GEN-CONSUL-23/12-0006

FINANCIAL SERVICES COMMISSION

SUPERVISORY GUIDANCE FOR INDUSTRY CONSULTATION

MANAGEMENT OF CYBER RISKS

Table of Contents

1. Background and Context 1
1.0 Legislative Reference 1
1.1 Context 1
2. Definitions 2
3. Cyber Risk Governance 2
3.0 Preamble 3
3.1 Board Oversight of Cyber Risks 3
4. Overseeing the Cyber Risk Management Framework 5
4.0 Preamble 5
First Line of Defence: Operational Management 5
4.1 Structure and Expertise 5
4.2 Roles and Responsibilities 6
4.3 Third Party Dependencies 9
4.4 Risk Identification and Assessment 10
4.5 Risk Mitigation and Control 12
4.6 Risk Monitoring and Reporting 13
Second Line of Defence: Risk Management 14
4.7 Risk Management Function 14
Third Line of Defence: Independent Assurance 15
4.8 Internal Audit Function 15
5. Key Reports to Board 16
5.0 Preamble 16
5.1 Board Reports on Cybersecurity Effectiveness 16
6. Tone at the Top – Cyber Risk Aware Culture 18
6.0 Preamble 18
6.1 Reinforcing a Cyber Risk-Aware Culture 18
6.2 Cyber Hygiene Best Practices 19

Appendix:

1. Relevant Legislation
2. Cyber Resilience Principles
3. 60 Questions to Ask at the Next Board Meeting to Strengthen Cybersecurity
4. Industry Standards on Cybersecurity

Additional Reference Material

1. Background and Context

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

This consultation paper 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 Insurance Act, the Pensions Act, and the Securities Act. Each licensed financial institution ("FI") 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 Legislative Reference

1.0.1 These Guidelines on the management of cyber risks are issued pursuant to Section 6(2) of the Financial Services FSC Act to promote the adoption of procedures designed to control and manage cyber risk. (See Appendix 1: Cyber Risk Related Legislation)

1.1 Context

1.1.1 **Cyber attacks are becoming more frequent, and they continue to evolve** in terms of their complexity and sophistication.

1.1.2 **A successful cyber attack could have a debilitating impact on financial institutions** which could cause a significant financial or operational impact on a financial institution.

1.1.3 **Cyber risk refers to the potential threat or vulnerability of a computer system,** network, or device to unauthorized access, use, disclosure, disruption, modification, or destruction. This includes risks from hacking, malware, phishing, and other types of cyberattacks, as well as from insider threats.

1.1.4 **Cyber risks can have significant consequences**, including financial loss, reputational damage, and loss of sensitive information. It is important for FIs to understand and manage their cyber risk to protect their assets and operations.

2. Definitions

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

Cybersecurity

(a) The systems, technologies, processes, governing policies and human activity that an organization uses to safeguard its digital assets. (Gartner)

(b) The practice of protecting critical systems and sensitive information from digital attacks. whether those threats originate from inside or outside of an organization. (IBM)

(c) Preservation of *confidentiality*, 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. (ISACA)

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 Framework

The arrangements put in place to establish, implement and review its approach to managing cyber risks and support cyber incident response and recovery activities toward cyber resilience.

3. Cyber Risk Governance

3.0 Preamble

3.0.1 **Cyber Risk Governance refers to the oversight provided by the board** to ensure the effective management of cyber risks through the establishment of a comprehensive cyber risk management framework. *(See Section 2: Overseeing the Cyber Risk Management Framework)*

3.0.2 **Unlike other types of risks, cyber risks possess a distinctive set of characteristics, marked by their stealthy nature, intricate sophistication, prolonged persistence and systemic impact potential.** These qualities make them particularly hazardous, as they have the capacity to trigger extensive disruptions not only within a financial institution's network but also throughout the broader financial system.

3.0.3 **The Board is expected to ensure the strategies and measures in a FI'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 and facilities. *(See Appendix 2: Cyber Resilience Principle 1: Not an IT Issue)*

3.1 Board Oversight of Cyber Risks

3.1.1 **Board of Directors ("The Board") must have full oversight of the institution's framework for management cyber risks.** This means that the Board, individually and collectively, must understand the seriousness of the cyber threat environment and ensure the creation of a cyber risk-aware culture throughout the organization. *(Appendix 3: 60 Must Ask Questions at the Next Board Meeting)*

3.1.2 The Board should seek to understand all aspects of operations of their business including the risks associated with IT outsourcing, and put in place mitigation measures *(See Section 4.5 Third Party Risk Management)*

3.1.3 **The Board should ensure its corporate risk appetite and tolerance** reflects the scope and level of cyber risk that the FI is willing to accept or avoid for its critical operations[1] and core business lines.

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

1. *The First Line of Defence:* Business units that own and manage cyber and IT-specific risks.

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

2. *The Second Line of Defence.* The Risk Management function oversees cyber and IT-specific risks.

3. *Third Line of Defence:* The Internal Audit function provides independent assurance over cyber and IT-specific risks.

3.1.5 **The Board must have an ongoing program to assess any gaps in the knowledge and expertise** of the board and management and to implement initiatives to address these gaps. For example, by appointing additional board members with the requisite expertise; training and upskilling the existing board members and senior managers or hiring outside expertise. (See Section 5: Reports to Board)

3.1.6 **The Board is expected to play a key role in assessing the effectiveness** of the above and empowers management to take decisions to deploy such activities. This is important to ensure board oversight of cyber risks remains effective in accordance with corporate governance principles.

4. Overseeing the Cyber Risk Management Framework

4.0 Preamble

4.0.1 **A Cyber Risk 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 cyber attacks. *(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 three lines of defence:** Operational Management, Risk Management and Internal Audit, along with appropriate policies and procedures.

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

- *design an appropriate structure with expertise to effectively manage cyber risks, outlined in Sections 4.1-4.2.*
- *incorporate third party dependency factors within the framework outlined in Section 4.3.*
- *assess their exposure and susceptibility to cyber risks, threat actors 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 to effectively manage cyber risk, equipped with adequate resources and cyber expertise**.**

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 a crucial to minimize 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 programs include topics passwords, malware, viruses, phishing and others clickjacking.

4.2 Roles and Responsibilities

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

- Establish a sound, robust and enterprise-wide cyber risk management process to manage cyber risks in relation to business objectives, risk appetite and regulatory requirements.
- Develop a Cybersecurity Strategy informed by the cyber risk management process to build the FIs 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.
- Ensure the FIs cybersecurity preparedness strategy is in alignment with the institution’s overall business strategy, as well as, monitor and evaluate existing and future trends in technology that may impact the business strategy, including monitoring of overall industry trends.
- Ensure 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
- Ensure cybersecurity awareness and training is applied enterprise-wide including knowledge at the top. This is because the weak link is typically people and behaviour — a problem that is only resolved through a combination of technology investment and culture change.
- Establish and enforce cyber hygiene practices and provide continuous cybersecurity training as technologies change and the threat landscape evolves. This is helps to reminded employees of their role and responsibility to keep the organization safe.

- Implement policies, procedures and controls that support cybersecurity preparedness and cyber incident response and recovery (CIRR) activities.
- Engage with business and technical functions within the organisation to develop, exercise, maintain, manage, support and improve CIRR objectives and plans consistent with organisational needs.
- Inform members of the Board promptly or within 5 days of any cyber or IT-specific vulnerability, threat, issue or incident that may have a significant impact on the Commission, its suppliers, customers or the greater financial system.

4.2.2 **The responsibilities of the Chief Information Officer (CIO) should include to:**

- Oversee all aspects of information technology (IT) and information systems.
- Lead the digital transformation strategy or technology innovation program to improve digital capabilities of the organisation.
- Ensure 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 to:**

- Develop cybersecurity strategy and oversee the program and ensure continuous alignment with business *objectives*.
- Manage cyber risk management processes
- Enforce cybersecurity policies
- Ensure adequate resources are in place
- Ensure security metrics and monitoring are implemented and carried out.
- Keep abreast of cyber threats and keeping the Board informed to understand the risks and related dependences.
- Ensure 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:**

- Incident coordinator. FI 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 **The responsibilities of the Portfolio/Program/Project Management Office (PMO) include to:**

- Provide centralized coordinated management and support for technology-related projects and change management initiatives in the organization
- Leverage strategic partnerships for adaptive program coordination and delivery, resource management, risk mitigation and effective organization management to deliver CISO-driven requirements.
- Develop and manage procedures, policies, templates, and other documentation shared by the projects.
- Audit 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 strategy may address focus areas such as:**

- Critical infrastructure security. Practices for protecting the computer systems, networks, and other assets that society relies upon for national security, economic health, and/or public safety
- 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 CSPs (cloud service providers). 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 against unauthorized access, online attacks, and insider threats.

- 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.

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 FI <u>must</u> engage in robust planning and due diligence to identify risks related to third 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. SOC 2 reports[2].

4.3.3 **Before entering new third party relationships, FIs <u>must</u> conduct cyber risk assessments** and due diligence to consider whether these relationships are consistent with their cyber strategy.

4.3.4 **Contracts between the FI and third parties <u>must</u> 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 **FIs <u>must</u> employ controls to verify that resilient operational processes are in place** at the third party and consistent with the FIs 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 FIs tolerance for disruption.

4.3.6 **FIs should provide cybersecurity awareness education** especially to personnel engaged in the operations of 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.

4.4 Risk Identification and Assessment

4.4.1 **Risk identification entails the determination of the threats and vulnerabilities to a FIs 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 **FIs 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.

- *Four broad cyber risk categories are:*
    1. Online threats
    2. Physical threats
    3. Insider threats
    4. Data breaches
- *Sources of the cyber risk can be natural, human or environmental. The human element is the most significant sources of threats through deliberate acts or omissions which could inflict extensive harm to a financial institution and its information systems.*
    1. Natural sources include events like natural disasters that disrupt infrastructure.
    2. Human sources encompass insider threats, social engineering, negligence, and malicious actors.
    3. Environmental sources include physical conditions, supply chain vulnerabilities, regulatory changes, and physical security.

4.4.4 **Following risk identification, FIs should perform an analysis** and quantification of the potential impact and consequences of these risks on their overall business and operations.

4.4.5 **FIs should analyse the impact and likelihood of the threats** and vulnerabilities that could cause harm to the organization, including most likely scenarios.

4.4.6 **FIs should also account for risk propagation, such as contagion and concentration risks,** due to interdependency, interconnectivity, scale, and complexity factors within the IT infrastructure, between FIs and across the larger financial system**.** For example, cyber risks that manifest in denial of service (DoS) attacks, ransomware, internal sabotage, malware infestation or others, could cause severe harm and amplified disruption to the operations of FIs with consequential losses for all parties affected.

4.4.7 **FIs should develop a means to prioritize cyber risks based on likelihood and impact assessments.** In addition, FIs should assess their risk tolerance for damages and losses in the event that a given risk-related event materializes.

4.4.8 **FIs 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. FIs 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.

4.4.9 **FIs should carry out regular scenario-based cyber exercises** to validate its 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.

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

4.4.11 **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 FI's production systems, the exercise **must** be closely supervised and performed in a controlled environment.

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

[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 FI'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 FI's critical business functions or services.

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 FI; as well as to assist in the identification of the tactics, techniques and procedures most likely to be used in such attacks.

4.4.13 **Ensure to take in considerations all available threat intelligence** through Information Sharing and Analysis Centres (ISACs) established for the financial sector, such as the Jamaica Cyber Incident Response Team (JaCIRT) information sharing program and other designated information-sharing platforms.

4.4.14 **FIs should have effective cyber threat intelligence processes** and actively participate in information and intelligence sharing arrangements and collaborate with trusted stakeholders within the industry.

4.5 Risk Mitigation and Control

4.5.1 **Mitigating cyber risk is crucial for FIs 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, FIs should develop and implement risk 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, FIs should give priority to threat and vulnerability pairings** that could cause significant harm or impact to a FIs operation. The costs of risk controls should be balanced against the benefits to be derived.

4.5.4 **FIs 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 **FIs must constantly monitor their attack surface to identify and block potential threats as quickly as possible.** As FIs 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 **FIs 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. FIs 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, FIs 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, FIs 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, FIs 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 FI's IT operation should review and update its IT risk control and mitigation approach**, taking into account changing circumstances and variations in the FIs risk profile and cyber threat landscape.

4.6.5 **FIs <u>must</u> provide to the FSC 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[7] or an independent attestation[8].

4.6.6 **FIs <u>must</u> 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.

[7] 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 is 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.

[8] 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).

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 to:**

- Monitor cyber risk as part of operational risk
- Facilitate effective risk management and control practices
- Propose the risk tolerance of the institution for approval by the Board
- Liaise with the CISO or equivalent to incorporate cybersecurity into overall governance, risk and compliance program and processes
- Report risk-related information
- Provide risk treatment plans for identified cyber risks

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 both existing and future business opportunities
  e) Percentage of service level agreements breached

4.7.3 **FIs should institute effective risk management practices and internal controls** to achieve data confidentiality [9], 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.

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

Third Line of Defence: Independent Assurance

4.8 Internal Audit Function

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

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

5. 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

5.1 Board Reports on Cybersecurity Effectiveness

5.1.1 **Board reports on vulnerability tests should be provided at least twice yearly and penetration testing at least annually.** 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.

5.1.2 **Senior Management should, at minimum, establish, track and analyse key performance indicators (KPIs) and key risk indicators (KRIs)** to provide high-visibility reports to the Board on cybersecurity effectiveness. Metrics used in board reports should include:

- 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 programs.
- 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

6. 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**, which highlights *Cyber Risk-Aware Culture* as a key focus area for financial institutions. (See Appendix 2: Cyber Resilience Principles, Principle 1) Applying the 10 Cyber Resilience Principles 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 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 FI.

6.1 Reinforcing a Cyber Risk-Aware Culture

6.1.1 **The Board 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)

6.1.2 **The Board 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 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 **FIs 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 **FIs 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 **FIs should eliminate implicit trust in any one person, node, or service on the FIs 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:**

1. Security breaches from phishing, malware, and viruses.
2. Data loss from hacking or corruption.
3. Outdated software that is more vulnerable to cyber-attacks.
4. Out-of-date antivirus and malware software that provides less effective protection.
5. Misuse or abuse of privileges.

6.2.2 **Regardless of whether a device belongs to a member of Board member, 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 FIs 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 <u>must</u> be exercised 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 <u>must</u> 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 back 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. Be 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 take control of application permissions to access device features and data .
12. Deleting data on desktop or mobile devices before disposing, repurposing, donating, reselling, or recycle 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 (2023). 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.
- GDPR (2018). Sets out data protection and privacy measures for organizations handling the personal data of 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 European Union. 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—are expected to comply with DORA requirements before January 17, 2025

APPENDIX 2
Cyber Resilience Principles

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

Ensure the strategies and measures in a financial institution’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 and facilities.

Focus Areas:

- Cyber Risk-Aware Culture.
- Integration with Business Strategy.
- Remote Working.

Principle 2. Legal Basis

Ensure 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.

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 2: 60 Must-Ask Questions at the Next Board Meeting to Strengthen Cybersecurity)

Focus Areas:

- Cybersecurity Strategy.
- Regular Reporting.

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.
- Training and Awareness.

Principle 5. Transparent, Thorough and Targeted

Ensures board and management discussions about cyber resilience include identification of cyber risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Focus Areas:

- Transparency.
- Performance Metrics.
- Threat Information Sharing.

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.

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.

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.

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.

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.
- Privacy as the Default.

APPENDIX 3
60 Must-Ask Questions
at the Next Board Meeting to Strengthen Cybersecurity

Board members play a crucial role in overseeing an organization's cybersecurity posture.

- While they may not be cybersecurity experts, Boards should ask informed questions to ensure the organization is adequately protected against cyber threats.
- Now is not the time to have an understaffed IT department and cybersecurity personnel. In fact, there is nothing worse than having an understaffed IT department in a company that gets hacked. There are helpful solutions for this, like managed service providers, and machine-learning driven cybersecurity orchestration and automation solutions. Understand the risks, and put additional controls in place.

Cyberattacks are really bad for business

- **Cyberattacks can disrupt operations, damage data or wipe out data with nothing to recover.** They are not only costly but also can cause unquantifiable negative publicity, reputational harm, litigation and regulatory proceedings, each of which negatively impacts customers, employees, shareholders, suppliers and other organisations involved.
- Five of the most prevalent cyber-attacks are: 1) Phishing; 2) Ransomware attacks; 3) Malware attacks; 4) Social Engineering and 5) Credential Stuffing. These cyber threats highlight the diverse range of tactics and techniques. It's crucial to stay vigilant and implement cybersecurity measures to protect against these threats.

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

- 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

considerations, as shown in the table on the next page, that every board should explore to safeguard their organization's digital assets and uphold their fiduciary responsibility.

Board's Responsibility	Questions for Next Board Meeting
☐ 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?
☐ 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?
☐ 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?

Board's Responsibility	Questions for Next Board Meeting
	11. When was the last phishing simulation conducted? Are the results showing an improvement over-time? How can we close that gap?
□ 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?
□ Assess the financial, reputational, and operational risks associated with cyber incidents.	13. What is the potential impact of a cyberattack on our business?
□ Ensure the organization is in compliance 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?
□ Ensure employees are educated about cybersecurity best practices and the risks associated with cyber threats.	15. What cybersecurity training and awareness programs are in place for employees?
□ 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 the results telling us? What additional resources or expertise is needed to close that gap?
□ 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?
□ 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?
□ Determine whether the organization has cybersecurity insurance and the extent of coverage it provides.	19. What cybersecurity insurance coverage do we have?
□ 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?

Board's Responsibility	Questions for Next Board Meeting
□ 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?
□ 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 cyber included in our risk register?
□ Explore how the organization stays current with evolving cybersecurity threats and technologies.	23. What investments are we making in emerging cybersecurity technologies?
□ Discuss the organization's vision for cybersecurity and how it plans to adapt to future threats.	24. What is our long-term cybersecurity strategy?
□ 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? 26. How do we communicate cybersecurity matters to stakeholders, including customers and investors? 27. How do we communicate cybersecurity matters to stakeholders, including customers and investors?
□ Stay informed about the latest cybersecurity threats and incidents in the industry and how they might affect the organization.	28. Are there any recent cybersecurity incidents or trends in the industry that we should be aware of?
□ Ensuring data is securely retained and can be restored effectively in the event of data loss or disasters.	29. What is the company's back-up procedure and what back-up media are used by the IT department? 30. What is the policy for retaining backup data, and are there plans for archiving older backups? 31. How long are different types of data retained, and what criteria are used to determine retention periods?

Board's Responsibility	Questions for Next Board Meeting
	32. How frequently are backups performed, and is there a schedule for different types of data? How frequently are backups performed, and is there a schedule for different types of data? How frequently are backups performed, and is there a schedule for different types of data? 33. Is there a disaster recovery plan that includes backup data? What is the process for monitoring and addressing backup failures or anomalies?
□ Review the company's password policy and access controls.	34. What is the company's password policy? Is it complex enough? 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 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? Are there any users with privileged access rights who are anticipated to leave the company in the near future?
□ 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?

Board's Responsibility	Questions for Next Board Meeting
☐ 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?
☐ Review the capacity gaps within IT and cybersecurity	46. Does your 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? 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

Board's Responsibility	Questions for Next Board Meeting
	IT and cybersecurity? What are the recurring gaps and most alarming findings?
☐ 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

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

Ransomware accounts for one of the most common types of security attacks and organizations **must** train users; reduce vulnerabilities and strengthen controls. Insufficient safeguards around assets, data, 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.
- **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.
- **Cryptojacking.** In cryptojacking 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.
- **IoT (Internet of Things) 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:

- NIST Cybersecurity Framework. Provides guidelines for organizations to manage and reduce cyber risk. It consists of five functions: 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.
- 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.
- 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.
- COBIT. Provides a framework for the governance and management of enterprise IT, including Cybersecurity aspects.
- ITIL (Information Technology Infrastructure Library). Provides best practices for managing IT services, and can be integrated with cybersecurity practices and frameworks to enhance an organization's overall cybersecurity posture.
- FAIR (Factor Analysis of Information Risk). Helps organizations analyze and quantify information and Cybersecurity risk in financial terms, making risk management decisions more data-driven.
- MITRE ATT&CK. Provides a matrix of tactics and techniques used by attackers during different stages of the cyber attack lifecycle.
- CMMI (Capability Maturity Model Integration): A capability improvement framework that can be adapted to Cybersecurity practices to enhance an organization's maturity in managing Cybersecurity processes.
- BSIMM (Building Security In Maturity Model): This is a framework specifically designed for software security. It's a set of best practices derived from studying real-world software security initiatives.

- PCI DSS (Payment Card Industry Data Security Standard). 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/764690/792725ab3e779617a2fe28a03c303 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