STANDARD OF SOUND PRACTICE

MANAGEMENT OF CYBER RISKS

Table of Contents

01 Background and Context

Cyber threats and incidents to the financial sector in Jamaica, and globally, pose a serious hazard to financial stability.

This Standard of Sound Practice on the Management of Cyber Risks ("Guidelines") is intended to establish minimum standards and guidelines on the management of cyber risk for the licensees under the Banking Services Act, 2014. Each licensee is expected to put an effective framework in place to manage the cyber risk exposures inherent in their operations, which could also result in significant financial loss, legal liabilities and reputational damage.

1.0 Legal Basis

1.0.1 Bank of Jamaica conducts risk-based examinations of licensees in accordance with section 34D of the Bank of Jamaica Act, to assure compliance with standards set out herein on the management of cyber risks. These Guidelines are issued pursuant to section 132(1)a of Banking Services Act. (See Appendix 1: Cyber Risk Related Legislation)

1.1 Context

1.1.1 **It is important for deposit-taking institutions ("DTIs") to understand and manage their cyber risk to protect their assets, operations and information entrusted to them by customers and stakeholders.** This is to build trust and confidence, which are two of the most important attributes of a financial sector.

1.1.2 **Cyberattacks are becoming more frequent, and they continue to evolve** in terms of their complexity and sophistication. A successful cyberattack could have a debilitating impact on a DTI which could cause a significant financial or operational impact on a financial institution.

1.1.3 **Cyber threats i.e. risks from hacking, malware, phishing, and other types of cyberattacks, as well as from insider threats, can have significant financial loss, reputational damage, and loss of sensitive information**, each of which negatively impacts customers, employees, shareholders, suppliers and threatens stability of the financial system and wider economy.

02 Definitions

For the purpose of these Guidelines, the following definitions are provided:

Critical Operations	Systems and processes, the failure of which will cause significant disruption to the DTI's operations or materially impact the DTI's service to its customers.
Cyber Incident	Any observable occurrence in an information system that i. jeopardizes the cybersecurity 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.
Cyber Resilience	The ability to recover quickly and deliver intended services and outcomes despite cyber incidents.
Cyber Risk	Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a system via electronic means from the unauthorized access, use, disruption, modification, or destruction of the system.
Cyber Risk Governance	The arrangements put in place by the Board to establish, implement and review its approach to managing cyber risks and support cyber incident response and recovery activities toward cyber resilience.
Cyber Risk Management Framework	A structured approach to identify, assess, and mitigate potential cyber threats to an organization. It involves establishing clear roles and responsibilities, defining risk tolerance levels, and implementing controls along with others policies, frameworks, guidelines and standards to minimize the likelihood and impact of cyber-attacks.
Cybersecurity	(a) The systems, technologies, processes, governing policies and human activity that an organization uses to safeguard its digital assets. (b) The practice of protecting critical systems and sensitive information from digital attacks, whether those threats originate from inside or outside of an organization. (c) 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.

03 Cyber Risk Governance

3.0 Preamble

3.0.1 **Cyber Risk Governance refers to the arrangements put in place by a board to ensure the effective management of cyber risks** through:

- *the establishment of a comprehensive cyber risk management framework to inform their cybersecurity strategy. (See Section 4: Overseeing the Cyber Risk Management Framework)*
- *the creation of cyber risk aware culture towards a cyber-resilient organisation.* (Section 6: Tone at the Top- Cyber Risk Aware Culture)
- *regular reports on cybersecurity effectiveness and threat intelligence for shared cyber resilience.* See Section 5: Key Reports to the Board)

3.0.2 **Strong cyber risk governance is essential to a DTI's implementation of a systematic and proactive approach to managing the prevailing and emerging cyber threats that it faces**. It also supports efforts to appropriately consider and manage cyber risks exposure of an organization and to provide appropriate resources and expertise to deal with these risks.

3.0.3 **Cyber risks are characterised by their stealthy nature, intricate sophistication and prolonged persistence** that have the capacity to trigger extensive disruptions not only within a financial institution's network but also throughout the broader financial system.

3.0.4 **The DTI's Board of Directors ("The Board") is expected to ensure the strategies and measures in a DTI's cyber risk management framework** is not restricted to securing the viability of its information technology operations alone, but should also cover people, processes, data, facilities and testing. *(See Appendix 2: Cyber Resilience Principle 1: Not Just an IT Issue)*

3.1 Board Oversight of Cyber Risks

3.1.1 **The Board <u>must</u> have full oversight of the institution's framework for management cyber risks.** *(See Appendix 3: Cyber Risk Oversight Expectations and Questions to Ask)*

3.1.2 **The Board <u>must</u>** ensure the creation of a cyber risk-aware culture throughout the organization. *(Section 6: Tone at the Top- Cyber Risk Aware Culture)*

3.1.3 **The Board, individually and collectively, must understand the seriousness of the cyber threat environment.** It should ensure that it collectively possesses the appropriate balance of skills, knowledge and experience to understand and assess the cyber risks facing the DTI. It should also be sufficiently informed and capable of credibly challenging the recommendations and decisions of designated senior management.

3.1.4 **The Board and Senior Management must have an ongoing programme to assess any gaps in the knowledge and expertise** of the Board and management and to implement initiatives to address these gaps. That is, the Board and Senior Management team shall be appropriately constituted with representatives who have an appreciation of cyber risk management and programme implemented to ensure all members undergo continuous training.

3.1.5 **The Board must review and approve a cyber risk management framework, which should at minimum incorporate four lines of defence:**

1. *The First Line of Defence:* Business units that own and manage cyber and IT-specific risks.
2. *The Second Line of Defence.* The Risk Management function that oversees cyber and IT-specific risks.
3. *Third Line of Defence:* The Internal Audit function that provides independent assurance over cyber and IT-specific risks.
4. *Fourth Line of Defence:* Information sharing arrangements and independent external assurance over cyber and IT-specific risks.

3.1.6 **The Board should be responsible for setting the DTI's risk tolerance for cyber risks and for closely overseeing the DTI's implementation of its cyber risk management framework** and the policies, procedures and controls that support the continuity of critical operations[1] and core business lines. *(See Section 4: Overseeing the Cyber Risk Management Framework)* This should incorporate interconnected factors associated with third-party dependencies (supply chain, procurement and outsourcing). *(See Section 4.3 Third Party Dependencies)*

3.1.7 **The Board and Senior Management should ensure that cyber risk, implementation of the cyber risk management framework and any associated issues appear regularly on the Board's meeting agenda.** Boards should have adequate access to cybersecurity expertise (whether internal or external), and discussions about cyber risk management should be given adequate time on the Board's meeting agenda. *(See Section 5.1: Board Reports on Cybersecurity Effectiveness, and refer to Appendix 2: Cyber Resilience Principle 3: Attention on the Agenda)*

3.1.8 **The Board is expected to play a key role in assessing the effectiveness of the above and empowering management to take decisions to deploy such activities**. This is important to ensure board oversight of cyber risks remains

[1] The term "critical operations" means systems and processes, the failure of which will cause significant disruption to the DTI's operations or materially impact the DTI's service to its customers.

effective in accordance with corporate governance principles. *(See Corporate Governance: Board Oversight Handbook on BOJ website)*

3.1.9 **The Board must review, deliberate and challenge the cyber risk information contained in the reports from sub-committee.** Evidence of this deliberation and decision-making must be documented in relevant board minutes. It is not sufficient to circulate reports from the sub-committees for individual members to read at their convenience.

04 Overseeing the Cyber Risk Management Framework

4.0 Preamble

4.0.1 **A Cyber Risk Management Framework is a structured approach** to identifying, assessing, and mitigating potential cyber threats to an organization. It involves establishing clear roles and responsibilities, defining risk tolerance levels, and implementing controls to minimize the likelihood and impact of cyberattacks. *(See Appendix 4: Types of Cyber Attacks)*

4.0.2 **Critical to the design of a Cyber Risk Management framework is defining the accountabilities for the four lines of defence:** Operational Management, Risk Management, Internal Audit along with Information Sharing & External Assurance.

4.0.3 **Starting with the first line of defence, DTIs must have an operational framework in place to:**

- *design an appropriate structure with roles, responsibilities and expertise to manage cyber risks effectively, outlined in Sections 4.1 to 4.2.*
- *incorporate third-party dependency factors within the framework, outlined in Section 4.3.*
- *assess their exposure and susceptibility to cyber risks, threat factors and events, outlined in Section 4.4.*
- *establish internal controls which manage the impact of cyber risks, outlined in Section 4.5.*
- *monitor and report on cyber risks to the relevant stakeholders, outlined in Section 4.6.*

First Line of Defence: Operational Management

4.1 Structure and Expertise

4.1.1 **Senior Management must ensure that there is an appropriate organisational structure** in place, equipped with adequate resources and cyber expertise to manage cyber risks effectively**.**

4.1.2 **These may include relevant enterprise-wide committees, functions and/or designated officers** with the requisite expertise to perform the responsibilities of a:

- *Chief Information Officer (CIO) or equivalent*
- *Chief Information Security Officer (CISO) or equivalent*
- *Cyber Incident Response & Recovery (CIRR) function or equivalent*
- *Project Management Office (PMO) or equivalent.*

4.1.3 **Senior Management should carry out due diligence in the selection of staff, vendors and contractors that includes** comprehensive and effective screening processes and security clearance checks. This is crucial to minimizing cyber and IT-specific risks due to internal sabotage or fraud.

4.1.4 **Senior Management should ensure all employees participate in mandatory cybersecurity awareness programmes**, as one uninformed employee can be the weakest link. Typical cybersecurity awareness programmes include topics such as password policy, multi-factor authentication, social engineering, phishing and mobile device security.

4.2 Roles and Responsibilities

4.2.1 **The responsibilities of Senior Management include:**

- *Establishing a sound, robust and enterprise-wide cyber risk management process to manage cyber risks in relation to business objectives, risk appetite and regulatory requirements.*
- *Using leading international, national and industry-level standards, guidelines or recommendations, reflecting current industry best practices in managing cyber threats, as a benchmark for designing its cyber resilience framework and incorporating the most effective cyber resilience solutions.* *(Appendix 5: Industry Standard on Cybersecurity)*
- *Developing a Cybersecurity Strategy that is informed by the cyber risk management process, to build the DTI's cybersecurity capabilities to prevent, monitor and defend against cyber-attacks that attempt to access, change, or destroy data; extort money from users or the organization; or aim to disrupt normal business operations.*
- *Ensuring the DTI's cybersecurity preparedness strategy is in alignment with the institution's overall business strategy, as well as, monitoring and evaluating existing and future trends in technology that may impact the business strategy, including monitoring of overall industry trends.*
- *Ensuring that effective internal controls are implemented to protect against cyber threats and achieve reliability, resiliency and recoverability of critical infrastructure, IT systems, data and other digital assets*

- *Ensuring cybersecurity awareness and training is conducted enterprise-wide especially to personnel engaged in critical operations and core business lines, including those from third-parties and adequately train them to perform their information security-related duties and responsibilities consistent with related processes and agreements.*
- *Establishing and enforcing cyber hygiene practices and providing continuous cybersecurity training as technologies change and the threat landscape evolves. This helps to remind employees of their role and responsibility to keep the organization safe.*
- *Implementing policies, procedures and controls that support cybersecurity preparedness and cyber incident response and recovery (CIRR) activities.*
- *Engaging with business and technical functions within the organisation to develop, exercise, maintain, manage, support and improve CIRR objectives and plans consistent with organisational needs.*
- *Informing members of the Board promptly or within 72 hours of any cyber or IT-specific vulnerability, threat, issue or incident that may have a significant impact on the DTI, its suppliers, customers or the greater financial system.*

4.2.2 **The responsibilities of the Chief Information Officer (CIO) should include, but not limited to:**

- *Overseeing all aspects of information technology (IT) and information systems.*
- *Leading the digital transformation strategy or technology innovation programme to improve digital capabilities of the organisation.*
- *Ensuring that information security and data protection is aligned with business strategy and objectives.*

4.2.3 **The responsibilities of the Chief Information Security Officer (CISO) should include, but not limited to:**

- *Developing Cybersecurity Preparedness Strategy and overseeing the programme and ensuring continuous alignment with business objectives.*
- *Managing cyber risk management processes*
- *Enforcing cybersecurity policies*
- *Ensuring adequate resources are in place*
- *Ensuring security metrics and monitoring are implemented and carried out.*
- *Keeping abreast of cyber threats and keeping the Board informed to understand the risks and related dependencies.*
- *Ensuring the roles of data owner, data custodian and user are clearly defined, assigned and administered.*

4.2.4 **The roles within the Cyber Incident Response & Recovery (CIRR) Function should include, but not limited to:**

- **Incident coordinator.** *DTIs should identify an individual or a team to coordinate actions and communications for a cyber incident. The designated incident coordinator or team minimises the potential for CIRR respondents to receive conflicting orders or information from different stakeholders, thereby improving the flow of information and aiding the coordination of response and recovery efforts.*
- **Executive sponsor.** *Management should demonstrate commitment by creating an organisational environment where staff are encouraged to report or escalate cyber incidents to management.*

4.2.5 **Relevant responsibilities of the Portfolio/Programme/Project Management Office (PMO) should include, but not limited to:**

- *Providing centralized coordinated management and support for technology-related projects and change management initiatives in the organization*
- *Leveraging strategic partnerships for adaptive programme coordination and delivery, resource management, risk mitigation and effective organization management to deliver CISO-driven requirements.*
- *Developing and managing procedures, policies, templates, and other documentation shared by the projects.*
- *Auditing projects to ensure compliance with set standards, including IT security, data security, data protection standards.*
- *Coordinating communication across technology-related projects to assure strategic alignment and benefits realisation.*

4.2.6 **Programmes and projects supporting the Cybersecurity Preparedness Strategy should address focus areas such as:**

- **Network security.** *Security measures for protecting the underlying networking infrastructure (both wired and wireless) from unauthorised misuse, or theft. It involves creating a secure infrastructure for devices, applications, users to work in a secure manner.*
- **Application security.** *Security measures that help protect applications operating on-premises, mobile and in the cloud. Security and privacy considerations should be built into applications at the design stage, with considerations for how data is handled and users are authenticated.*
- **Storage security.** *Security measures to assure the physical and digital security of data storage facilities including storage redundancies of encrypted, immutable and isolated data copies to support recovery, minimizing the impact of a cyber-attack.*
- **Cloud security.** *Security measures used to protect applications, data, and infrastructure hosted by external data centres owned by third-party providers or cloud service providers (CSPs). This includes applying security policies, practices, controls, and other technologies such as identity and access management and data loss prevention tools to help secure cloud environments including access,*

transfer, migration of data or applications or infrastructure between the cloud and/or other environments.

- **Information security.** *Data protection to secure vital, sensitive or personally identifiable information, digital or physical, from unauthorized access, exposure, or theft.*
- **Cybersecurity awareness and training.** *Building cybersecurity awareness across the organization to educate individuals within the organisation to recognize and mitigate cyber threats, thereby enhancing overall security. For example, users can be trained to delete suspicious email attachments, avoid using unknown USB devices, etc.*
- **Business continuity and disaster recovery planning***. Tools and procedures for responding to unplanned events, such as system or network failures, natural disasters, power outages, or cyber incidents, with minimal disruption to critical operations.*
- **Emerging technologies.** *Security measures and privacy considerations in the design, development and testing of emerging technologies such as artificial intelligence, machine learning and quantum computing, etc.*

4.3 Third-Party Dependencies

4.3.1 **Sound risk management practices to identify and mitigate cyber risks include third-party service provider dependencies.**

4.3.2 **The DTI must engage in robust planning and due diligence to identify risks related to third-party service providers** and establish processes to measure, monitor, and control the risks associated with them. The process for risk identification and monitoring controls effectiveness may include testing or auditing of security controls with the third-party e.g. Service Organization Control (SOC) 2 Type 2 with TSP reports[2].

4.3.3 **Before entering new third-party relationships, DTIs must conduct cyber risk assessments** and due diligence to consider whether these relationships are consistent with their cyber strategy.

4.3.4 **Contracts between the DTI and third-parties must be drafted to define clearly which party is responsible** for configuring and managing system access rights, configuration capabilities, and deployment of services and information assets.

4.3.5 **DTIs must employ controls to verify that resilient operational processes are in place** at the third-party and consistent with the DTI's internal standards. This includes verifying and validating that third-party systems used for delivering critical operations and core business lines that will be operational during

[2] SOC 2 (Service Organization Control 2) is a framework developed by the American Institute of Certified Public Accountants (AICPA) to assess and report on the cybersecurity and data protection controls of service organizations. It focuses on five key principles: security, availability, processing integrity, confidentiality, and privacy. SOC 2 audits are conducted by third-party auditors to verify the effectiveness of these controls.

disruptions or able to return to operation in accordance with the DTI's tolerance for disruption.

4.4 Risk Identification and Assessment

4.4.1 **Risk identification entails the determination of the threats and vulnerabilities to a DTI's IT infrastructure** including internal and external networks, hardware, software, applications, third-party services, systems interfaces, operations and human elements throughout the supply chain.

4.4.2 **DTIs should be vigilant in identifying and analysing cyber risks** as it is a crucial step in the risk containment exercise. *(See Appendix 4: Types of Cyber Threats)*

4.4.3 **A cyber risk may take the form of any condition, circumstance, incident or person with the potential to cause harm** by exploiting a vulnerability in a system.

4.4.4 **DTIs should carry out penetration tests** in order to conduct an in-depth evaluation of the cybersecurity posture of the system through simulations of actual attacks on the system. DTIs should conduct penetration tests on internet-facing systems **at least annually**, or whenever these systems undergo major changes or updates. Full scope penetration tests **at least** once every two years.

4.4.5 **DTIs should carry out regular scenario-based cyber exercises** to validate their response and recovery, as well as communication plans in case of a cyber-attack. These exercises could include social engineering[3], table-top[4], cyber range[5] or adversarial attack simulation[6] exercises.

4.4.6 **Based on the type and objectives of the exercise, the DTI should involve all relevant stakeholders** including management, business functions, corporate communications, crisis management team, service providers, and technical staff responsible for cyber threat detection, response and recovery.

4.4.7 **The objectives, scope and rules of engagement should be defined before the commencement of the exercise.** To ensure that the activities executed don't disrupt the DTI's production systems, the exercise **must** be closely supervised and performed in a controlled environment.

4.4.8 **DTIs should bear in mind that the simulation of realistic adversarial simulation attacks** ought to be designed based on plausible cyber-attacks, and

[3] Social engineering is a process in which cyber criminals manipulate an unsuspecting person into divulging sensitive details such as passwords through the use of techniques such as phishing, identity theft and spam.
[4] Table-top exercise is a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
September 2006.
[5] Cyber ranges are interactive, simulated representations of an organization's local network, IT system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and secure environment for product development and security posture testing.
[6] Adversarial attack simulation exercise provides a more realistic picture of a DTI's capability to prevent, detect and respond to real adversaries by simulating the tactics, techniques and procedures of real-world attackers to target people, processes and technology underpinning the DTI's critical business functions or services.

therefore should design the exercises by using threat intelligence that is relevant to their IT environment. This technique facilitates the identification of threat actors who are highly probable to pose a threat to the DTI; as well as to assist in the identification of the tactics, techniques and procedures most likely to be used in such attacks.

4.5 Risk Mitigation and Control

4.5.1 **Mitigating cyber risk is crucial for DTIs to protect their digital assets and maintain operational continuity.** Risk mitigation entails a methodical approach for evaluating, prioritizing and implementing appropriate risk-reduction controls. A combination of technical, procedural, operational and functional controls would provide a rigorous mode of reducing risks. In addition, acquiring insurance coverage for various insurable risks, including recovery and restitution costs should be considered.

4.5.2 **For each type of risk identified, DTIs should develop and implement risk treatment plan including mitigation and control strategies** that are consistent with the criticality of the information system assets and the level of risk tolerance.

4.5.3 **As it may not be practical to address all known risks simultaneously or in the same timeframe, DTIs should give priority to threat and vulnerability pairings** that could cause significant harm or impact to a DTI's operation. The costs of risk controls should be balanced against the benefits to be derived.

4.5.4 **DTIs must manage and control risks in a manner that will maintain their financial and operational viability and stability, paying attention to the design of control standards and control patterns to secure their IT infrastructure**, to mitigate cyber and IT-specific risks based on their risk appetite statement. The control objectives should cover all types of technology and cybersecurity controls which should map to industry standards. (Appendix 5: Industry Standards on Cybersecurity)

4.5.5 **DTIs must constantly monitor their attack surface to identify and block potential threats as quickly as possible.** As DTIs seek to expand their digital footprint and embrace new technologies, every effort should be made to ensure controls implemented are automated and/or can be technically enforced.

4.6 Risk Monitoring and Reporting

4.6.1 **DTIs should maintain a risk register which facilitates the monitoring and reporting of cyber and IT-specific risks.** Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. DTIs should update the risk register periodically, and institute a monitoring and review process for continuous assessment and treatment of risks.

4.6.2 **To facilitate risk reporting to management, DTIs should develop cyber and IT-specific risk metrics to highlight systems, processes or infrastructure that have the highest risk exposure.** An overall cyber and IT-specific risk profile of the organization should also be provided to the Board. In determining the cyber and IT-specific risk metrics, DTIs should consider risk events, regulatory requirements, vulnerability assessments, penetration test results and audit observations. (See Section 5: Key Reports to Board)

4.6.3 **Risk parameters may shift as the IT environment, cyber threat landscape and delivery channels change.** Thus, DTIs should review and update the risk processes accordingly, and conduct a periodic evaluation of risk-control methods that includes an assessment of the adequacy and effectiveness of IT controls and risk management processes.

4.6.4 **Management of the DTI's IT operation should review and update its IT risk control and mitigation approach**, taking into account changing circumstances and variations in the DTI's risk profile and cyber threat landscape.

4.6.5 **DTIs must conduct continuous monitoring of emerging cybersecurity threats** such as denial of service attacks, internal sabotage, and malware infestations to facilitate prompt detection of intrusion attempts, unauthorized or malicious activities by internal and external parties.

4.6.6 **Incidents must be reported promptly to the Bank of Jamaica and appropriate authorities** within 72 hours**. Local authorities may include:**

a) Bank of Jamaica
b) Financial Services Commission
c) Jamaica Cyber Incident Response Team
d) Office of the Information Commissioner
e) Major Organised Crime and Anti-corruption Agency
f) Financial Investigation Division of the Ministry of Finance
g) Jamaica Constabulary Force

Second Line of Defence: Risk Management

4.7 Risk Management Function

4.7.1 **As the second line of defence, the responsibilities of Risk Management function should include:**

- *Monitoring cyber risk as part of operational risk*
- *Facilitating effective risk management and control practices*
- *Proposing the risk tolerance of the institution for approval by the Board*

- *Liaising with the CISO or equivalent to incorporate cybersecurity into overall governance, risk and compliance programme and processes*
- *Reporting risk-related information*
- *Ensuring that a suitable risk treatment plan has been prepared by the first line of defence*

4.7.2 **A financial institution's cyber risk assessment process should be consistent with its enterprise risk management framework.** Such consistency is important, and recognises that a financial institution's cyber risk assessment process is likely to share common elements with the policies, procedures and controls that it has established to manage other areas of risks.

- *Evaluation of cyber risks in a systematic, impact-driven structure from the board level down to control objectives and metric thresholds.*
- *Examples of metrics to measure impact of a cyber risk include:*
  a) Duration of unavailability of critical functions and services
  b) Number of stolen records or affected accounts
  c) Volume of customers impacted
  d) Amount of lost revenue due to business downtime, including existing and future business opportunities
  e) Percentage of service level agreements breached

4.7.3 **DTIs should institute effective risk management practices and internal controls** to achieve data confidentiality [7], information security, reliability, resiliency and recoverability in the organization.

4.7.4 **This process should be updated in response to material changes** in the business model, operating environment and strategic direction.

Third Line of Defence: Internal Audit

4.8 Internal Audit Function

4.8.1 **As the third line of defence, the responsibilities of Internal Audit function should include:**

- *Giving independent assurance that the cybersecurity policies and controls are operating effectively.*
- *Producing audit reports on findings over key information security risks in the environment.*

7 Data confidentiality refers to the protection of sensitive or confidential information such as customer data from unauthorized access, disclosure, etc.

4.8.2 The Internal Audit function should support coordination between independent cybersecurity accessors and relevant regulators to measure the cyber risk governance framework against defined cybersecurity standards, such as NIST Cybersecurity Framework.

Fourth Line of Defence: Information Sharing & External Assurance

4.9 Information Sharing

4.9.1 **Senior Management should establish cyber information sharing arrangements to take in consideration all available threat intelligence** through information sharing and analysis centres established for the financial sector, at the national level, regionally and globally. This includes sharing of cyber threats, incidents and attacks with other financial institutions and local authorities that strengthens overall cyber resilience for the financial sector.

4.9.2 **DTIs should establish an information sharing relationship with the Jamaica Cyber Incident Response Team (JaCIRT)** to align with the national cyber strategy and support testing activities, collective intelligence and coordinated responses to cyber threats and strengthen internal control systems.

4.9.3 **DTIs should establish processes designed to maintain effective situational awareness capabilities** to reliably predict, analyse and respond to changes in its operating environment, cyber threat landscape while maintaining effective incident response.

4.9.4 **DTIs should have a programme for gathering, analysing, understanding, and sharing information about vulnerabilities** and threats to arrive at actionable intelligence. Actionable intelligence can be gathered from various public and private sources.

4.10 External Assurance

4.10.1 **DTIs must report cyber incidents and data breaches promptly to the Bank of Jamaica within 72 hours along with relevant authorities** (See Section 4.6.6)**.** A digital forensics report from an external cybersecurity assessor may be requested.

4.10.2 **DTIs must provide to Bank of Jamaica (BOJ) an annual attestation**, to include areas of weakness, compensating controls in areas of non or partial compliance, as well as initiatives being undertaken to address the concern(s). The yearly attestation shall alternate between a self-attestation or an independent attestation.

- Self-attestation – *The assessment is performed and report prepared by the entities' internal resource which is second or third line of defence (that is, the functions are internal to the institution and does not own and manage any of the*

risk). This shall include; Internal Auditor, Corporate Risk Officer or Compliance Officer.

- Independent Attestation – *The assessment is performed and report prepared by an independent external organization which has existing cybersecurity assessment experience, and individual assessors who have relevant security industry certification(s).*

4.10.3 DTI**s should use the findings from external audits and information sharing activities** to continuously improve its cybersecurity posture, adapting to emerging threats and changing regulatory requirements.

4.10.4 **External reports on vulnerability tests should be provided at <u>least twice yearly</u> and penetration testing at <u>least annually</u>.** Early detection of flaws under real-scenario conditions helps to remediate gaps, evaluate the effectiveness of incident response plans, ensure business continuity and prevent costly data breaches.

05 Key Reports to Board

5.0 Preamble

5.0.1 **Reporting to the Board on cybersecurity effectiveness is crucial** to assure the protection of an organization's digital assets. This should include evaluating:

- *Security breaches and incidents*
- *Vulnerability scanning and penetration testing results*
- *Compliance with regulatory requirements and industry standards*
- *Employee security awareness and training completion rates*
- *Incident response time and effectiveness*

5.0.2 Senior management should regularly provide a written report to the Board on the overall status of its cyber resilience programme and keys risks and issues.

5.0.3 As part of the Board's updates, senior management should provide their budgeting and forecasting activities plan for ongoing and future resource needs to ensure cyber resilience objectives are achieved continually.

5.1 Board Reports on Cybersecurity Effectiveness

5.1.1 **Senior Management should must** provide reports to the Board on cybersecurity effectiveness. Metrics used in board reports should include, but not limited to:

- *Recovery Point Objectives (RPOs) (i.e. the maximum allowable data loss that an organization can tolerate in the event of a disruption)*
- *Recovery Time Objectives (RTOs) (i.e. the maximum allowable downtime that an organization can tolerate for its systems and applications)*
- *Dwell time (i.e. the duration between the time a threat actor has gained access until completely removed)*
- *The number of security incidents detected and resolved within a specific period (e.g., month, quarter, or year).*
- *The percentage of incidents prevented due to proactive security measures, such as endpoint protection, intrusion detection systems, and threat intelligence.*
- *The number of false positives and false negatives generated by security monitoring tools, and how these numbers are being reduced through continuous refinement of the monitoring process.*

- *The level of employee security awareness and the frequency of cybersecurity awareness training programmes.*
- *The frequency of simulated phishing attacks to test phishing attack susceptibility.*
- *The percentage of devices on the corporate network have the latest security patches installed.*
- *The percentage of high-risk vulnerabilities identified that have been resolved.*
- *The number of systems that failed vulnerability scans.*
- *The volume of incidents detected and responded via automation*

06 Tone at the Top – Cyber Risk-Aware Culture

6.0 Preamble

6.0.1 **The Board is expected to adopt the Financial System Stability Committee (FSSC) Cyber Resilience Principles.** Applying the 10 Cyber Resilience Principles at all levels of the organisation is expected to:

- *enhance board oversight of cyber risks to assure a cyber-resilient financial institution.*
- *strengthen cybersecurity preparedness to withstand cyber threats and recover quickly from cyber incidents, thereby safeguarding financial system stability.*
- *foster collaboration across the financial sector with public and private stakeholders to ensure that each regulated entity supports the overall resilience of the interconnected whole.*

6.0.2 **The Board must ensure it holds senior management accountable for promoting a cyber risk aware culture** enterprise-wide, and hold them accountable for enforcing appropriate penalties for behaviours that are contrary to the corporate culture and values of the DTI.

6.1 Reinforcing a Cyber Risk-Aware Culture

6.1.1 **Senior Management is expected to foster a culture of risk awareness and responsibility throughout the organization**, emphasizing the importance of identifying and mitigating cyber risks. (See Appendix 2: Cyber Resilience Principles, Principle 1)

6.1.2 **Senior Management should designate a culture owner such as the CIO, CISO or a non-technical influencer to promote a cyber risk-aware culture.** The culture owner should use messages that resonate with employees and communicate in terms and engagement formats employees understand. For example, saying "protect your data and systems" may be clearer and connect better than using the term "cybersecurity".

6.1.3 **The culture owner should use multiple channels or formats to communicate** key messages such as: videos, digital displays, blogs, alerts, emails, learning modules, phishing simulation tests, events, and training to connect with employees on multiple fronts.

6.1.4 A cyber risk-aware culture should be reinforced at three levels:

- *Leadership Level: Board and management must prioritize cybersecurity, aligning it with corporate values. Non-cyber executives, including the Board, must visibly support and exemplify the mission.*
- *Group Level: Team Leaders should foster cybersecurity discussions from informal chats to formal meetings. Non-technical groups should seek guidance on securing personal and work devices, emphasizing the importance of cyber hygiene.*
- *Individual Level: Employees should develop awareness of potential threats and feel empowered to respond to suspicious activities.*

6.1.5 **DTIs should prioritize and institutionalize cybersecurity measures and include mandatory cybersecurity training** sessions from the Board to senior management to all staff. This may include e-learning modules or simulation exercises tied to employee performance assessments.

6.1.6 **DTIs should apply the principle of least-privilege to every user access decision including Board and senior management,** where the answers to the questions of who, what, when, where, and how are critical for appropriately provisioning/deprovisioning or allowing/denying access to resources.

6.1.7 **DTIs should eliminate implicit trust in any one person, node, or service on the DTI's core network** and instead require continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

6.1.8 **The Board must ensure that every job description includes explicit ethical expectations of all employees across the organization** and the requirement to report instances of misconduct and non-adherence to company values.

6.2 Cyber Hygiene Best Practices

6.2.1 **Cyber hygiene addresses common problems that can compromise cybersecurity, such as:**

- *Security breaches from phishing, malware, and viruses.*
- *Data loss from hacking or corruption.*
- *Outdated software that is more vulnerable to cyber-attacks.*
- *Out-of-date antivirus and malware software that provides less effective protection.*

6.2.2 **Regardless of whether a device belongs to a member of the Board, senior management, IT administrators and other user account groups with elevated privileges, by default, controls must be in place** to ensure that all portable data storage media, personal computers and internet-of-things devices are prevented

from accessing the DTI's core network. Prior approval of use of device and routine scanning of media should be required.

6.2.3 **Board member, senior management, IT administrators and other user account groups must exercise extreme caution when reviewing incoming emails** and other forms of text messages. If an email or text message appears suspicious, refrain from clicking on any links, downloading attachments, or interacting with the email's contents.

6.2.4 **Board must ensure policies and procedures are in place to ensure cyber hygiene best practices are established and enforced for all users and devices. This must include:**

1. Regularly backing up important data and keeping them encrypted, offline and offsite
2. Enforcing lengthy and complex passwords, updated regularly
3. Connecting to secure, trusted and protected Wi-Fi networks
4. Enabling multi-factor authentication (MFA) where possible
5. Installing the latest software patches from trusted sources
6. Providing users with the minimal amount of permissions necessary for their specific job roles
7. Installing reputable antivirus and anti-malware software, updated regularly
8. Recognising and reporting phishing and other suspicious messages and system activity
9. Being cautious about sharing personal information over the phone, email, social media and publicly
10. Encrypting messages, storage media and devices that contain sensitive data
11. Reviewing the privacy and security settings on applications and taking control of application permissions to access device features and data .
12. Deleting data on desktop or mobile devices before disposing, repurposing, donating, reselling, or recycling it.

APPENDIX 1
Cyber Risk Related Legislation
(Jamaica and Other Jurisdictions)

- **Cybercrimes Act, 2015.** Provides a legal framework aimed at combating cybercrime and protecting the country's digital infrastructure.

- **Jamaica Data Protection Act, 2020.** Provides companies that collect, process, and store data for people in Jamaica with a set of requirements for protecting that data and maintaining the privacy of individuals.

- **General Data Protection Regulation (GDPR), 2018.** Sets out data protection and privacy measures for organizations handling the personal data of European Union (EU) citizens.

- **UK Data Protection Act, 2018.** The UK's implementation of the General Data Protection Regulation (GDPR).

- **Canada Personal Information Protection and Electronic Documents Act, PIPEDA.** Sets out the rules for the collection, use, and disclosure of personal information in commercial activities.

- **Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018** of the United States. Address issues related to cross-border data access and law enforcement investigations, particularly in the context of cloud computing and data storage.

- **Digital Operational Resilience Act (DORA), 2022** of the EU. Creates a binding, comprehensive information and communication technology (ICT) risk management framework for the EU financial sector. Financial institutions providing services to EU financial service firms.

APPENDIX 2
Cyber Resilience Principles

Extracted from Financial System Stability Committee Statement on 10 Cyber Resilience Principles (2023)

Cyber resilience is essential for safeguarding financial stability.

Financial institutions are expected to adopt these 10 Cyber Resilience Principles, which serve as a set of guiding concepts to manage cyber risks and to enhance each financial institution's ability to safeguard its operations, assets, and reputation in an increasingly digital and interconnected financial system.

Principle 1. Not Just an IT Issue

Ensures the strategies or measures in a financial institution's cyber risk management framework is not restricted to securing the viability of its IT operations alone, but should also cover people, processes, data and facilities.

Focus Areas:

- *Cyber Risk-Aware Culture.* Foster a culture of risk awareness and responsibility throughout the organization, emphasizing the importance of identifying and mitigating cyber risks.
- *Integration with Business Strategy.* Align cyber risk management with the organization's business strategy, ensuring that technology initiatives across the organization support and enhance the achievement of strategic goals.
- *Remote Working.* As organizations shifted to remote working and non-IT department are technology enabled, the source of technology and cyber incidents often happens outside of IT. Non-IT areas such as sales, marketing, legal, projects and other business units are key partners to promoting cybersecurity awareness, imbedding cybersecurity standards in its processes, practices and reporting of cyber incidents.

Principle 2. Legal Basis

Ensures the board and management understand the legal implications of technology and cyber incidents, including data privacy, as they relate to their company's specific circumstances.

Focus Area:

- *Legal and Regulatory Compliance.* Ensure that cyber risk management practices comply with relevant laws, regulations, and industry standards, minimizing legal and compliance risks.

Principle 3. Adequate Attention on Agenda

Ensures due attention is given to cyber risk at the board level and allocate adequate discussion time on board meeting agendas to reduce risk exposure to direct losses, legal claims, reputational damage, ICT disruption and misuse of technology. (See Appendix 3: 60 Must-Ask Questions at the Next Board Meeting to Strengthen Cybersecurity)

Focus Areas:

- *Proactive Cybersecurity Preparedness Strategy.* Given the digital nature of cyber risks, prioritize cybersecurity as a critical component of corporate governance, develop a Cybersecurity Preparedness Strategy, and maintain policies and protocols that covers preparedness, people, data, infrastructure, applications and service providers.
- *Regular Reporting*. Establish reporting mechanisms that provide regular board and management updates on the effectiveness of investments in penetration testing and vulnerability assessments (technology), cyber hygiene training and simulation tests (people), IT security control and service provider audits (process), backup capacity and testing (data), cyber incident disclosure (communications) and post-incident reviews (lessons learned), all of which enable informed decision-making.

Principle 4. Accountability with Expertise

Ensures an enterprise-wide Cyber Risk Governance framework integrates with organizational operations and prevents the interruption of activities due to cyber threats or attacks, including staffing and budget for cybersecurity expertise, training, response and recovery.

Focus Areas:

- *Clear Roles and Responsibilities*. Clearly define the roles and responsibilities of key stakeholders, including the board, executives, technology leaders, and risk management teams, regarding Cyber Risk Governance.
- *Training and Awareness*. Provide regular training and awareness programmes for employees, executives, and board members on cyber risks, promoting a well-informed and vigilant approach.

Principle 5. Transparent, Thorough and Targeted

Ensures board and management discussions about cyber resilience include high visibility reporting on gaps in addressing cyber risks using cyber resilience maturity models and assessments of cybersecurity effectiveness augmented by threat information sharing and penetration testing programmes.

Focus Areas:

- *Transparency.* Promote transparency by communicating technology governance principles and cyber risk management practices, related policies, guidelines and outcomes to stakeholders. Ensure accountability for risk management actions and decisions.
- *Performance Metrics.* Define key risk indicators (KRIs) and metrics to measure the effectiveness of Cyber Risk Governance efforts. Use these metrics to guide improvements over time.
- *Threat Information Sharing.* Timely access to threat intelligence allows organizations to detect potential threats before they escalate into full-blown attacks. Threat information sharing through a financial-sector information sharing and analysis centre contributes to an organization's overall cyber resilience.

Principle 6. Defence in Depth

Ensures multiple layers of security controls and mechanisms exist to protect an organization's information systems and data. These layers are designed to work together to provide comprehensive security, with the assumption that no single security measure is fool proof. If one layer is breached, others should still provide protection.

Focus Area:

- *Incident Response & Recovery.* Develop comprehensive incident response plans that outline how the organization will respond to and recover from technology-related incidents, such as data breaches or system outages.

Principle 7. Need-to-know

Ensures restricted access to information and resources only to individuals who have a legitimate and specific need for that access to perform their job responsibilities. It limits the exposure of sensitive data to the minimum required, reducing the risk of unauthorized access or data breaches.

Focus Area:

- *Risk Assessment and Mitigation.* Implement a robust cyber risk assessment process that identifies, evaluates, and prioritizes technology and cyber-related risks. Develop *appropriate* mitigation strategies, controls, and response plans.

Principle 8. Least Privilege

Ensures only the minimum level of access or permissions necessary to perform their tasks or functions are granted. This principle limits potential damage or misuse that could occur if users or systems were granted excessive privileges.

Focus Area:

- *Continuous Permissions Right-Sizing*. Regularly reviewing and adjusting access controls to ensure that users have the least privilege necessary to perform their job tasks. This approach helps to reduce the risk of security breaches by limiting the access granted to sensitive data and systems.

Principle 9. Segregation of Duties

Ensures critical tasks or responsibilities are divided among different individuals or systems to prevent a single point of failure or misuse. It helps prevent conflicts of interest and reduces the risk of fraud or unauthorized actions by requiring multiple authorizations for certain actions.

Focus Area:

- *Sufficient Resources.* Allocate sufficient resources, including budget and expertise, for effective cyber risk *management*, ensuring that risks are adequately addressed.

Principle 10. Security by Design

Ensures security measures and considerations are integrated into the design and development of software, systems, and products from the outset. It prioritizes proactive security planning rather than attempting to retrofit security after the fact.

Focus Areas:

- *Third-Party Management.* Establish guidelines for assessing and managing cyber and IT-specific risks associated with third-party vendors and service providers. Ensure that their risk management practices align with your organization's standards.
- Privacy as the Default. *Privacy should be the default in all systems and processes, where personal data is collected, processed, and retained solely for specified purposes. Users need not opt-out or take action to protect their privacy; systems should proactively offer strong privacy safeguards as the default, allowing users to opt-in for additional data sharing or processing.*

APPENDIX 3
Cyber Risk Oversight Expectations for Boards and Questions to Ask

To effectively safeguard their organizations, board members must actively engage by asking the right questions.

Board members play a crucial role in overseeing an organization's cybersecurity posture. While not cybersecurity experts, Boards should ask informed questions to ensure the organization is adequately protected against cyber threats.

By posing the right questions, board members can gain a deeper understanding of their organization's security posture, identify potential risks, and work collaboratively with cybersecurity experts to ensure the highest level of protection against the ever-present cyber threats.

While asking questions about the latest offline backups, how suspicious email are handled and the company's password policy are useful conversation starters, there are a wider spectrum of critical cybersecurity risk considerations, as shown in the table below, that every board should explore to uphold their fiduciary responsibility and safeguard their organization's digital assets.

Board Oversight Expectations	Questions for Next Board Meeting
A. Understand the organization's current state of cybersecurity and any recent incidents or breaches.	1. What is our current cybersecurity posture? 2. Do we have a comprehensive cybersecurity policy and governance framework in place? 3. Is there a documented incident response plan, and has it been tested? 4. What are the existing cybersecurity policies and procedures and training manuals in place? When last have they been updated? What measures are in place to detect a breach? How many policy breaches were reported since its effective date? How many of those were escalated? Why? 5. What do we consider our most valuable business assets? How many layers of cyber and physical security measures are enforced to ensure its secure and recoverable?

Board Oversight Expectations	Questions for Next Board Meeting
B. Identify critical data and systems that need the highest level of protection.	6. What are our most valuable digital assets and data? 7. Do we think there is adequate protection in place if someone wanted to get at or damage our corporate "crown jewels" or other highly sensitive data? What would it take to feel confident that those assets/data were protected?
C. Ensure cybersecurity training and awareness programme is improving both competence and behaviour.	8. Does the company perform employee training on a semi-regular basis (at least twice a year or more)? Does this training address email policies and social media sites that employees might visit? 9. Are we spending wisely on cybersecurity tools and training? Do we know if our spending is cost effective? 10. Are there metrics in place to measure the effectiveness of our cybersecurity awareness and training initiatives? 11. When was the last phishing simulation conducted? Are the results showing an improvement over-time? How can we close that gap?
D. Ensure organisation's capacity for cyber threat monitoring and information sharing.	12. Does our organization participate in any of the public or private sector ecosystem-wide cybersecurity and information-sharing organizations? Should we?
E. Assess the financial, reputational, and operational risks associated with cyber incidents.	13. What is the potential impact of a cyberattack on our business?
F. Ensure the organization is compliant with relevant data protection and privacy regulations. Review and understand the organization's cybersecurity policies, incident response plan, and disaster recovery plan.	14. How are we addressing regulatory and compliance requirements related to cybersecurity? What is outstanding? How can we close that gap?
G. Ensure employees are educated about cybersecurity best	15. What cybersecurity training and awareness programmes are in place for employees?

Board Oversight Expectations	Questions for Next Board Meeting
practices and the risks associated with cyber threats.	
H. Inquire about the frequency of security assessments, penetration tests, and audits to evaluate the effectiveness of security controls.	16. How often are security assessments and audits conducted? What are the results telling us? What additional resources or expertise is needed to close that gap?
I. Ensure the organization has a well-defined incident response plan and that it is regularly tested to ensure readiness in case of a breach.	17. What is our incident response plan, and has it been tested?
J. Understand the budget allocated to cybersecurity and how it aligns with the organization's risk profile.	18. What is our cybersecurity budget and how is it allocated?
K. Determine whether the organization has cybersecurity insurance and the extent of coverage it provides.	19. What cybersecurity insurance coverage do we have?
L. Assess how the organization evaluates and manages cybersecurity risks associated with third-party vendors and suppliers.	20. What is our strategy for third-party vendor risk management?
M. Understand the tools and processes in place for monitoring the network and identifying potential threats.	21. How do we monitor and detect cybersecurity threats and incidents?
N. Determine who the Chief Information Security Officer (CISO) or equivalent is and their role in managing cybersecurity.	22. Who is managing our cybersecurity? Who is responsible for cybersecurity at the executive level? Do we have the right talent and clear lines of communication, accountability and responsibility for cybersecurity? Is cybersecurity risk included in our risk register?
O. Explore how the organization stays current with evolving cybersecurity threats and technologies.	23. What investments are we making in emerging cybersecurity technologies?

Board Oversight Expectations	Questions for Next Board Meeting
P. Discuss the organization's vision for cybersecurity and how it plans to adapt to future threats.	24. What is our long-term Cybersecurity Preparedness Strategy?
Q. Understand the organization's approach to transparency and communication regarding cybersecurity incidents.	25. How do we communicate cybersecurity matters to stakeholders, including customers and investors?
R. Stay informed about the latest cybersecurity threats and incidents in the industry and how they might affect the organization.	26. Are there any recent cybersecurity incidents or trends in the industry that we should be aware of?
S. Ensuring data is securely retained and can be restored effectively in the event of data loss or disasters.	27. What is the company's back-up procedure and what back-up media are used by the IT department? 28. What is the policy for retaining backup data, and are there plans for archiving older backups? 29. How long are different types of data retained, and what criteria are used to determine retention periods? 30. How frequently are backups performed, and is there a schedule for different types of data? 31. Is there a disaster recovery plan that includes backup data? 32. What is the process for monitoring and addressing backup failures or anomalies?
T. Review the company's password policy and access controls.	33. What is the company's password policy? Is it complex enough? 34. Is the current password policy considered sufficiently robust and in compliance with industry standards and best practices? 35. What is the password expiration policy, and how often do passwords expire for employees? 36. Do we have a process in place to promptly revoke access for ex-employees? 37. How many former employees, promoted and transferred employees still have active access to

Board Oversight Expectations	Questions for Next Board Meeting
	resources tied to their previous role, and what steps are being taken to address this? 38. Are there any users with privileged access rights who are anticipated to leave the company in the near future?
U. Review the frequency and effectiveness of the company's patch programme.	39. When are critical patches and updates made to the network? Once a week, once a month? 40. How quickly are critical or emergency patches made? 48 hours, 72 hours, two weeks, or longer?
V. Review the effectiveness of email security to filter suspicious emails, and other email security measures.	41. Does your company have in place some sort of email 'filtering' system in order to reject any emails that might appear normal, but are actually sent from a spoofed or copycat address? 42. What is the incident response plan for handling detected phishing emails or email security breaches? 43. How are email attachments and downloads scanned for malware and other threats? 44. Are multi-factor authentication (MFA) and strong password policies enforced for email accounts? 45. Is there a regular testing and evaluation process for email security effectiveness such as simulated phishing tests and email security assessments?
W. Review the capacity gaps within IT and cybersecurity	46. Does the company have enough IT staff to handle not just security alerts that need to be investigated, but also handle patching, applications, the Cloud, and a host of other daily jobs that need to be performed? 47. What is the current state of our IT infrastructure, and how well does it support our business operations and objectives? 48. What is the IT department's current workload, and do they have the necessary resources to manage it effectively? 49. Are there any skill gaps within our IT team, and if so, which areas need improvement?

Board Oversight Expectations	Questions for Next Board Meeting
	50. What is our cybersecurity budget, and is it aligned with industry benchmarks and our risk profile? 51. Are there specific cybersecurity skills or expertise that we lack internally? 52. Are there regular assessments or audits to identify and address capacity gaps within IT and cybersecurity? What are the recurring gaps and most alarming findings?
X. Assess and strengthen the organization's approach to managing risks associated with external partners	53. What is our strategy for assessing and managing cybersecurity risks associated with third-party vendors and suppliers? 54. What due diligence processes are in place before onboarding new third-party vendors or partners? 55. Is there a risk ranking or categorization system for vendors based on their potential impact on our organization's security? 56. Are there contractual agreements that specify cybersecurity requirements and responsibilities for our vendors? 57. How do we monitor third-party vendors' ongoing compliance with cybersecurity requirements and agreements? 58. What reporting mechanisms are in place for third-party vendors to notify us of cybersecurity incidents or breaches? 59. How do we ensure that our third-party vendors comply with relevant cybersecurity regulations and industry standards? 60. Do we have alternative vendors or contingency plans in place in case a critical third-party vendor experiences a security incident or disruption?

APPENDIX 4
TYPES OF CYBER ATTACKS

Cyberattacks can take various forms, targeting different aspects of computer systems, networks, and data.

Organizations **must** train users on the types of cyber attacks; reduce vulnerabilities and strengthen controls. Insufficient safeguards around assets, data and technology provide an environment for cyber criminals to penetrate, blend in and then launch attacks that disrupt operations and deny services, mostly for financial gain.

Here are some common types of cyberattacks:

- **Phishing**. In phishing attacks, attackers impersonate legitimate entities to trick individuals into revealing sensitive information such as usernames, passwords, and credit card details.
- **Social Engineering.** Social engineering attacks manipulate human psychology to deceive individuals into divulging sensitive information or performing actions that benefit the attacker.
- **Password Attacks.** Password-based attacks, such as brute force and dictionary attacks, aim to guess or crack user passwords to gain unauthorized access to accounts or systems.
- **Malware**. Malicious software, including viruses, worms, Trojans, ransomware, and spyware, are designed to infect and compromise computer systems.
- **Ransomware**. Ransomware encrypts a victim's files or systems and demands a ransom payment in exchange for the decryption key. It can have devastating effects on organizations and individuals.
- **Insider Threats.** These attacks involve individuals within an organization intentionally or unintentionally compromising security, such as employees leaking sensitive information or sabotaging systems.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks.** These attacks flood a target system or network with excessive traffic, causing it to become overwhelmed and unavailable to legitimate users.
- **Man-in-the-Middle (MitM) Attacks.** In MitM attacks, attackers intercept and possibly alter communication between two parties without their knowledge. This can compromise the confidentiality and integrity of data.
- **Structured Query Language (SQL) Injection.** Attackers inject malicious

SQL code into input fields on web applications to gain unauthorized access to databases or manipulate data.

- **Cross-Site Scripting (XSS).** XSS attacks involve injecting malicious scripts into websites or web applications that are then executed by unsuspecting users' browsers, potentially stealing data or compromising accounts.
- **Zero-Day Exploits.** These attacks target vulnerabilities in software or hardware that are not yet known to the vendor or have not been patched, making them highly effective for attackers.
- **Crypto-jacking.** In crypto-jacking attacks, malicious actors use victims' computing resources to mine cryptocurrencies without their consent or knowledge.
- **Drive-By Downloads.** Attackers exploit vulnerabilities in web browsers or plugins to download and install malware on a user's device when they visit a compromised website.
- **Internet of Things (IoT) Exploitation.** Hackers target vulnerabilities in IoT devices, such as smart cameras and thermostats, to gain control or use them as part of a botnet for other attacks.
- **Eavesdropping/Sniffing.** Attackers intercept and monitor network traffic to capture sensitive data, such as login credentials or financial information, being transmitted over the network.
- **Supply Chain Attacks.** Attackers compromise the software or hardware supply chain, injecting malicious code or components into products before they reach end-users.
- **Fileless Attacks.** These attacks operate without leaving traditional traces on the victim's system, making them challenging to detect and often leveraging legitimate system tools.
- **Watering Hole Attacks**. Attackers compromise websites or online resources frequently visited by their target audience, infecting visitors' devices with malware.
- **Advanced Persistent Threats (APTs).** APTs are prolonged, targeted attacks by well-funded and skilled adversaries, often nation-states, with the goal of stealing sensitive information or maintaining long-term access.

APPENDIX 5
Industry Standards on Cybersecurity

Common industry standards include:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework. Provides guidelines for organizations to manage and reduce cyber risk. The NIST Cybersecurity Framework Core consists of six functions: Govern, Identify, Protect, Detect, Respond, and Recover.
- NIST SP 800-53. Provides a comprehensive catalogue of security and privacy controls for federal information systems and organizations. It's widely used not only by the government but also by various industries.
- Cyber Risk Institute (CRI). A cybersecurity and resiliency framework based on the NIST Framework, tailored for the financial services industry.
- International Organization of Standardization (ISO) 27001. A widely recognized standard for information security management systems (ISMS). It provides a systematic approach to managing sensitive information and ensuring its confidentiality, integrity, and availability.
- ISO 27002 is an international standard that provides guidelines for implementing an information security management system (ISMS). It outlines a framework for identifying, assessing, and managing information security risks, as well as implementing controls to protect sensitive information.
- Center for Internet Security (CIS) Controls. Offers a prioritized set of actions for improving an organization's Cybersecurity posture. It's divided into three implementation groups, each with a varying level of complexity and coverage.
- Control Objectives for Information and Related Technologies (COBIT). Provides a framework for the governance and management of enterprise IT, including Cybersecurity aspects.
- Information Technology Infrastructure Library (ITIL). Provides best practices for managing IT services, and can be integrated with cybersecurity practices and frameworks to enhance an organization's overall cybersecurity posture.
- Factor Analysis of Information Risk (FAIR)). Helps organizations analyse and quantify information and Cybersecurity risk in financial terms, making risk management decisions more data-driven.
- MITRE Adversarial, Tactics, Techniques and Common Knowledge) (ATT&CK). Provides a matrix of tactics and techniques used by attackers during different stages of the cyberattack lifecycle.

- Capability Maturity Model Integration (CMMI)): A capability improvement framework that can be adapted to Cybersecurity practices to enhance an organization's maturity in managing Cybersecurity processes.
- Building Security in Maturity Model (BSIMM)): This is a framework specifically designed for software security. It is a set of best practices derived from studying real-world software security initiatives.
- Payment Card Industry Data Security Standard (PCI DSS) (). Widely used framework that outlines security requirements for protecting payment card data.
- Cryptocurrency Security Standard (CCSS). A framework that sets security guidelines for cryptocurrency systems and exchanges. It helps improve security measures in the cryptocurrency industry, covering areas like key management and data protection, reducing risks and enhancing digital asset protection.

ADDITIONAL REFERENCE MATERIAL

- Banks for International Settlements, Financial Stability Institute ("FSI") Insights on policy implementation No 50 – Banks' Cybersecurity – a second generation of regulatory approaches – June 2023: https://www.bis.org/fsi/publ/insights50.pdf

- Banks for International Settlements, Guidance on Cyber Resilience For Financial Market Infrastructures - June 2016 https://www.bis.org/cpmi/publ/d146.pdf

- Bouveret, Antoine. Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund. 2018 – https://www.bis.org/publ/work1039.pdf

- Doerr, Sebastian, Leonardo Gambacorta, Thomas Leach, Bertrand Legros, and David Whyte. Cyber risk in central banking. 2022 – https://www.bis.org/publ/work1039.pdf

- European Central Bank. Cyber resilience and financial market infrastructures - https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html

- FFIEC Information Technology Examination Handbook: Information Security - September 2016: https://www.ffiec.gov/press/pdf/ffiec_it_handbook_information_security_booklet.pdf

- FFIEC Cloud Computing Statement, April 2018: https://www.ffiec.gov/press/pdf/FFIEC_Cloud_Computing_Statement.pdf

- Financial Stability Board ("FSB") Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence – October 2021: https://www.fsb.org/wp-content/uploads/P191021.pdf

- Financial Stability Board ("FSB") Cyber Lexicon – 2023 Update https://www.fsb.org/wp-content/uploads/P130423-3.pdf

- G-7 Fundamental Elements for Threat-Led Penetration Testing, October 2018: https://www.bundesbank.de/resource/blob/764690/792725ab3e779617a2fe

28a03c303 940/mL/2018-10-24-g-7-fundamental-elements-for-threat-led-penetration-testing-data.pdf

- International Monetary Fund. The global cyber threat. 2021 – https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

- Mendez-Barreira, Victoria. Risk Management Benchmarks. 2023 – https://www.centralbanking.com/benchmarking/risk-management/7958596/risk-managementbenchmarks-2023-presentation

- NIST Framework for Improving Critical Infrastructure Cybersecurity – April 2018: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

- NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations – September 2020: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

- NIST Special Publication 800-150 - Guide to Threat Information Sharing – October 2016: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf