	An individual, a group or an organisation believed to be operating with malicious intent. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Threat Assessment	Process of formally evaluating the degree of threat to an organisation and describing the nature of the threat. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Threat Intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Threat Vector	A path or route used by the *threat actor* to gain access to the target. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Vulnerability	A weakness, susceptibility or flaw of an *asset* or control that can be exploited by one or more threats. Source: https://www.fsb.org /2018/11/cyber-lexicon/
Vulnerability Assessment	Systematic examination of an *information system*, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. Source: https://www.fsb.org /2018/11/cyber-lexicon/

References

https://eba.europa.eu/documents/10180/2522896/

EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf

EBA Guidelines on outsourcing arrangements

https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements/38c80601-f5d7-4855-8ba3-702423665479

EBA Guidelines on major incident reporting under PSD2

https://eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf

Irish Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks

https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2

Israel - Cyber Defense Management

https://www.boi.org.il/en/BankingSupervision/SupervisorsDirectives/ProperConductOfBankingBusinessRegulations/361_et.pdf

Singapore Technology risk related guidelines

https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

German circular on Supervisory Requirements for IT in Financial Institutions

https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1710_ba_BAIT_en.html?nn=9866146

ECB Cyber Resilience Oversight Expectations for FMIs

https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/

Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

Central Bank of Liberia Cyber Security Guidelines

Risk Based Cyber Security Framework Central Bank of Nigeria

Bank of Ghana–Cyber and Information Security Directive