FINANCIAL SYSTEM
STABILITY COMMITTEE

CYBER RESILIENCE PRINCIPLES

FOR THE FINANCIAL SECTOR

Table of Contents

Additional Reference Material

01 Background and Context

1.0 About the Financial System Stability Committee

1.0.1 **The Financial System Stability Committee (FSSC)** provides support to the Bank in respect of the identification, mitigation and control of systemic macroprudential threats to the financial system. The FSSC is largely tasked with:

(i) undertaking assessments in relation to developments in the financial system and international markets as well as the links between the financial sector and developments in other sectors of the Jamaican economy and the global economy; and

(ii) giving oversight to the design and conduct of periodic stress tests regarding plausible systemic threats to the stability of Jamaica's financial system.

1.0.2 **The FSSC comprises of the Bank of Jamaica (BOJ), Financial Services Commission (FSC) and the Jamaica Deposit Insurance Corporation (JDIC), the Ministry of Finance** as well as two members appointed by the Minister of Finance and the Public Service on the recommendation of the Governor of BOJ.

1.0.3 **The FSSC contributes to the development of prescriptive rules, standards and codes for financial institutions which specifically address gaps and imbalances that could threaten the stability of the financial system.** On the passage of the amendments to the Bank of Jamaica Act in 2020, the FSSC began to make recommendations to the Bank via the Financial Policy

Committee in respect of policies related to its financial system stability mandate.

1.0.4 In general, these objectives focus on policies and procedures appropriate to the strengthening and regulation of the financial system including:

- Licensees under the Banking Services Act
- Licensees under the Insurance Act
- Licensees under the Pensions Act
- Licensees under the Securities Act

1.1 Context

1.1.1 **The Financial System Stability Committee recognises that cyber resilience is essential for safeguarding financial stability.** The highly interconnected nature of financial institutions and financial market infrastructures, locally and globally, means the potential impact of a cyberattack could spread beyond one financial institution and affect entire industries, sectors and the economy.

1.1.2 **Cyber resilience is important because cyberattacks are no longer a matter of 'if' but 'when.' In fact, financial institutions must assume a breach has already occurred but remains undetected.** [1] Rather than waiting on a cyberattack to happen, financial institutions must be cyber-resilient.

1.1.3 **Resilience to cyber risk comprises of the capacity to withstand cyberthreats,** maintain functioning of critical systems during a cyber incident and the capabilities to restore safely and quickly after a cyber incident and end up stronger.

1.1.4 **In light of the evolving nature and scope of cyber risks**, regulated entities within the financial sector must prioritize cyber resilience and a risk-based approach to strengthen cybersecurity.

1.1.5 **As the first Principle points out, cyber risk is not solely an IT issue. It impacts everybody.** The importance of spotting phishing

[1] According to a 2023 study by IBM, the average time to detect and response to a breach is 277 days.

emails or verify with whom we converse on the telephone, for example have been two of the most prolific vectors of attack.

1.1.6 **Dialogue about how the 10 Cyber Resilience Principles can be applied are therefore critical at all levels**: from the board room, to the back office and the front desk receptionist as well as third party service providers.

1.1.7 **The financial sector is a prime target for cyberattacks due to its significant economic importance and the wealth of valuable sensitive data it holds.** As a result, a significant cyber incident can have far-reaching consequences, including:

- Direct financial loss
- Theft of intellectual property
- Software/data deletion or destruction
- Physical damage
- Business disruption/interruption
- Reputational loss
- Investigation/response costs
- Third-party liabilities (customers, employees, shareholders, regulators)

1.1.8 **The FSSC recognizes that only collective action and partnership can meet the systemic cyber-risk challenge effectively.** It is no longer sufficient just to ensure the cybersecurity of a financial institution is intact. Cyber resilience demands that financial institutions work in concert using the Cyber Resilience Principles outlined in this document as a guide to guard themselves and mature their cyber risk management framework, cybersecurity preparedness, cyber incident response and recovery programme and overall IT operations.

1.2 Objective

1.2.1 **The FSSC establishes 10 Cyber Resilience Principles for the financial sector of Jamaica 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.

1.3 Proportionality

1.3.1 **The Cyber Resilience Principles applies to all regulated entities within the financial sector.** These include banks, non-banks and financial market infrastructures such as clearing and settlement systems operating in Jamaica's National Payment System.

1.3.2 **These high-level principles are aligned with relevant international standards** including principles and guidelines provided by the Bank of International Settlement (BIS), International Organization of Securities Commissions (IOSCO) and Financial Stability Board (FSB).

1.3.3 **The extent and degree to which regulated entities and operating financial market infrastructures implement these 10 Cyber Resilience Principles** should be commensurate with the level of risk and complexity of the financial services offered and the technologies supporting such services.

1.3.4 **Implementation of these principles is to ensure that institutions are positioned to identify, protect, detect, respond and recover** in a timely and effective manner to assure cyber resilience for the overall financial system.

1.3.5 **Focus areas are highlighted under each Principle** for regulated entities to prioritize within context towards the effective management of cyber risks, strengthened cybersecurity preparedness and adequately tested recoverability measures to assure high availability of critical systems.

1.4 Relevant Legislation (Jamaica and Other Jurisdictions)

1.4.1 Cybercrimes Act (2015). Provides a legal framework aimed at combating cybercrime and protecting the country's digital infrastructure

1.4.2 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.

1.4.3 GDPR (2018). Sets out data protection and privacy measures for organizations handling the personal data of EU citizens.

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

1.4.5 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.

1.4.6 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.

1.4.7 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.

02 Definitions

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

Cyber Incident	A cyber event 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	Refers to 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.
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)

03 Cyber Resilience Principles

The 10 Cyber Resilience Principles were established by the Financial System Stability Committee in 2023 to serve as foundation guidelines for all financial institutions in Jamaica to enhance cyber risk oversight at the board-level, strengthen cybersecurity strategy at the management-level, and promote effective capabilities to respond to and recover from cyber incidents through sector-wide cooperation.

The 10 Cyber Resilience Principles are:

Principle 1. Not Just an IT Issue

Principle 2. Legal Basis

Principle 3. Adequate Attention on Agenda

Principle 4. Accountability with Expertise

Principle 5. Transparent, Thorough and Targeted

Principle 6. Defence in Depth

Principle 7. Need-to-know

Principle 8. Least Privilege

Principle 9. Segregation of Duties

Principle 10. Security by Design

The principles are not prescriptive in nature. They intend to guide the behaviour of the board, management and staff of each regulated financial institution and by extension third-party vendors and customers. The principles are internally consistent, meaning that no principle contradicts any other principle. However, in practice there may be times when the principles can overlap. Under each principle, one or more focus areas are highlighted as priority considerations.

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.* 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 unit are key partners to promote cybersecurity awareness, embed cybersecurity standards in its processes, practices and reporting of cyber incidents.

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.* 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.

Focus Areas:

- *Proactive Cybersecurity Strategy.* Given the digital nature of cyber risks, prioritize cybersecurity as a critical component of corporate governance, develop a cybersecurity 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 programs 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 adjust 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.

04 Conclusion

The Financial System Stability Committee recognises that cyber resilience is essential for safeguarding financial stability. The highly interconnected nature of financial institutions and financial market infrastructures, locally and globally, means the potential impact of a cyberattack could spread beyond one financial institution and affect entire industries, sectors and economies.

The FSSC introduces ten (10) guiding principles for the financial sector to enhance board oversight of cyber risks and strengthen its capacity and capabilities to withstand and recover quickly from cyberattacks. It is also the intention for these principles to encourage information sharing across the sector on cyber threats, improving overall cyber resilience towards safeguarding financial system stability.

The 10 Cyber Resilience Principles are:

Principle 1. Not Just an IT Issue

Principle 2. Legal Basis

Principle 3. Adequate Attention on Agenda

Principle 4. Accountability with Expertise

Principle 5. Transparent, Thorough and Targeted

Principle 6. Defence in Depth

Principle 7. Need-to-know

Principle 8. Least Privilege

Principle 9. Segregation of Duties

Principle 10. Security by Design

The extent and degree to which financial institutions implement these 10 Cyber Resilience Principles should be commensurate with the level of risk and complexity of the financial services offered and the technologies supporting such services.

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