



BANK OF UGANDA CYBER AND TECHNOLOGY RISK MANAGEMENT GUIDELINES, 2024

DECEMBER 2024

CONTENTS

PART 1: PRELIMINARY	3
1.0 Citation and Commencement	3
1.1 Background.....	3
1.2 Authorization.....	3
1.3 Definitions	3
 PART 11: STATEMENT OF GUIDELINE.....	 8
2.1 Purpose.....	8
2.2 Scope.....	8
2.3 Responsibility.....	8
2.4 Legal Context of Cyber Security Guidelines	8
2.5 Examples of Sources of Cybercrime	9
 PART 111: SPECIFIC REQUIREMENTS	 9
3.1 Governance.....	9
3.2 Regular Independent Assessments and Tests	13
3.2.1 Role of Risk Management Function	13
3.2.2 Role of Internal Auditors.....	14
3.2.3 Role of External Auditors	14
3.3 Outsourcing	14
3.4 Cloud Computing	15
3.5 Training/Awareness	16
3.6 Secure Software Development Lifecycle and Project Management	16
3.7 IT Services Management.....	17
3.8 Cyber Security Operations.....	18
3.9 Response and Recovery	18
3.10 Security Testing and Remediation.....	19
3.11 Identity Management.....	20
3.12 Personal Data Protection and Privacy	20
3.13 Data Security and Management.....	20
3.14 Cryptography	21
3.15 Cybersecurity Supply Chain Risk Management.....	21
 PART IV: Reporting	 21
 ANNEXES.....	 23
ANNEX I: Cyber and technology Incident Record (<i>Immediate</i>)	23
ANNEX II: Cyber and technology Incident Record (<i>Quarterly</i>).....	24

PART 1: PRELIMINARY

1.0 Citation and Commencement

These Guidelines may be cited as the Bank of Uganda Cyber and Technology Risk Management Guidelines, 2024 and shall come into force on **1st December 2024**.

1.1 Background

Technologies such as the cloud, big data analytics, mobile computing, the blockchain, Internet of Things (IoT) and Artificial Intelligence (AI) are transforming the way supervised financial institutions (SFIs) manage their day-to-day business, from decision making to customer service. The resulting paradox is that whilst supervised financial institutions are continuing to adopt digitalization the vulnerability to cyber related attacks is also becoming a concern. Cyber and Technology risks are inherently complex and could result in severe implications on supervised financial institutions should the threat not be properly managed. It is against this backdrop, that regulatory requirements aim at ensuring that robust Cyber and Technology risk management practices are in place.

1.2 Authorization

These Guidelines shall apply to all Bank of Uganda supervised financial institutions under the Financial Institutions Act, 2004 (as amended) and the Microfinance Deposit Taking Institution Act, 2003. It is intended to facilitate the regulation of Cyber and Technology risks in supervised financial institutions including Financial Holding Companies domiciled in Uganda with centralized Information Systems and their subsidiaries.

1.3 Definitions

- 1.4.1 **Asset:** Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.
- 1.4.2 **An API (Application Programming Interface) :** A set of services that is made available by a software component for use by other software components through a published interface.
- 1.4.3 **Air-gapped Backups:** A backup strategy where the backup storage device or system is physically and electronically isolated from the primary system and network, providing protection against cyber and technology incidents that may compromise the primary system.
- 1.4.4 **Black box testing** refers to a testing approach in which the tester is unaware of the system's internal workings. It evaluates the system's fundamental features and has no or little impact on the system's underlying logical structure.
- 1.4.5 **Bring Your Own Device (BYOD):** A policy that allows employees to use their personally owned devices (e.g., smartphones, tablets, laptops) to access enterprise networks,

applications, and data.

- 1.4.6 **Business Continuity'** is a state of continued and uninterrupted operation of a business.
- 1.4.7 **Business Continuity Management'** is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely manner in the event of disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.
- 1.4.8 **Business Continuity Plan'** is a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organization in the event of a disruption.
- 1.4.9 **Critical assets:** Resources and data that are essential for maintaining operations of the financial institution.
- 1.4.10 **Critical function:** Functions within the information infrastructure of a financial institution that must continue at a sufficient level without interruption or restart within given time frames after a disruption to the service.
- 1.4.11 **Critical system:** Systems whose failure will cause significant disruption to the operations of the relevant financial institution or materially impact the relevant financial institution's service to its customers. This includes systems which: (a) process transactions that are time critical; or (b) provide essential services to customers.
- 1.4.12 **Cyber and technology event:** Any observable occurrence in an information system that can make it malfunction, thus affecting the overall organizations operations.
- 1.4.13 **Cyber and technology incident:** An event, whether resulting from malicious activity or not, which: (a) jeopardizes the security of an information system or the information the system processes, stores or transmits; or (b) violates the security policies, security procedures or acceptable use policies.
- 1.4.14 **Cyber and technology attack:** The use of an exploit by an adversary to take advantage of a weakness with the intention of achieving an adverse effect on the information and communication technology environment.
- 1.4.15 **Cyber and technology Incident Response Plan:** The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber or technology incident.
- 1.4.16 **Cyber and technology resilience:** The ability of a financial institution to continue to carry out its operation by anticipating and adapting to cyber or technology threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering

from cyber and/or technology incidents.

- 1.4.17 **Cyber and technology risk:** The combination of the probability of cyber and technology incidents occurring and their impact.
- 1.4.18 **Cyber and technology threat:** A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber and /or technology security.
- 1.4.19 **Cyber and technology-crime:** According to the International Organization of Securities Commissions (IOSCO), ‘cyber-crime’ or ‘the cyber threat’ refers to a harmful activity, executed by one group or individual through computers, Information Technology (IT) systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity.
- 1.4.20 **Cybersecurity**’ is an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
- 1.4.21 **CISO**’ is an acronym referring to the chief information security officer. He/ She is the executive management level within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.
- 1.4.22 **Critical Information Infrastructure (CII)**’ refers to interconnected information systems and networks, the disruption of which would have serious impact on the economic well-being of customers, or on the effective functioning of financial institutions and the economy.
- 1.4.23 **Cyberspace:** The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.
- 1.4.24 **Cloud Service Providers (CSPs):** Entities that provide cloud computing services, which enable on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services).
- 1.4.25 **Data breach:** A compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, and/or access to data transmitted, stored or otherwise processed.
- 1.4.26 **Data retention policies:** The policies of persistent data and records management for meeting legal and business data archival requirements.
- 1.4.27 **Data retention period:** The period of time that a financial institution holds an information.
- 1.4.28 **DevOps (development and operations)** : is a software development methodology that combines software development (Dev) with information technology operations (Ops). The

goal of DevOps is to shorten the systems development life cycle and provide continuous delivery with high software quality.

- 1.4.29 **DevSecOps:** An approach that integrates security practices into the DevOps software development and deployment lifecycle, emphasizing collaboration, automation, and continuous monitoring to enhance the security posture of applications and infrastructure.
- 1.4.30 **Grey box testing:** refers to a testing approach in which the tester has a limited knowledge of a system's internal workings and also its fundamental aspects/features.
- 1.4.31 **Information asset:** refers to any piece of data, device or other component of the environment that supports information-related activities. In the context of this guidance, information assets include data, hardware and software. Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services.
- 1.4.32 **IT Infrastructure** refers to the hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and or customers and is usually internal to an organization and deployed within owned facilities.
- 1.4.33 **Managed Security Services:** Outsourced monitoring and management of security devices and systems, such as firewalls, intrusion detection systems, and virtual private networks (VPNs).
- 1.4.34 **Multi-factor authentication:** The use of two or more of the following factors to verify a user's identity: (a) knowledge factor, "something an individual knows"; (b) possession factor, "something an individual has"; (c) biometric factor, "something that is a biological and behavioural characteristic of an individual".
- 1.4.35 **Penetration testing:** The process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access.
- 1.4.36 **Recovery point objective (RPO):** The point to which information used by an activity is to be restored to enable the activity to operate on resumption.
- 1.4.37 **Recovery time objective (RTO):** The period of time following an incident within which a product or service or an activity is to be resumed, or resources are to be recovered.
- 1.4.38 **Red Team Exercise'** refers to an all-out attempt to gain access to a system by any means necessary, and usually includes cyber penetration testing, physical breach, testing all phone lines for modem access, testing all wireless and systems present for potential wireless access, and also testing employees through several scripted social engineering and phishing tests. These are real life exercises carried out by an elite small team of trained professionals that are hired to test the physical, cyber security, and social defenses of particular systems.

- 1.4.39 **Restoration:** The process of copying backup data from secondary storage and restoring it to its original location or a new location. A restore is performed to return data that has been lost, stolen or damaged to its original condition or to move data to a new location.
- 1.4.40 **Software as a Service (SaaS):** A cloud computing service model in which the provider hosts and delivers software applications to customers over the internet, eliminating the need for customers to install and run applications on their own systems.
- 1.4.41 **Security Operations Center (SOC):** A centralized unit that deals with security issues on an organizational and technical level, monitoring, detecting, analyzing, and responding to cybersecurity incidents using combination of technology solutions and a strong set of processes.
- 1.4.42 **Situational awareness:** The ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event.
- 1.4.43 **Third-party provider:** An external person or company who provides a service or technology as part of a contract.
- 1.4.44 **Threat intelligence:** Threat information that has been aggregated, transformed, analyzed, interpreted or enriched to provide the necessary context for decision-making processes.
- 1.4.45 **Vulnerability:** A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.
- 1.4.46 **Vulnerability assessment:** The 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.

PART 11: STATEMENT OF GUIDELINE

2.1 Purpose

This Guidance Note outlines the minimum requirements that institutions shall build upon in the development and implementation of strategies, policies, procedures and related activities aimed at mitigating cyber and technology risks. Therefore, the purpose of this Guidance Note is to:

- Create a safer and more secure cyberspace that underpins information system security priorities and promote stability of the Ugandan banking sector;
- Establish a coordinated approach to the prevention and combating of cybercrime; Up-scaling of identification and protection of critical information infrastructure;
- Ensure adoption of robust and sound risk practices for management of cyber and technology risk.
- Promotion of compliance with appropriate technical and operational cybersecurity standards;
- Development of requisite skills, continuous building of capacity and promote a culture of fostering a strong interplay between policy, leveraging on technology to do business and risk management; and
- Maintenance of public trust and confidence in the financial system.

2.2 Scope

This Guidance Note sets the minimum standards that institutions should adopt to develop effective cybersecurity governance and cyber and technology risk management frameworks. It is not a replacement for and does not supersede the legislation, regulations and guidelines that institutions must comply with as part of their regulatory obligations; particularly in the areas of risk management, outsourcing, information communication technology, data protection and privacy, internal controls and corporate governance. The Guidance applies without prejudice to the more restrictive rules provided for by the legal and regulatory provisions in force.

The guidance provides detailed requirements for Supervised Financial Institutions(SFIs) but allows for flexibility based on the FI' differences in size, volume, value of transactions, and role within the financial system. The Bank of Uganda will consider this flexibility when assessing compliance to ensure risk mitigation measures are proportionate to the specific institutions' risk magnitude.

2.3 Responsibility

The board of directors and executive management of an institution are expected to formulate and implement cyber and technology risk management strategy, framework, policy, procedures, guidelines and set minimum standards for an institution. All these must be documented and made available for review by external auditors and Bank of Uganda.

2.4 Legal Context of Cyber Security Guidelines

In Uganda, the general legal framework regarding cybercrime and electronic evidence is set out in the Computer Misuse Act 2011 (“CMA”). In addition, other legislations such as the Copyright and Neighboring Rights Act 2006, Regulation of Interception of Communications Act 2010 and Penal Code Act of Uganda also

provide for laws related to cybercrime and electronic evidence. The Electronic Signatures Act 2011 makes provision for and regulates the use of electronic signatures, whereas the Electronic Transactions Act 2011 provides a legal and regulatory framework to enable and facilitate electronic communications transactions and to provide legal recognition to electronic records. These laws and the National Cyber Security Strategy seek to reinforce cyber security capacity through enhanced private public partnership, reinforce citizens' trust in the use of ICT services, enhance international cooperation on cybersecurity and promote a culture of cyber security across all levels of society.

These guidelines in no way replace, remove or seek to diminish the SFIs statutory responsibilities and accountability but are an additional tool to reinforce the need for a safer and more secure cyberspace that underpins information system security priorities and promote stability of the Ugandan banking sector.

2.5 Examples of Sources of Cybercrime

Cyber-attacks launched against information systems have placed the abuse of cyberspace high in the domestic as well as international agenda. Some illustrations of cybercrime activities include:

- A breach in institutions' databases exposing data to cyber criminals.
- Improper access to privileged accounts – A non-privileged user who gains access to a privileged account could control the entire system. For example, hiding criminal acts by modifying or deleting log files or disabling detection mechanisms as well as creation of unknown users. People related attacks like phishing, malware introductions through social engineering that can be utilized to gain privileged system access to critical systems.
- Interconnectedness of institutions could lead to compromise in the institution's entry points such as through service providers.
- Internal IT systems can themselves be a source of cyber risk. For example, data replication arrangements that are meant to safeguard business continuity could transfer malware or corrupted data to the backup systems.
- Poor authentication controls to protect customer data, transactions, and systems.

PART 11: SPECIFIC REQUIREMENTS

3.1 Governance

a) Bank of Uganda

Bank of Uganda is mandated by law to ensure a safe and sound financial system for protection of depositor's funds and conducive for macro-economic stability. Today, the financial sector is highly digitized and integrated on a local and international scene. In keeping with the Financial Institutions Act 2004, BOU is responsible for regulating the financial institutions in Uganda.

b) Board of Directors

- i. All board members should understand the nature of their institution's business and the cyber threats involved. Robust oversight and engagement on cyber risk matters at the board level promotes a security risk conscious culture within the institution. The Board must have at least one member with

the requisite experience and skills to understand and manage technology risks, which include risks posed by cyber threats.

The responsibilities of the board in relation to cyber risk include:

- i. Oversee the cultivation and promotion of an ethical governance, management culture and awareness. Setting “the right tone from the top” is a crucial element in fostering a robust cyber risk management culture.
- ii. Engage management in establishing the institution’s vision, risk appetite and overall strategic direction with regards to cybersecurity Allocation of an adequate cybersecurity budget based on the institution’s structure, the mandated level of cyber preparedness and to ensure that business-related system developments not compete for resources intended for the protection of IT systems The training needs of cyber security staff should also be budgeted for each year.
- iii. Promote the adoption and implementation of international standards that secure and safeguard the organization information, data and digital assets and infrastructure and enforce regulatory compliance.
- ii. Review management’s determination of whether the institution’s cybersecurity preparedness is aligned with its cyber and technology risks. Adoption of an effective internal control framework to achieve security and reliability of its IT operating environment with submission of periodic independent reports. Institutions should determine the scope and frequency of independent reports. However, comprehensive independent reports from internal and external audit should be performed continuously .
- iii. Establish or review cyber and technology risk ownership and management accountability and assign ownership and accountability to relevant stakeholders; the coverage should include relevant business lines and not just the IT function.
- iv. Approve and continuously review the cyber and technology risks management strategy, governance charter, policy and framework. The purpose of the cyber and technology risks management strategies, policies and framework is to specify how to identify, manage, and mitigate cyber and technology risks in a comprehensive and integrated manner. The strategy, policies and frameworks should be tailored based on the institution’s risk profile, size, complexity and nature of their business processes.
- v. Ensure that the cyber and technology risk management policies applied to all of the bank’s operating entities, including subsidiaries, joint ventures and geographic regions.
- vi. Review on a regular basis the implementation of the institution’s cyber and technology risk management framework and implementation plan, including the adequacy of existing mitigating controls. The review should be done at least once in 12 months or as frequently as the risk landscape dictates.
- vii. Ensure that cyber and technology risk management matters are adequately discussed at board meetings and other relevant sub-committee meetings.
- viii. Review the results of management’s ongoing monitoring of the institution’s exposure to and preparedness for cyber threats.
- ix. Ensure that it receives periodic reports on material cyber and technology incidents, on the evolution of the threat landscape including current and emerging risks, on the findings of internal audits, external audits and testing exercises and on the overall status and effectiveness of the cyber and technology risk management framework.

- x. Appoint a Chief Information Officer, Chief Technology Officer, or Head of IT, and a Chief Information Security Officer, possessing the requisite expertise and experience. These appointments should be at executive management level.

c) Executive Management

Executive Management of an institution is responsible for implementing the institution's business strategy, risk appetite and threats. As such, the Executive Management should: -

- i. Implement the board approved cyber and technology risk management strategy, policy and framework.
- ii. Understand cyber organizational scope as well as identify cyber threats, critical business processes and assets.
- iii. Put in place adequate systems, processes and frameworks to secure and maintain the digital landscape of the organization with adequate controls, clear decision points, well-defined escalation paths, and cross-organizational and collaboration platforms to support a safer financial sector digital and cyber landscape.
- iv. Ensure the creation of mitigation and recovery procedures to contain cyber risk incidents, reduce losses and return operations to normal. However, it is worth noting that an institution is also required to have in place Business Continuity Management (BCM) processes for the entire institution as cyber risk is managed within the context of overall IT risk management.
- v. Continuously improve collection, analysis, and reporting of cyber incident and cybercrime information. This can be achieved through understanding the business environment institutions operate in, potential cyber risk points and referring to international best practices.
- vi. Oversee deployment of strong authentication measures to protect customer data, transactions and systems.
- vii. Ensure the provision of sufficient number of skilled staff including contractors and service providers that have the requisite level of competence and skills to perform the IT functions and manage cyber and technology risks, who should be subjected to enhanced background and competency checks.
- viii. Carry out, background checks on staff and third parties with access to the FI's data and IT systems should be performed to mitigate insider risk, including the risk of data breach, sabotage, and fraud by staff, contractors, and service providers.
- ix. Ensure timely and regular reporting to the board on the cyber risk status of the institution.
- x. Establish a cybersecurity benchmarking framework with the Board's endorsement.
- xi. Incorporate cyber and technology risk management matters as a standard agenda in Executive Management meetings.
- xii. Provide regular reports of the institution's cybersecurity posture to the board.
- xiii. Document cyber and technology incident response plan providing a roadmap for the actions the institution will take during and after a cyber and technology incident. The plan should address inter-alia:
 - The roles and responsibilities of staff;
 - Incident detection and assessment, reporting; and
 - Escalation and mitigation strategies deployed.

- xiv. Collaborate with other institutions and the security agencies to share the latest cyber threats/attacks encountered by the institution.
- xv. Create a post incident analysis framework to determine corrective actions to prevent similar incidents in the future.
- xvi. Oversee the evaluation and management of risks introduced by third party service providers; institutions may require attestation/assurance reports provided by reputable independent auditors for service providers.

d) Chief Information Security Officer (CISO)

The CISO **should be** an Executive management role reporting to either the Chief Executive or Executive Director and is responsible for:

- i. Overseeing and implementing the institution's cybersecurity program and enforcing the cyber and technology policy.
- ii. Ensuring that the institution maintains a current enterprise-wide knowledge base of its users, devices, applications, software licenses and their relationships, including but not limited to:
 - Software and hardware asset inventory;
 - Network maps (including boundaries, traffic and data flow); and
 - Network utilization and performance data.
- iii. Ensuring that information systems meet the needs of the institution, and the ICT strategy, in particular information system development strategies, comply with the overall business strategies, risk appetite and ICT risk management policies of the institution.
- iv. Design cybersecurity controls with the consideration of users at all levels of the organization, including internal (i.e. management and staff) and external users (i.e. contractors/consultants, business partners and service providers).
- v. Organizing professional cyber related trainings to improve technical proficiency of staff.
- vi. Ensure that regular and comprehensive cyber risk assessments are conducted at least once a year.
- vii. Ensure that adequate processes are in place for monitoring IT systems to detect cyber and technology events and incidents in a timely manner.
- viii. Review and assess risks associated with exceptions/deviations to the approved cyber and technology policies and procedures and gain senior management approval for risk assessments.
- ix. Review periodically the approved exceptions/deviations to ensure the residual risks remain at an acceptable level.
- x. Reporting to the CEO on an agreed interval but not less than once per quarter on the following:
 - Assessment of the confidentiality, integrity and availability of the information systems in the institutions.
 - Detailed exceptions to the approved cyber and technology policies and procedures.
 - Assessment of the effectiveness of the approved cybersecurity program.
 - All material cyber and technology events that affected the institution during the period.
- xi. Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.
- xii. Incorporate the utilization of scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.

- xiii. Ensure frequent data backups of critical IT systems (e.g. real time back up of changes made to critical data) are carried out to a separate storage location.
- xiv. Ensure the roles and responsibilities of managing cyber risks, including in emergency or crisis decision-making, are clearly defined, documented and communicated to relevant staff.
- xv. Continuously test disaster recovery and Business Continuity Plans (BCP) arrangements to ensure that the institution can continue to function and meet its regulatory obligations in the event of an unforeseen attack through cyber-crime.
- xvi. Safeguarding the confidentiality, integrity and availability of information.

3.2 Regular Independent Assessments and Tests

The understanding of the cyber threat landscape within institutions requires a collaborative approach that encompasses the following functions: Risk Management, Internal Audit and External Audit. Institutions should conduct an **independent** assessment of their cyber environment leveraging on sufficient cybersecurity expertise to assist in understanding their cyber threat landscape. Institutions should carry out an independent cyber threat test at least once a year in addition to the routine two-year Information Technology audits by the external auditors.

3.2.1 Role of Risk Management Function

This comprises risk, control, and compliance oversight functions which ultimately ensure that an institution's management of data, processes, risks, and controls are effectively operating. Risk management has the duty to ensure that cyber and technology risks are managed within the enterprise risk management portfolio. The institution's risk management function should include and is not limited to the tasks below:

- i. Identify threats to information assets; (ii) identify vulnerabilities that could be exploited by the threats; (iii) identify existing controls; and (iv) identify potential consequences in various scenarios should threats exploit vulnerabilities.
- ii. Take into consideration financial, operational, legal, reputational, and regulatory factors when identifying potential consequences.
- iii. Institute a process for assessing and monitoring changes in risk.
- iv. Assessing the cyber and technology risks and determining whether they are aligned with the institution's risk appetite and comprise a material risk for which a capital allocation should be made as part of the internal capital adequacy assessment process.
- v. Monitoring current and emerging risks and changes to laws and regulations.
- vi. Collaborating with system administrators and others charged with safeguarding the information assets of the institution to ensure appropriate control design.
- vii. Maintain comprehensive cyber risk registers: Key cyber and technology risks should be regularly identified and assessed. Risk identification should be forward looking and include the security incident handling.
- viii. Ensure implementation of the cyber and technology risk management strategy.
- ix. Ensure that a comprehensive inventory of Information assets, including their ownership and the roles and responsibilities of the staff managing these assets, classified by business criticality, is established and maintained. A Business Impact Analysis process is in place to regularly assess

- the business criticality of Information assets.
- x. Quantify the potential impact by assessing the residual cyber risk and considering risks that need to be addressed through insurance as a way of transferring cyber risk.
- xi. Reporting all enterprise risks consistently and comprehensively to the board to enable the comparison of all risks equally in ensuring that they are prioritized correctly.

3.2.2 Role of Internal Auditors

- i. All institutions to incorporate qualified Information and Communication Technology (ICT) Auditors within the Internal Audit team. ICT Auditors can be outsourced or on permanent employment. The institution's internal ICT auditors should then ensure that the audit scope includes and is not limited to the tasks below:
- ii. Identify a comprehensive set of auditable areas ("audit universe") for Cyber and technology risk to perform an effective risk assessment during audit planning.
- iii. Continuously review and report on cyber risks and controls of the ICT systems within the institutions and other related third-party connections.
- iv. Assess both the design and effectiveness of the cyber and technology risk management framework implemented.
- v. Ensure regular independent threat and vulnerability assessment tests are conducted.
- vi. Report to the board the findings of the assessments.
- vii. Align the scope and frequency of audits with the criticality and risk profile of the information assets, functions, and processes.

3.2.3 Role of External Auditors

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

- i. Obtaining an understanding of the institution's IT infrastructure, use of IT, operations and the impact of IT on financial reporting statements.
- ii. Understanding the extent of the institution's automated controls as they relate to financial reporting. This should include an understanding of:
 - IT general controls that affect the automated controls.
 - Reliability of data and reports used in the audit that are produced by the institution.
- iii. Conduct independent threat and vulnerability assessment.
- iv. Comprehensive review of the approved cyber and technology strategy and policy.
- v. Conduct comprehensive penetration tests on demand and at least once every two years
- vi. Report at on demand and least once every two years to the Board and Bank of Uganda on the findings of the assessments.

3.3 Outsourcing

Institutions are rapidly expanding their reliance on outsourcing, cloud providers and other services that are time saving and reduce operation costs. However, with this trend, risks such as cyber risk could also emanate. Institutions should therefore ensure that their third-parties comply with legal and regulatory frameworks as well as the international best practices. Generally, institutions should:

- ✓ Policies that govern outsourcing arrangements.

- ✓ Have in place adequate governance of outsourcing agreements including due diligence on prospective service providers, documented outsourcing agreements and adequate monitoring of service delivery.
- ✓ Consider all Information and Communication Technology outsourcing agreements as critical infrastructure for regulation and protection for purposes of security of the banking sector and the economy at large. Select their vendors based on compliance and risk assessments.
- ✓ Ensure all computing resources are secured including registrations, licensing, compliance and verification.
- ✓ Ensure all outsourcing contracts require service providers to comply with applicable legal and regulatory frameworks.
- ✓ Understand the inherent risk arising from each third party.
- ✓ Perform analytics on an institution's outsourcing portfolio to understand which pose the most relative risk to an institution and determine how that risk may translate into a capital allocation in accordance with its ICAAP.
- ✓ Work collaboratively with third parties to mitigate risks that pose the most risk to an institution.
- ✓ Monitor contracted third parties for changes in their business and cyber posture including expansions, divestitures, breaches and new attacks that may alter the third parties' exposure. Service Level Agreements should have robust provisions in relation to security, service availability, performance metrics or penalties.
- ✓ Develop exit management strategies and contingency plans.
- ✓ Should maintain, on an ongoing basis, a register of all its third-party service providers (including cloud services).
- ✓ To access compliance with this guidance, contracts should explicitly reserve the right for the BOU or its designees to access vendor facilities directly involved in delivering outsourced services or possess internationally recognized and accredited certificates.

3.4 Cloud Computing

- ✓ The BOU must be notified of plans to contract with Cloud Service Providers (CSPs) for delivering or materially supporting the delivery of critical services, with sufficient lead time of at least three months (90 calendar days). This way BOU has adequate time to perform a risk assessment and conduct an adequacy assessment of terms and conditions under which a CSP shall be contracted, prior to granting a No-Objection.
- ✓ In the aforementioned notification and request for no objection, there must be attached the following at a minimum: a comprehensive risk register for the CSP services being contracted for; risk mitigation measures for each of the risks in the Risk Register; and capital to held or being set aside by the financial institution that adequately covers the financial implications of any and all residual risk arising from contracting with a CSP.
- ✓ The use of cloud-based services should be approved by the board, and a register of all cloud services used by the institutions for business functions should be available at all times.
- ✓ The board and institutions must understand and discharge their responsibilities regarding the security of cloud resources under the institution's own control ("security in the cloud"), whilst obtaining independent assurance that there is adequate CSP commitment and capacity regarding the security of the infrastructure of said cloud resources ("security of the cloud").
- ✓ The institutions must retain logical access over the location of stored and processed financial and

personal data within CSPs.

- ✓ Cloud-based storage and processing of financial and personal data must be restricted to jurisdictions with laws or international treaties that ensure the same level of protection for financial and personal data as domestic legislation.
- ✓ The institutions must require the CSP to comply with relevant local and international data protection and privacy laws before sub-contracting parts of the outsourced service.
- ✓ The institutions must require the CSP to ensure strict logical separation of its data and virtualized resources from other CSP tenants.
- ✓ All SFIs must ensure that they have in place In-country Primary Data Centers and Disaster Recovery Sites as stipulated in the Bank of Uganda Directive date **5 November 2015**.

3.5 Training/Awareness

- Institutions should implement IT security awareness training programs to make the Board and staff aware of the applicable laws, regulations, and guidelines pertaining to the use of, and access to, information assets. The programs should provide information on good IT security practices, common threat types and the institution's policies and procedures. The training should be provided to all employees including senior management and the board.
- A formalized plan should be put in place to provide ongoing technical training to cybersecurity specialists within the institution.
- Cyber and technology 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.
- The training program should be periodically reviewed to ensure its contents remain current and relevant. The review should take into consideration changes in the FI's IT security policies, prevailing and emerging risks, the evolving cyber threat landscape, lessons learned from previous training initiatives, and any training needs identified through behavioral observations (e.g. unannounced phishing tests on staff)".

3.6 Secure Software Development Lifecycle and Project Management

SFIs should :

- ✓ Establish a project steering committee for major projects to ensure effective oversight and governance
- ✓ Implement a project management framework covering policies, standards, procedures, processes, and activities from project initiation to closure
- ✓ Maintain detailed IT project documentation, including business case, scope, budget, milestones, activities, deliverables, and roles and responsibilities.
- ✓ Establish standards and procedures for vendor evaluation and selection based on the criticality of project deliverables
- ✓ Establish an SDLC framework defining processes, procedures, and controls in each phase
- ✓ Incorporate security specifications, perform continuous security evaluation, and adhere to security practices throughout the SDLC
- ✓ Involve the IT security function in each phase of the SDLC
- ✓ Establish a methodology for comprehensive system testing, including business logic, system function,

security controls, and performance.

- ✓ Track and remediate issues and software defects discovered during source code review and testing
- ✓ Establish safeguards for secure API development and provisioning.

3.7 IT Services Management

SFIs should :

- ✓ Establish a robust framework for supporting IT services and operations, including processes for configuration management, change management, incident management, and problem management.
- ✓ Develop comprehensive operations manuals to enable skilled staff to perform routine activities and run IT operations with minimal disruption.
- ✓ Implement physical security controls for all IT infrastructure, including access controls, surveillance, and protection against environmental threats and conduct periodic audits of physical security.
- ✓ Segregate duties for software development, testing, and release. Manage SaaS through encryption, access management, and security monitoring.
- ✓ Maintain accurate hardware and software configuration information. Use standardized configurations when possible.
- ✓ Avoid using outdated and unsupported hardware or software. Monitor end-of-support dates and develop refresh plans.
- ✓ Establish a process to ensure timely implementation of patches based on criticality. Test patches before applying to production.
- ✓ Assess, test, review, and approve changes before implementation. Conduct risk analysis, test thoroughly, and establish rollback plans.
- ✓ Establish a framework to quickly restore affected IT services or systems to a secure and stable state. Define processes for handling incidents, emergency changes, and evidence collection.
- ✓ Record solutions to incidents in a knowledge base. Determine and resolve root causes to prevent recurrence.
- ✓ Establish policies for identity and access management, including password controls, multi-factor authentication, and access provisioning based on roles and responsibilities. Conduct periodic access reviews.
- ✓ Secure the network using various methods, including but not limited to, firewalls, network segmentation, and access controls. Regularly review network architecture and access rules.
- ✓ Develop data loss prevention policies and implement measures to detect and prevent unauthorized access, modification, or transmission of confidential data. Encrypt data at rest and in transit.
- ✓ Establish robust security standards across all virtualization solution components. This includes: implementing strict access controls around/for administrative access to hypervisors and host operating systems; defining and enforcing policies governing the entire lifecycle of virtual images and snapshots, from their creation through to destruction in order to safeguard against unauthorized access or viewing or modification.
- ✓ Conduct risk assessments and implement appropriate security measures for BYOD environments when applicable.
- ✓ Establish procedures for secure disposal of Information assets, considering data privacy and environmental aspects.

3.8 Cyber Security Operations

SFIs should :

- ✓ Establish processes to collect, analyze, and share cybersecurity-related information, including participation in collaborative industry or national information sharing networks. Procure cyber intelligence monitoring services and actively engage in timely and actionable cyber threat information-sharing arrangements with trusted parties.
- ✓ Implement continuous monitoring, detection, and response capabilities through a security operations center, managed security services, or dedicated functions. Define processes, roles, and responsibilities for security operations, including pre-authorized delegated authority for emergency actions.
- ✓ Establish a process to collect, review, and retain system logs to facilitate security monitoring and digital forensics. Define a baseline of minimum logging requirements and protect logs against unauthorized access. Establish baseline profiles of IT systems' routine activities and analyze system activities against these profiles to identify anomalies. Correlate multiple log events to detect suspicious activity patterns and promptly escalate them to relevant stakeholders.
- ✓ Develop a cyber incident response and management plan integrated with wider crisis response plans. The plan should outline procedures to isolate and neutralize threats, securely resume affected services, investigate breaches, and identify security deficiencies. Leverage cyber intelligence and lessons learned from incidents to enhance controls and improve the incident management plan.

3.9 Response and Recovery

SFIs should :

- ✓ Establish a robust business continuity management process to ensure the ongoing provision of services, meet availability goals, and minimize losses during severe business disruptions. Conduct business impact analysis (BIA) to assess exposure to and impact from disruptions, considering various scenarios and the criticality of business functions, processes, third parties, and information assets.
- ✓ Align system recovery time and recovery point objectives with BIA results and ensure ICT systems' availability features are consistent with the BIA. Develop documented and management-approved business continuity and disaster recovery plans that consider risks to ICT systems and services and coordinate with relevant stakeholders during plan development.
- ✓ Train staff on the plans and update and test them at least annually or after significant changes in ICT systems or business processes. Involve relevant stakeholders in testing, which should cover various plausible disruption scenarios and address recovery dependencies among information assets, including those managed by third parties.
- ✓ Define policies and procedures for regular backups and data archival to enable recovery from system disruptions, data corruption, or deletion. Implement a strategy to manage the backup data lifecycle, considering backup frequency, retention period, storage management, and secure destruction of backup media. Consider air-gapped backups to address ransomware risks and periodically test backup restoration procedures. Secure confidential data in backups and store redundant copies of critical data at separate secure locations.

- ✓ Conduct threat and vulnerability risk assessments (TVRA) for data centers to identify vulnerabilities, weaknesses, and protective measures against physical and environmental threats. Ensure adequate redundancy for power, network connectivity, cooling, and other critical systems to eliminate single points of failure. Implement fire detection and suppression systems and establish geographically separated primary and secondary data centers.
- ✓ Monitor data center physical security and environmental controls 24/7 and establish appropriate escalation and response plans for incidents. Implement strict physical access controls, including need-based access, visitor protocols, and segregation of delivery and common areas from sensitive areas.
- ✓ Develop an Incident response and tracking Matrix, that clearly delineates accountable persons, actions taken or to be taken, timelines for each expected action etc.

3.10 Security Testing and Remediation

SFIs should :

- ✓ Establish a process for regular vulnerability scanning based on the criticality of the IT system and its associated security risks.
- ✓ Conduct penetration testing to understand the effectiveness of cyber security defenses. Perform penetration tests on externally facing digital services at least annually and after any significant changes to the underlying systems.
- ✓ Carry out penetration testing to obtain an in-depth evaluation of its cyber and technology defences. A combination of black box and grey box testing should be conducted in this regard.
- ✓ Carry out regular cyber exercises to validate incident response and recovery procedures, including communication plans.
- ✓ Involve relevant stakeholders, such as senior management, business units, corporate communications, crisis management teams, service providers, and technical staff.
- ✓ Establish a comprehensive remediation process to track and resolve issues identified through vulnerability scanning, penetration testing, and cyber exercises.
- ✓ Include severity assessment and classification of issues, timeframes for remediation based on severity, and risk assessment and mitigation strategies for deviations from the framework.

SFIs are encouraged to :

- ✓ Perform red team exercise to validate the effectiveness of cyber and technology defense and response plans against prevalent threats and incidents.
- ✓ Define objectives, scope, and rules of engagement before commencing the exercise and conduct it in a controlled manner.
- ✓ Design the exercise scenario using relevant threat intelligence to identify likely threat actors, tactics, techniques, and procedures.

3.11 Identity Management

It is easier for an external or internal threat actor to gain unauthorized access to an SFI's assets or data by using valid user credentials rather than “hacking” the environment. Furthermore, every incident must clearly account for the perpetrators. Therefore, SFIs shall strive to properly account for digital identities paying keen attention to.

- i. Establish and maintain an inventory of all accounts/digital identities managed in the organization and continuously validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
- ii. Enforce non-repudiation techniques e.g. multi factor authentication for digital identities accessing data classified as sensitive or performing high risk or high value transactions.
- iii. Manage digital identity permissions and privileges in a manner that restricts access to defined roles and responsibilities following a least privilege principle.
- iv. Establish processes that manage the lifecycle of a digital identity from creation, maintenance to expiry and removal.

3.12 Personal Data Protection and Privacy

Data Privacy & Protection Act (2019) protects the privacy of the individual by regulating the collection and processing of personal information and provides for the rights of the persons whose data is collected and the obligations of data collectors, data processors and data controllers. In addition, Uganda has ratified several international human rights instruments:

In keeping with the data protection and privacy legal and regulatory framework SFIs shall:

- i. Collect and process personal data using lawful, transparent and fair means and with the knowledge or consent of the data subject.
- ii. Limit the collection of personal information to what is directly relevant and necessary to fulfill organizational data needs and regulatory requirements, i.e. SFIs should collect the minimum amount of data they require for their intended processing operation; and should never collect unnecessary personal data.
- iii. Personal data must be collected for specified, explicit and legitimate purposes, which are determined at the time of the collection of the personal data, and not be further processed in a manner that is incompatible with those purposes.
- iv. Personal data must be processed in a manner that ensures the appropriate level of security and confidentiality for the personal data, including protection against unauthorized or unlawful processing and against accidental loss.
- v. Designate a person as the data protection officer responsible for ensuring compliance with Data Protection and Privacy Act.

3.13 Data Security and Management

- i. Establish and maintain a documented data management process that addresses data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and

retention standards.

- ii. Establish, maintain, review and update a data inventory with a priority on sensitive data.
- iii. Securely dispose of data in a manner that is commensurate with data sensitivity.

3.14 Cryptography

- i. SFIs shall develop and implement processes and tools to securely create and manage cryptographic keys used to protect data on its assets.
- ii. The bank shall ensure that cryptographic keys are generated with secure cryptographic techniques.
- iii. Cryptographic keys shall be stored in secure tamper proof locations and only retrieved during usage.
- iv. The bank shall provide mechanisms with which parties can verify validity and authenticity of cryptographic keys.

3.15 Cybersecurity Supply Chain Risk Management

SFIs shall

- i. Perform thorough due diligence on prospective suppliers that is consistent with procurement planning and commensurate with the level of risk, criticality, and complexity of each supplier relationship.
- ii. Assess the suitability of the technology and cybersecurity capabilities and the risk management practices of prospective suppliers.
- iii. Conduct supplier risk assessments against business and applicable cybersecurity requirements, including lower-tier suppliers and the supply chain for critical suppliers.
- iv. Assess the authenticity, integrity, and security of critical products prior to acquisition and use.

PART IV: Reporting

- a) SFIs are required to revise their Cyber and technology risk management Policies, strategies and frameworks within one month following approval of the revision by the Board.
- b) SFIs should forward to the Bank of Uganda all cyber and technology risk incidents, which have significant and adverse impact on the institution's ability to provide adequate services to its customers, its reputation or financial condition. This should be time bound - within 24 hours (**Annex I**).
- c) On a quarterly basis, SFIs should report all occurrences of cyber and technology incidents and how they handled them (**Annex II**).
- d) SFIs shall submit a report on all testing exercises, including vulnerability assessments, scenario-based testing exercises, penetration tests and red team tests, conducted during the previous calendar year, on an annual basis, by the end of the first quarter of each year.
- e) On an annual basis, SFIs to perform and provide to the Bank of Uganda, by the end of first quarter, a self-assessment on cyber and technology risks. The self-assessment on risks should include (i) inherent risk profile (ii) a measurement of the risk exposure / quantity of risk; (iii) individual

assessment of the effectiveness of (a) the board, (b) executive management, (c) operational management, (d) risk management, (e) compliance, (f) internal audit and (g) external audit; (iii) assessment of the direction (increasing, decreasing or stable) of the cyber and technology risk for the year.

- f) On receipt of this guidance, the SFIs shall undertake a gap analysis and provide a detailed report on its compliance status to the Bank of Uganda within **180 calendar days**, along with the timeline for achieving compliance with the mandated requirements. For each requirement, the SFIs shall indicate its compliance status using four categories: (i) compliant, (ii) partially compliant, (iii) non-compliant, and (iv) not applicable. For the “partially compliant” and “not applicable” categories, an explanation of the reasons is necessary.

ANNEXES

ANNEX I: Cyber and technology Incident Record (*Immediate*)

[Insert Name of participant]

[Insert Date and Time of reporting]: Date..... Time.....

Date of Incident	Time of Incident	Nature of Incident (Chronological order of events)	Impact Assessment

Submit the cyber and technology incident report within 24 hours after a cyber and technology incident(s) to the Bank of Uganda, Supervision Department.

Signed for and behalf of

By the duly authorized Signatories

Name.....

Designation.....

Signature

Name

Designation

Signature

ANNEX II: Cyber and technology Incident Record (*Quarterly*)

[Insert Name of participant]Quarter.....

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

Submit this report on the 5th day after the end of every quarter to the Bank of Uganda, Supervision Department.

Signed for and behalf of

By the duly authorized Signatories

Name.....

Designation.....

Signature

Name

Designation

Signature