BANK OF CANADA
BANQUE DU CANADA

Expectations for Cyber Resilience of Financial Market Infrastructures

October 2021

Table of Contents

Introduction

A cyber attack to the financial system may cause a systemic event that will have a significant impact on financial stability and overall confidence in the financial system. The safe and efficient operation of financial market infrastructures (FMIs) plays a critical role in ensuring financial stability. If not properly managed, FMIs can transmit financial shocks across domestic and international financial markets, leading to adverse economic impacts. In this context, the cyber resilience of FMIs is essential for the safety and efficiency of the financial system.

In June 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published *Guidance on cyber resilience for financial market infrastructures* (Cyber Guidance). The Cyber Guidance was developed to supplement the Principles for financial market infrastructures (PFMI), which the Committee on Payment and Settlement Systems and IOSCO published in April 2012.[1] The Cyber Guidance complements the PFMIs, setting out additional details related to the preparations and measures that FMIs should take to enhance their level of cyber resilience. The Bank of Canada (Bank) expects designated FMIs to implement the Cyber Guidance.

As the cyber threat landscape continuously grows in sophistication and complexity, and with the ever-evolving nature of technology, it becomes necessary to adapt by evolving and strengthening cyber resilience practices while accounting for all relevant developments. The Bank has developed this document as a tool to complement the Cyber Guidance and clearly communicate to overseers and FMIs the Bank's expectations for cyber resilience. To ensure this document remains relevant to future developments, additional chapters that focus on specific subjects may be introduced at a later date.

Purpose

The *Expectations for Cyber Resilience of Financial Market Infrastructures* (the ECR) supplements the Cyber Guidance. It provides further clarity and transparency to both the FMI and overseer on how to apply the Cyber Guidance to continuously improve an FMI's cyber resilience. The ECR will enable the Bank to communicate expectations clearly and consistently across all domestic designated FMIs. This will help lead to the appropriate management of cyber risks across the Canadian financial system and will provide assurance that financial stability is maintained.

Although the ECR is aimed directly at FMIs, it is important for FMIs to take an active role in communicating with their participants and other relevant stakeholders to promote understanding and support of cyber resilience objectives and their implementation. Given the extensive interconnections in the financial system, an FMI's cyber resilience is dependent in part on that of other FMIs, service providers and participants.

---

[1] The Bank of Canada adopted PFMIs as its risk management standards for designated clearing and settlement systems (i.e., FMIs).

Approach

The Bank conducted an expert review of leading international standards (e.g., NIST Cybersecurity Framework and 800 Special Publication Series, ISO/IEC 27001/27002, COBIT 2019) to identify areas that are relevant for FMIs and consistent with the expectations of the Cyber Guidance. The Bank also leveraged other guidance developed by regulatory authorities, notably the European Central Bank's Cyber Resilience Oversight Expectations for Financial Market Infrastructures and the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool. In addition, the expert review considered and assessed recent developments that should be accounted for to ensure a current and robust cyber resilience program. The findings provided the basis for the Bank to clarify and provide additional details on its expectations for Canadian FMIs. During the development of the ECR, the Bank consulted with designated FMIs to seek their feedback on the content of the document.

Structure

The ECR is presented in sections, comparable to the chapters of the Cyber Guidance. These sections outline five primary risk management categories and three overarching components that should be addressed across an FMI's cyber resilience framework. The risk management categories are (i) governance, (ii) identification, (iii) protection, (iv) detection, and (v) response and recovery. The overarching components are (i) testing, (ii) situational awareness, and (iii) learning and evolving. Each section of the ECR begins with an italicized preamble that summarizes the main objectives of the section. The preamble is extracted from the comparable chapter preamble in the Cyber Guidance.

The topics addressed in each section are divided into subsections that largely align with the layout of the Cyber Guidance. However, unlike the Cyber Guidance, the numbering of the ECR begins at the Governance section rather than the Introduction. Each subsection begins with a preamble that has either been extracted from the Cyber Guidance or drafted by the Bank. Each subsection contains a numbered list of discrete expectations that set out concrete steps that FMIs can take to implement the Cyber Guidance. In addition, the glossary in the CPMI-IOSCO Cyber Guidance has been enhanced and revised as needed, including to reflect the Canadian context.

Applicability of expectations

The Bank of Canada expects all domestic designated FMIs[2] to fully observe the Cyber Guidance and to consider the expectations set out in the ECR when implementing the Cyber Guidance. If an affiliate of an FMI develops, implements and/or executes the FMI's cyber security framework, the FMI and its board are responsible for ensuring that the guidance is implemented. The FMI must ensure that cyber risk is managed effectively, in conjunction with the affiliated entity and consistent with the FMI's cyber resilience strategy and objectives. The expectations set out in

[2] The *Payment Clearing and Settlement Act* provides the Bank of Canada with the authority to designate clearing and settlement systems that pose systemic or payments system risk.

this document must therefore apply to both the FMI (the designated clearing and settlement system and its clearing house) and any affiliated entity that the FMI relies on to implement its cyber resilience framework. The FMI should use the ECR as a tool to help it fully observe the expectations set out in the Cyber Guidance and reach the level of cyber resilience necessary to ensure financial stability.

As noted in the Cyber Guidance, components of an FMI's information and communication technology (ICT) environment and entities within its ecosystem are not of equal criticality to its operations. They may also be impacted to varying degrees by different types of cyber risk.[3] In applying the Cyber Guidance, an FMI is expected to adopt a risk-based approach and prioritize its risk mitigation efforts so that risk mitigating measures implemented are commensurate with the various levels of cyber risk it faces. The ECR is not intended to be a checklist of controls or technical requirements. The Bank will assess whether the FMI is meeting the expectations set out in the ECR in accordance with the FMI's own risk-based approach and its role in the Canadian financial system.

Observing the Cyber Guidance is not a "once only" effort. FMIs should aim to advance their level of cyber maturity on an ongoing basis, including improving their capabilities to resume critical operations and recover from successful cyber attacks. This evolution and improvement should occur through discussions between the FMI and the Bank over a sustained period and commensurate with the specific FMI's criticality.

The Cyber Guidance is principles-based in recognition that the dynamic nature of cyber threats requires evolving mitigation methods. While the ECR sets out detailed expectations for FMIs to implement the Cyber Guidance, the Bank will allow for flexibility in the methods chosen to meet the expectations. Although, in some cases, the ECR uses examples of specific cyber resilience measures, including ICT controls, to illustrate and clarify certain points, these examples are not intended to impose specific requirements or to provide the Bank's endorsement of the use of these controls. The selection and implementation of cyber resilience measures should be driven by the FMI's cyber risk assessments. Furthermore, due to the rapid pace of innovation in information technology and changes in the threat landscape, cyber resilience practices may evolve over time.

FMIs are heterogeneous and will differ in size, organizational and operating structure, business model and infrastructure design. Consequently, it is feasible that FMIs may fulfill the underlying expectations using different processes, technologies and methodologies.

Managing cyber risks from interconnections

Over the past several years, there has been an increase in the interconnections between FMIs and other entities, such as participants, linked FMIs, service providers and vendors as well as

[3] Section 1.3.6 of the Cyber Guidance states that cyber risks posed by entities in the FMI's ecosystem—participants, linked FMIs, service providers and vendors—will also vary and not necessarily in relation to the degree of the entity's relevance to the FMI's business.

vendor products. As FMIs modernize and update their core business functions they often implement solutions from outsourced service providers, such as providers of financial technology. These interconnections provide FMIs with multiple benefits, such as greater innovation and access to advanced technologies, operational efficiency, tailored products and services, and cost reductions; however, they could present increased challenges for an FMI's management of cyber risk.

It is important that designated FMIs manage the cyber risks they face from their interconnected entities by appropriately identifying, assessing and implementing protective measures to mitigate the risks. The ECR provides guidance on how a designated FMI can manage this risk, with details in each section (governance, identification, protection, detection, response and recovery, testing, situational awareness, learning and evolving). The Bank expects FMIs to take a risk-based approach when implementing its guidance on managing risks stemming from interconnections.

Interpretation of resumption versus recovery

Within the PFMI and the Cyber Guidance (and within the cyber security industry as a whole), the terms "resumption" and "recovery" are used often, sometimes interchangeably; however, there are subtle differences between the two terms. PFMI 17.6 states that an FMI's business continuity plan "should ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events." Section 6.2.2 of the Cyber Guidance discusses "resumption within two hours," and then introduces the acronym "RTO" as shorthand. Within the cyber security community, however, RTO means "recovery time objective," which can be interpreted differently from resumption within two hours. Resumption tends to refer to and focus on resuming business processes, whereas recovery tends to refer to restoring IT systems and data to an operating state. This discrepancy may cause confusion. In the context of a cyber attack, it is reasonable to interpret the concept of a two-hour RTO as meaning the recovery of those elements or components of IT systems and data that are necessary for the FMI to resume critical business operations. It may not be safe to attempt to fully recover the entire system within two hours. We have endeavoured to make this distinction between resumption and recovery throughout the expectations within this document.

1 Governance

1.1 Preamble

Cyber governance refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks. Effective cyber governance should start with a clear and comprehensive cyber resilience framework that prioritises the security and efficiency of the FMI's operations, and supports financial stability objectives. The framework should be guided by an FMI's cyber resilience strategy, define how the FMI's cyber resilience objectives are determined, and outline its people, processes and technology requirements for managing cyber risks and timely communication in order to enable an FMI to collaborate with relevant stakeholders to effectively respond to and recover from cyber attacks. It is essential that the framework is supported by clearly defined roles and responsibilities of the FMI's Board (or equivalent) and its management, and it is incumbent upon its Board and management to create a culture which recognises that staff at all levels have important responsibilities in ensuring the FMI's cyber resilience.

Strong cyber governance is essential to an FMI'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 at all levels within the organization and to provide appropriate resources and expertise to deal with these risks.

This section provides guidance on what basic elements an FMI's cyber resilience strategy and framework should include and how an FMI's governance arrangements should support that strategy and framework.

1.2 Cyber resilience strategy

A cyber resilience strategy is an FMI's high-level principles and medium-term plans to achieve its objective of managing cyber risks.

1. The FMI should develop a cyber resilience strategy, with the involvement of all relevant business units across the organization. The strategy should be aligned with the FMI's corporate, business and other relevant strategies (e.g., business continuity and IT) and with its overall response and recovery priorities.
2. The FMI should ensure that the following aspects are addressed in the strategy:
    a. the FMI's cyber resilience vision and mission;
    b. the strategic cyber resilience goals, objectives and intended outcomes that the FMI will work toward;
    c. the importance of cyber resilience to the FMI and its key internal and external stakeholders;
    d. the FMI's cyber risk tolerance to ensure that it remains consistent with the FMI's overall risk tolerance, business objectives and corporate strategy;

e. the cyber risks that the FMI bears from and poses to its participants, other FMIs and third parties;

f. clear and credible cyber maturity targets that are periodically reviewed;

g. the governance necessary to enable cyber resilience to be designed, transitioned, operated and improved;

h. the delivery, management and funding, including the budgeting process and organizational capabilities; and

i. the integration of cyber resilience in all aspects of the FMI, including people, processes, technology and new business initiatives.

3. The FMI's board[4] should approve the cyber resilience strategy and should ensure that it is periodically reviewed and updated according to the FMI's threat landscape.

1.3 Cyber resilience framework

A cyber resilience framework consists of the policies, technical standards, procedures and controls that an FMI has established to identify, protect, detect and respond to and recover from the plausible sources of cyber risks it faces.

4. The FMI should have a documented cyber resilience framework that clearly articulates how it determines its cyber resilience objectives[5] and risk tolerance, as well as how it effectively identifies, mitigates and manages its cyber risks to support its objectives.

5. The FMI's cyber resilience framework should:

a. be endorsed by the FMI's board to ensure it is aligned with the FMI's formulated cyber resilience strategy;

b. use leading international, national and industry-level standards, guidelines or recommendations (e.g., ISO/IEC 27000 series, NIST Cybersecurity Framework and Special Publications) as benchmarks for designing its cyber resilience framework and incorporating the most effective cyber resilience solutions;

c. clearly define the roles and responsibilities, including accountability for decision-making within the organization, for identifying, mitigating and managing cyber risk in "business as usual" conditions and in cyber-related crisis or emergency situations;

---

[4] If the FMI belongs to a corporate group, the cyber resilience strategy may be developed at the corporate level. In this case, the board of the FMI should ensure that the FMI is consulted in the development of the cyber resilience strategy. This will ensure that the corporate cyber resilience strategy is aligned with the FMI's cyber resilience objectives.

[5] These objectives should aim to maintain and promote the FMI's ability to anticipate, withstand, contain and recover from cyber attacks to limit the likelihood of a successful cyber attack on its operations or the impact it would have on the broader financial system (CPMI-IOSCO, "Guidance on cyber resilience for financial market infrastructures," section 2.2.1).

d. systematically incorporate the requirements (i.e., policies, technical standards and controls) related to governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving;

e. be aligned with its enterprise operational risk management framework and enterprise architecture;

f. include requirements for timely communication and coordination arrangements to enable the FMI to collaborate with relevant stakeholders to effectively respond to and recover from cyber attacks;

g. consider the cyber risks that the FMI bears from and poses to its participants, other FMIs, vendors, vendor products and its service providers, which are collectively referred to as an FMI's ecosystem; and

h. be regularly reviewed and updated.

6. The FMI should regularly assess and measure the adequacy and effectiveness of and adherence to its cyber resilience framework (including all security controls) through independent compliance programs and audits. In doing so, the FMI is encouraged to use relevant metrics and maturity models and the results of its testing programs. The FMI should periodically commission an external audit.

7. The FMI should periodically review and update its cyber resilience framework (including all policies, technical standards, procedures and controls), particularly when there are changes to the FMI's cyber resilience strategy or objectives. The FMI should develop a methodology for conducting the review, which could consider such factors as:

    a. current and evolving cyber threats (e.g., those associated with the supply chain, use of cloud services, social media, mobile applications and internet of things);

    b. threat intelligence on threat actors and new tactics, techniques and procedures that may specifically impact the FMI;

    c. the results of risk assessments of the FMI's critical functions, key roles, processes, information assets, third-party service providers and interconnections;

    d. cyber incidents that have impacted the FMI directly or cyber incidents that have impacted an entity in the FMI's ecosystem;

    e. lessons learned from certification, audits or other forms of assurance and tests on the cyber resilience framework;

    f. the FMI's performance against the relevant metrics; and

    g. new business developments and future strategic objectives.

8. The FMI should continuously track its progress in developing its cyber resilience capabilities from a current state to a defined future state (i.e., a target maturity level). A maturity model can assist the FMI in documenting this progress.

9. The FMI should have a plan for achieving its target maturity level that clearly sets out a roadmap for how it will be resourced and delivered.

1.4 Role of the board and senior management

1.4.1 Board and senior management responsibilities

10. The FMI's board is ultimately responsible for ensuring that cyber risk is effectively managed.[6,7] The board should clearly define roles and responsibilities for addressing cyber risk, set the FMI's cyber risk tolerance and cyber resilience strategy, and endorse the cyber resilience framework.

11. The board and senior management should establish a process to ensure that cyber risk is identified and addressed on an ongoing basis. All business units should be involved in the decision to accept, mitigate or avoid these risks, consistent with the FMI's operational reliability objectives.

12. The FMI should develop relevant risk metrics, identifying trends and patterns, to be used by senior management and the board to make risk-informed decisions and to demonstrate progress in the implementation of its cyber resilience framework.

13. The board and senior management should ensure that the FMI's cyber risks[8] and the management of those risks are regularly reviewed during board meetings.

14. Senior management should closely oversee the FMI's implementation of the cyber resilience framework, and the policies, technical standards, procedures and controls that support it. This oversight includes:

    a. prioritizing cyber resilience deliverables and resource allocation based on the results of cyber resilience assessments, key performance indicators, key risk indicators, overall business objectives and evolution against target maturity;

    b. regularly conducting cyber resilience self-assessments to evaluate the FMI's cyber maturity;

    c. reviewing the self-assessment as well as lessons learned from test results and making appropriate decisions to improve the effectiveness of cyber activities;

---

[6] Consistent with section 3.2.8 of the PFMIs, the FMI's board has a role in monitoring senior management's oversight of the implementation of the cyber resilience framework and ensuring that the FMI meets the expectations set out in the Cyber Guidance and the ECR. This also applies when the FMI belongs to a corporate group in which the cyber resilience strategy and framework is established at the corporate level.

[7] The FMI can consider leveraging a committee, such as the FMI's risk committee, to help the board discharge its responsibilities for cyber risk management and resilience.

[8] Reports to the board could include an evaluation of the cyber resilience situation compared with the last report, information about cyber resilience projects, cyber incidents and the results of penetration and red team tests.

d. ensuring that staff who are responsible for implementing the FMI's cyber resilience framework have suitable skills, knowledge, experience and resources and are sufficiently informed and empowered to make timely decisions; and

e. continuously reviewing the skills, competencies and training requirements to ensure that the FMI has the right set of skills as technologies and risks evolve.

15. Senior management should ensure that all employees understand their role in mitigating cyber risk and have access to the appropriate level of training.

16. The board and senior management should, as appropriate, develop succession plans for high-risk staff (e.g., senior management, system administrators, software developers and critical system operators). They should also develop recruitment requirements for key cyber roles that include suitable cyber skills, knowledge and experience in alignment with defined succession plans.

17. Senior management should help plan and participate in industry-wide exercises designed to test and strengthen the cyber resilience of the FMI's ecosystem.

1.4.2 Culture

18. The board and senior management should cultivate a strong level of awareness of and commitment to cyber resilience, leading by example to promote a culture that recognizes that staff at all levels have important responsibilities for ensuring the FMI's cyber resilience.

19. The FMI's senior management should ensure its cultural awareness of cyber risk improves continuously across the organization. Training programs should be updated regularly to take the evolving threat landscape of the ecosystem into account.

20. The FMI should establish policies that set out consequences for employees and contractors of failure to comply with cyber security policies. The policies should be clear and commensurate with the risk and context of a given situation.

1.4.3 Skills and accountability

21. To carry out their responsibilities in relation to the cyber resilience strategy and framework, the FMI's board and senior management should include members that possess the appropriate balance of skills, knowledge and experience to understand and manage the cyber risks facing the FMI. The board should be sufficiently informed and capable of credibly challenging the recommendations and decisions of designated senior management. To achieve this, the FMI should:

    a. appoint an individual with cyber security expertise to the board; and

    b. ensure that board members and senior management understand their roles and responsibilities in relation to cyber resilience (including their role in cyber risk management) and, if necessary, receive training.

22. The board and senior management should appoint a senior executive, such as a Chief Information Security Officer, who would be responsible and accountable for executing the cyber resilience framework within the organization.

23. The FMI should ensure that this senior executive has:

    a. sufficient authority and access to sufficient resources (people and technology);

    b. access to the board;

    c. operational independence from other IT operations; and

    d. the requisite knowledge and expertise to competently plan and execute the FMI's cyber resilience initiatives.

2 Identification

2.1 Preamble

Given that an FMI's operational failure can negatively impact financial stability, it is crucial that FMIs identify which of their operations and supporting information assets should, in order of priority, be protected against compromise. The ability of an FMI to understand its internal situation and external dependencies is key to being able to effectively respond to potential cyber threats that might occur. This requires an FMI to know its information assets and understand its processes, procedures, systems and all dependencies to strengthen its overall cyber resilience posture.

This section outlines how an FMI should identify and classify business processes, information assets and external dependencies and conduct risk assessments.

2.2 Identification and classification

It is important that the FMI understand which of its business functions and related processes are critical to its core operations and identify the information assets supporting them. Risk assessments should be carried out to identify what should be prioritized from a cyber resilience perspective.

2.2.1 Identification of business functions and processes

1. An FMI should have a process to identify and document its business functions, supporting processes and interdependencies (internal and external), including processes that are dependent on third-party service providers. The FMI should conduct a business impact analysis to quantify the impacts of disruptions on the FMI's critical operations. Identified business functions and processes should be classified in terms of criticality and associated with the FMI's operational reliability objectives. This information should be used to guide the FMI's prioritization of its protective, detective, response and recovery efforts.

2.2.2 Identification of information assets and related access

2. An FMI should be able to identify the information assets[9] supporting its business processes. It should:

    a. establish a standard for categorizing information and information systems according to the FMI's level of concern for confidentiality, integrity and availability;

    b. identify and maintain a current and centrally managed inventory of its information assets and system configurations in order to know at all times the assets that support its business functions and processes; and

    c. develop and maintain a current network diagram, illustrating:

        i. network resources (including IP addresses and subnets);

        ii. connected components; and

        iii. links to internal and external services (including interconnections with other stakeholders, internet-facing services, cloud services and any other third-party systems).

3. The FMI should adopt and apply a cyber security risk assessment process and maintain a risk register to document and monitor risks. The risk assessment process should identify the conditions under which assessments must be conducted and/or updated (e.g., system development and renewal, emerging threats and identified vulnerabilities within the FMI's systems or infrastructure). The risk register should identify and classify the risks in terms of criticality.

4. The FMI should conduct and document risk assessments of its information assets in accordance with its cyber security risk assessment process.

5. Following the completion or update of a risk assessment, the FMI should consult and update its risk register with the results. These results should drive the selection and implementation of security controls, prioritizing them according to the risks the FMI faces.

6. An FMI should maintain a central repository of individual and system accounts and permissions. The repository should:

    a. identify access rights to information assets and their supporting systems;

[9] As defined in the Cyber Guidance, an information asset is "any piece of data, device or other component of the environment that supports information-related activities." Information assets include data, hardware and software and are not limited to those that are owned by the FMI. They also include those that are rented or leased, and those that are used by service providers to deliver their services.

b. contain applicable information to assist the FMI in identification of anomalous activity:[10] and

c. be protected from unauthorized access and modification.

2.2.3 Regular review and update

7. An FMI should integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes and functions, its individual and system credentials, and its inventory of information assets so that that they remain current, accurate and complete.

2.3 Interconnections

The identification of an FMI's critical business processes and the information assets supporting them should extend to the entities in its ecosystem. An FMI's systems and processes are directly or indirectly interconnected with the systems and processes of the entities within its ecosystem. The cyber resilience of those entities could therefore have significant implications in terms of the cyber risk that the FMI faces, particularly since the significance of the risks they may pose is not necessarily proportionate to the criticality of their business relationship with the FMI.

8. The FMI should identify the cyber risks that it bears from or poses to entities in its ecosystem and coordinate with relevant entities, as appropriate. This may involve identifying vulnerabilities and threats that they share and taking appropriate measures collectively to address such risks, with the objective of improving the ecosystem's overall resilience.

9. To identify and assess the risks to the FMI from participants' interconnections, the FMI should consider a broad range of potential threat vectors and risks that could lead to a potential compromise of the FMI's key business functions. This process should include determining the likelihood of a potential threat occurring, assessing the impact in the event the threat is realized and analyzing the risk to the FMI. The FMI should also assess potential risks to the FMI's ecosystem that could arise from participant interconnections.

10. To identify and assess the risks from interconnections with third-party service providers, the FMI needs to understand the service provider's services and processes, including details on the services it provides the FMI and on how it will deliver the services. The FMI may need to rely on various sources to gather this information (e.g., publicly available information, self-assessments, third-party assessments) to understand, identify and assess the risks.

[10] Anomalous activity is any actions that are outside of what is expected, as measured against what "normally" should be happening.

3 Protection

3.1 Preamble

Cyber resilience depends on effective security controls and system and process design that protect the confidentiality, integrity and availability of an FMI's assets and services. These measures should be proportionate to an FMI's threat landscape and systemic role in the financial system, and consistent with its risk tolerance.

This section provides guidance on how the FMI should implement appropriate and effective safeguards in line with leading cyber resilience and cyber security practices to prevent, limit or contain the impact of a potential cyber event.

3.2 Protection of processes and assets

Protection of the FMI's processes and assets requires FMIs to adopt an approach of resilience by design, establish strong information and communication technology (ICT) controls, and employ layered defences.

3.2.1 Resilience by design

An FMI should consider cyber resilience at the earliest stage of system design and development, as well as throughout the system development life cycle. This will minimize vulnerabilities in software and hardware and ensure that the appropriate security controls are incorporated into systems and processes from their inception. If the system or any of its components are acquired from, or operated by, a third-party supplier, the FMI should obtain assurance that the vendor has applied the appropriate security controls.

1. The FMI should:
    a. adopt a system development methodology that embeds the resilience-by-design approach when designing, building, acquiring or modifying its systems, processes and products. At each stage of development, the FMI should manage its cyber risk and integrate resilience based on the results of risk analysis.
    b. establish and communicate principles for engineering secure systems and ensure processes and procedures are established, documented, maintained and applied to information system implementation efforts.
    c. when designing, developing and acquiring its systems and processes, capture security requirements alongside system and process requirements in order to identify the security controls necessary for protecting its systems, processes and data.

d. separate[11] development, testing and production environments to reduce operational risk. Each environment should be appropriately secured according to the FMI's security standards.

e. to the extent feasible and practical, ensure that the testing environment closely mirrors the production environment, especially with respect to its software, network configurations and hardware supporting critical systems.

f. review and rigorously test business critical applications, systems and networks against the FMI's security standards to ensure there is no adverse impact on organizational operations or security. Rigorous testing may include, for example, functional security testing of critical systems and software to determine if they behave as expected, boundary testing, robustness and fault tolerance testing, performance and load testing, data flow testing, and use-case testing. Ensure security testing is included within the system's acceptance testing programs for new information systems, upgrades and new versions.

g. limit attack surfaces as much as possible by, for example, disabling unnecessary or unused functionality and/or services and blocking software behaviours that are commonly abused by attackers or malware.

h. ensure changes to systems within the development life cycle are controlled through formal change control processes and procedures.

3.2.2 Controls

2. The FMI should establish policies and procedures that support the implementation of a comprehensive and appropriate set of protection controls that will allow it to achieve the cyber resilience objectives needed to maintain continuous operations, protect its assets and meet its business requirements. In selecting its ICT controls, the FMI is expected to use leading-practice cyber resilience standards such as those from NIST and ISO. The ECR is not intended to replace the FMI's existing standards.

3. The FMI should implement these controls based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections, in accordance with the risk assessment conducted in the identification phase.

While ICT controls are not the focus of the ECR, the following subsections provide a non-exhaustive set of important controls that an FMI should consider. The set of controls that an FMI chooses to implement will reflect a number of FMI-specific factors.

3.2.3 Strong ICT controls: Examples

[11] Physically and/or logically.

3.2.3.1 Protecting information—data and information protection controls

4. To ensure the confidentiality, integrity and availability of the FMI's data and information at rest and in use, the FMI should implement strong data and information protection controls. Examples include:

    a. protection against malware. Protection mechanisms should include scanning, blocking and/or quarantine at network entry and exit points, email gateways, servers and end systems. The FMI should update malicious code protection mechanisms whenever new releases are available and should apply the updates in accordance with its change and configuration management policies and procedures. Protection should include detection and mitigation of phishing attacks. FMI personnel should be trained on the effective use of anti-malware software and should be aware of phishing threats.

    b. integrity verification tools[12] to detect unauthorized changes to critical input files from internal and external sources (e.g., participating entities).

    c. data encryption commensurate with the FMI's criticality, sensitivity and risk assessment processes.

    d. encryption in line with recognized standards and processes, which cover aspects such as algorithm, key length, key generation and key management.

    e. physical protection of the equipment used to generate, store and archive keys.

    f. regular scans of its production environment to identify potential vulnerabilities and seek opportunities to upgrade its legacy technologies. Controls and additional defence layers should be implemented and tested to protect unsupported or vulnerable systems.

    g. validity checks performed for all information inputs in applications, in particular, for web-facing applications. Information inputs should be checked for valid syntax, data types, length, ranges and acceptable values.

    h. prevention of unauthorized disclosure, modification, removal or destruction of information stored on media.

    i. secure disposal of media when no longer required, using formal procedures.

    j. when transporting media, protection of information stored on the media against unauthorized access, misuse or corruption.

    k. assurance that any sensitive data and licensed software has been removed or securely overwritten before disposal or reuse of devices and/or media.

[12] For example, cryptographic hashes or digital signatures.

l. establishment and enforcement of a clear desk policy for papers and a clear screen policy for information processing facilities. Removable storage media should be stored in accordance with corporate policy.

3.2.3.2 Protecting information—communications and network security controls

5. The FMI should implement strong communications and network security controls. Examples include:

   a. secure network protocols and encryption,[13] when supported by a risk assessment, to protect the confidentiality and integrity of information exchanged within its network and beyond, including remote connections and third-party interconnections.

   b. a broad range of technologies and tools to detect and block actual and attempted attacks or intrusions, including those from authorized third-party connections (e.g., participants' networks). The FMI may use intrusion detection or prevention systems, end-point security solutions[14] or any other relevant solutions,[15] in particular, on devices and in environments used for accessing the FMI network remotely.

   c. controls that manage or prevent non-controlled devices from connecting to the FMI's logical internal network (including its remote access connectivity), ensuring that network access is restricted to authorized devices and that sessions are protected from eavesdropping, denial of service, spoofing, etc. The FMI's network infrastructure should be scanned regularly to detect rogue devices and access points.

   d. protection of critical information systems against denial of service attacks, including massive distributed denial of service (DDoS) attacks, to prevent disruption to the FMI's critical services. The FMI may use a variety of technologies, including, for example, boundary protection devices, third-party cloud DDoS protection services, and increased or emergency capacity and bandwidth to reduce the susceptibility to denial of service attacks.

   e. assurance that protection extends to the FMI's entire attack surface and that supporting or extended infrastructure[16] that may be used as an attack vector into the critical infrastructure is also formally authorized, monitored and controlled.

3.2.3.3 Configuration and change management

6. The FMI should have a configuration and change management policy, process and procedures in place. The configuration and change management process should be based on

---

[13] For example, transport layer security, internet protocol security or other virtual private networks.

[14] For example, antivirus software, a firewall, a host intrusion detection system or a host intrusion prevention system.

[15] For example, an access gateway or a jump box.

[16] For example, the use of voice over internet protocol, video conferencing, collaboration services and devices, smartphones and apps, etc.

well-established and industry-recognized standards and best practices (e.g., an information technology infrastructure library). Among measures to put in place, the FMI could:

a. establish a change advisory board, comprising key stakeholders (including business and IT management) to approve and prioritize the changes after considering the security and stability implications of the changes to the production environment.

b. monitor changes to the organization, business processes, information processing facilities and systems that affect cyber security to ensure they are controlled.

c. test, validate and document changes to the information system before implementing them into production (this might include, for example, integration tests, regression tests, user acceptance tests, etc.). The changes to information systems include, but are not limited to, modifying hardware, software or firmware components and systems and security configuration settings.

d. implement automated mechanisms to prevent changes and patches that have not been pre-approved from being installed on the information system.

e. establish baseline[17] system and security configurations for information systems and system components (including devices used for accessing the FMI network remotely) that:

    i. are documented, formally reviewed and regularly updated to adapt to the FMI's evolving threat landscape;

    ii. employ automated mechanisms (e.g., hardware and software inventory tools, configuration management tools, network management tools) to help maintain an up-to-date, complete, accurate and readily available baseline;

    iii. enable logging of security events; and

    iv. are configured to run essential capabilities only, with unnecessary system functions and services disabled or uninstalled.

f. maintain control over the types of software installed by identifying permitted and prohibited actions regarding software installation. For critical systems, the FMI should employ software whitelisting capabilities configured with a deny-all, permit-by-exception policy.

g. put necessary procedures in place to ensure that changes are implemented correctly and efficiently.[18]

h. analyze proposed system changes for potential security impacts prior to change implementation.

---

[17] NIST 800-53 R.4 defines baseline configuration as "a documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures."

[18] For example, code review and unit testing.

i. ensure that only authorized and qualified individuals can initiate changes to information systems, including upgrades and modifications.

j. ensure that processes are in place to schedule change implementation and communicate to those impacted prior to implementation, including consulting them when necessary.

k. have processes to identify, assess and approve genuine emergency changes (those that require immediate action). Post-implementation reviews should be conducted to validate that emergency procedures were appropriately followed and to determine the impact of the emergency change.

l. have the necessary processes and procedures for rolling back quickly when changes or patches fail. Any changes to the production environment must have an associated fall-back plan, when applicable.

3.2.3.4 Security settings consistent with levels of protection

7. The FMI should configure ICT systems and devices with security settings that are consistent with the expected level of protection. Examples of the types of controls that would achieve this objective are:

   a. establishment and documentation of baseline system security configuration standards to facilitate consistent application of security settings to operating systems, databases, network devices and enterprise mobile devices within the ICT environment. The FMI's baseline system security configuration standards should prescribe the technical IT security controls, parameters, features and specifications required to achieve the FMI's cyber security goals for the protection of information assets and technology-based solutions.

   b. integration of standards when planning, designing, building and maintaining systems and/or solutions.

   c. regular enforcement checks to ensure that non-compliance with such standards is promptly rectified.

   d. a formal, risk-based process for handling and approving any exceptions when a solution is unable to comply with a standard.

   e. periodic review of the baseline configuration standards and updates as needed.

3.2.4 Layered protection that facilitates response and recovery

8. The FMI's protective controls should enable monitoring and detection of anomalous activity. The FMI should:

   a. define and document the baseline profile of system activities, proportionate to risk, to help detect deviation from the baseline (e.g., anomalous activities and events). The baseline profile should address system-level technical activities (such as normal network traffic patterns, account usage and access patterns) and the system's

business activities (such as participants' normal or expected transaction frequency, size, timing and volume).

b. develop the appropriate capabilities, including the people, processes and technologies, to monitor and detect anomalous activities and events, by setting appropriate criteria, parameters and triggers to enable alerts. This may include, for example, adding functionality in the system's or application's business logic to detect unusual transactions[19] or behaviour,[20] or implementing advanced data analytics of trends and notifying the FMI when events occur outside of the normal trend.

c. use correlated log analysis, alerts and traffic flows to proactively take the appropriate measures to improve its cyber resilience capabilities.

9. To contain anomalous activity, the FMI should develop the appropriate capabilities, where possible and practical, to block suspect activity at the application and/or network.

10. To segregate systems and data of varying criticality, the FMI should:

a. establish a secure boundary that protects its network infrastructure.[21] The secure boundary should identify trusted and untrusted zones according to the cyber risk profile and criticality of information assets contained within each zone. Appropriate access requirements should be implemented within and between each security zone according to the principle of least privilege. A deny-all, permit-by-exception traffic policy should be used between zones where possible.

b. manage and control networks to protect information in systems and applications.

c. use a separate and dedicated logical network for information system administration.[22]

d. design its network connection infrastructure in a way that allows connections to be segmented or severed instantaneously to prevent contagion and/or lateral movement arising from cyber attacks. The FMI should ensure there are appropriate procedures to isolate or block its third-party connections (in a timely manner) if there is a cyber attack and/or a risk of contagion.

e. implement automated mechanisms that can isolate affected information assets in the case of an adverse event.

3.3 Interconnections

Third-party security management ensures protection of the FMI's assets that are accessible by participants, service providers, linked FMIs, vendors or other entities in its ecosystem, while

[19] For example, transactions that are unusually large or small, frequent or infrequent, out of sequence, etc.

[20] For example, activity conducted by unusual persons, at unusual times, from unusual locations.

[21] For example, by using tools such as a router, firewall, intrusion prevention system or intrusion detection system, virtual private network, demilitarized zone or proxies, etc.

[22] For example, a virtual local area network segment and internet protocol subnet.

maintaining an agreed level of information security and service delivery in line with service agreements to ensure disruptions to the FMI are minimized.

3.3.1 Risks from interconnections

11. Because of its systemic importance and unique position in the financial system, the FMI should implement protective measures to mitigate risks arising from the entities within its ecosystem. The appropriate controls for each entity will depend on the results of the risk assessment from the identification phase, incorporating the risk that arises from the connected entity and the nature of the FMI's relationship with the entity.

3.3.1.1 Participation requirements

12. An FMI should specify participation requirements as needed to ensure it can achieve its cyber resilience objectives. Areas where the FMI should impose requirements include:[23]

    a. connectivity restrictions,

    b. access control and privileged account management,

    c. identification and authentication management,

    d. confidentiality and integrity protection via encryption,

    e. vulnerability and patch management,

    f. detection and response management, and

    g. security awareness and training.

13. The FMI should obtain assurance from its participants that they meet the FMI's cyber resilience requirements. This can be achieved by requiring participant self-attestations, completed regularly, or asking participants for external third-party certifications of the participant's resilience.

3.3.1.2 Third-party cyber resilience

14. The FMI should obtain assurance from its third-party service providers and vendors such as ICT suppliers (collectively, third parties) that they meet its cyber resilience requirements. In negotiating or renewing its contracts with third parties, the FMI should ensure that provisions supporting the FMI's cyber resilience objectives are agreed upon and documented. Contracts should address items such as:

    a. validation of security capabilities. The FMI should require a third party to provide an assessment or validation of its security capabilities. For example, an FMI could request a self-assessment (e.g., self-assessment against PFMI Annex F or a questionnaire developed by the FMI) or a third-party assessment such as a certification, accreditation or external audit.

---

[23] FMIs that provide payment clearing and settlement services should include requirements to reduce the risk of wholesale payments fraud related to endpoint security in accordance with the strategy published in May 2018 by the Committee on Payments and Market Infrastructure.

b. information security requirements for mitigating the risks associated with third-party access to the FMI's information assets.[24]

c. confidentiality and non-disclosure requirements.

d. information security risks associated with information and communications technology services and product supply chains.

e. notification of changes to service levels or security functionality.

15. The FMI should reassess risks, as appropriate, upon notification of changes to third party service levels or security functionality.

3.4 Insider threats

An insider threat is anyone who has knowledge of or access to the organization's infrastructure and information and who uses, either knowingly or inadvertently, the infrastructure or information to cause harm. Insider threats can put the FMI's employees, customers, assets, reputation and interests at risk.[25]

3.4.1 Security analytics

16. An FMI should implement measures to capture and analyze anomalous behaviour by people with access to its systems. It should employ data loss identification and prevention techniques to protect against the removal of confidential data from its network.

3.4.2 Changes in employment status

17. An FMI should conduct screening and background checks on new employees to mitigate insider threats. It should conduct similar checks on all staff at regular intervals throughout their employment, commensurate with staff's access to critical systems. The FMI should also establish processes and controls to mitigate risks related to employees terminating employment or changing responsibilities.

18. The FMI should embed cyber security at each stage of the employment life cycle, specifying security-related actions required during the onboarding of each employee and their ongoing management, and upon the termination of their employment. This includes:

    a. carrying out pre-employment background security checks on all candidates (employees and/or contractors) commensurate with their future role and depending on the criticality of the assets and information they might have access to in order to fulfill their duty. Contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

---

[24] Information assets include assets under the direct ownership of the FMI and assets that the FMI relies on for its critical business operations but are not owned by the FMI itself.

[25] Source: Canadian Centre for Cyber Security, "How to Protect Your Organization from Insider Threats," ITSAP.10.003 (February 2020).

b. ensuring that current employees and contractors comply with established policies, procedures and controls.

c. when an employee is changing responsibilities, ensuring that all access rights related to their previous position and not necessary for their new responsibilities are revoked in due time. Employees in sensitive positions (such as those who change to roles requiring privileged access to critical systems or who become high-risk staff) should be pre-screened.

d. establishing procedures to revoke all departing employees' access rights from the information assets in a timely manner. Upon termination of employment, staff should be required to return all assets that belong to the FMI, including important documentation.[26]

19. All employees, contractors and external parties should be required to wear some form of visible identification and to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.

20. The FMI should ensure that access to secure areas or confidential information processing facilities, including for external support personnel, is granted only as required. This access should be authorized and monitored.

3.4.3 Access control

3.4.3.1 Logical access

21. The FMI should ensure the following:

a. Each individual user's identity has been verified prior to account authorization and creation. If users are members of an external participating entity, the FMI should ensure that identity verification is performed by the participating entity and is specified as a requirement in the participant agreement.

b. All users[27] have been uniquely identified and authenticated so that actions and activities can be attributed to individual users.

c. Authenticators[28] have sufficient strength for their intended use, meaning that this strength is proportional to the criticality of the information system, application process and/or user role. Multi-factor authentication should be enforced for the most critical systems, processes and roles. For password-based authentication, the FMI should establish and enforce password requirements.[29]

---

[26] For example, equipment, software and authentication hardware, and documents and correspondence containing business processes, technical procedures and contact details, etc.

[27] Including users who are internal (e.g., employees and contractors) and external (e.g., FMI participants).

[28] For example, passwords, tokens, biometrics, public key infrastructure certificates or key cards.

[29] Such as minimum password complexity (e.g., length, types of characters, etc.), password lifetime and rules concerning password reuse.

d. User access to resources is established and administered in accordance with a formal access control model[30] that enforces an access control policy.[31] The selected model should ensure that access to resources is granted only to authorized individuals. The access control policy should include actions to revoke access to resources when an individual is no longer authorized.

e. The principle of separation of duties applies to application processes and/or transactions that may be at risk of fraud or misuse.[32] This principle requires that no single person should be permitted to perform all parts of these processes and/or transactions.

f. Processes are established to manage the creation, modification or deletion of user accounts and access rights. Such actions should be submitted to and approved by appropriate staff and should be recorded for periodic review.

g. Limits are established and enforced on the number of unsuccessful login attempts. Actions to take when the maximum number of attempts has been exceeded are also specified.[33]

h. An inventory of all individual and system accounts (in particular, privileged and remote access accounts) and their associated access rights is maintained.

i. Automated mechanisms are implemented to support the management of information system access accounts. These might include security controls embedded in the information system, allowing it to automatically disable and/or remove inactive, temporary and emergency accounts after a predefined period. They may also include dedicated tools such as identity and access management.

j. Appropriate staff are automatically notified when user access has been elevated to privileged access.

k. Specific procedures have been implemented to allocate privileged access on a need-to-use or an event-by-event basis.

l. Automated mechanisms are employed that allow account creation and modification and continuous monitoring and auditing of enabling, disabling and removal actions in order to notify appropriate staff when potential malicious behaviour or suspicious activity is detected. The FMI's authentication mechanisms follow industry best practices and are aligned with relevant standards.[34]

---

[30] For example, role-based access control, rule-based access control or attribute-based access control.

[31] The policy may be established within the access control mechanisms and enforced technically, or it may be established as an abstract (e.g., written) and enforced through manual procedures (e.g., adding users to groups in a role-based access control model).

[32] For example, high-value and/or high-volume transactions.

[33] For example, temporarily block, block until released by an administrator, etc.

[34] For example, NIST 800-53, ISO 27001/27002.

3.4.3.2 Physical access

22. The FMI should ensure the following:

    a. Security perimeters are defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

    b. Secure areas are protected by appropriate entry controls to allow access only to authorized personnel.

    c. Critical computing equipment is located and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access. Physical protection of critical computing equipment should include emergency power and lighting, fire suppression capabilities, temperature and humidity controls and water damage protection. Wireless access points and power and telecommunications cabling for critical systems should be protected from tampering and damage.

    d. Equipment is correctly maintained to ensure its continued availability and integrity.

3.5 Training

23. All employees (including senior management and board members) and contractors should be required to apply information security in accordance with the FMI's established cyber resilience policies, technical standards and procedures.

3.5.1 All FMI staff

24. The FMI should:

    a. ensure that all staff, permanent or temporary, receive training to develop and maintain appropriate awareness of and competencies for detecting and addressing cyber-related risks (e.g., spear phishing training).

    b. train staff on how to report any unusual activity and incidents (e.g., phishing attempts, requests for sensitive information or passwords, and requests from unidentified sources).

    c. ensure that its employees have a good understanding of the cyber risk they might face when conducting their jobs and their roles and responsibilities in protecting the FMI's assets, particularly critical systems.

    d. include cyber security awareness training in the onboarding program for new staff.

    e. provide appropriate user training for staff operating new systems or applications before these systems or applications become operational.

    f. ensure that staff are familiar with standard operating procedures.

g. assess the effectiveness of its training to determine whether the training and awareness positively influence behaviour and adapt the training as required.[35]

3.5.2 High-risk groups

25. The FMI should identify employees and contractors in high-risk groups, such as those with privileged system access or in sensitive business functions and provide them targeted information security training.

4 Detection

4.1 Preamble

An FMI's ability to recognise signs of a potential cyber incident, or detect that an actual breach has taken place, is essential to strong cyber resilience. Early detection provides an FMI with useful lead time to mount appropriate countermeasures against a potential breach and allows proactive containment of actual breaches. In the latter case, early containment could effectively mitigate the impact of the attack—for example, by preventing an intruder from gaining access to confidential data or exfiltration of such data. Given the stealthy and sophisticated nature of cyber attacks and the multiple entry points through which a compromise could take place, an FMI should maintain effective capabilities to extensively monitor for anomalous activities.

This section outlines safeguards and capabilities that an FMI should have to help it detect anomalous activity, cyber events and incidents.

4.2 Continuous monitoring

Continuous monitoring encompasses the technology, processes, procedures, operating environments and people necessary to monitor and detect anomalous activity and events in real time (or near real time).

1. The FMI should implement continuous monitoring against the baseline profile of system activities discussed in Section 3 in 3.2.4.

2. The FMI should:

    a. develop and implement automated detection mechanisms (e.g., a security information and event management system) that correlate all the network and system alerts and any other anomalous activity across its business units.

    b. have capabilities to monitor:

        i. user activity, exceptions and cyber security events; and

        ii. network connections, external service providers, devices and software.

[35] For example, social engineering or phishing tests.

c. continuously monitor and inspect the network traffic, including remote connections, and endpoint configuration and activity to identify potential vulnerabilities or anomalous events in a timely manner.

d. compare the network traffic and the endpoint configuration with the expected traffic.

e. define alert thresholds for its monitoring and detection systems in order to trigger and facilitate the incident response process.

f. ensure that its detection capabilities, baseline profile of system activities and the criteria, parameters and triggers are regularly reviewed, tested and updated appropriately in a controlled and authorized manner.

g. continuously monitor connections among information assets throughout their life cycles, and collect, store and analyze these data to support incident response and forensic investigation.

4.3 Comprehensive scope of monitoring

The necessary scope of monitoring is both broad and deep. It encompasses business functions, transactions and application processes, as well as system and network devices and communications. It addresses internal activity and threats, as well as threats from external and third-party sources.

3. The FMI should:

   a. collect, monitor and analyze patterns and behaviour (e.g., network use patterns, work hours and known devices, etc.). This will help to identify anomalous activities and evaluate the implementation of emerging solutions (e.g., data analytics, machine learning and artificial intelligence, etc.) and controls to support detection and response to insider threat activity in real time.

   b. ensure that its detection capabilities are informed by threat and/or vulnerability information, which can be collected from different sources and providers.

   c. implement an advanced threat detection capability to identify known threats and increase the likelihood of identifying those threats that are attempting to exploit previously unknown (zero-day) vulnerabilities and those that are using previously unknown attack chains, methods and techniques.

   d. ensure that it understands and has modelled threats of misuse by insiders and trusted third parties and has developed capabilities to detect these threats within applications, databases, systems and networks.

   e. have processes to monitor activities that are not in line with its security policy and might lead to loss of confidentiality, loss of integrity, data theft or destruction.

4.4 Layered detection

The ability to detect an intrusion early is critical for swift containment and recovery.

4. The FMI should apply detection capabilities by instituting multi-layered detection controls covering people, processes and technology.[36] Each layer should serve as a safety net for preceding layers to enable them to detect, delay and disrupt an attacker's progress through an attack chain or sequence. An effective intrusion detection capability could assist an FMI in identifying deficiencies in its protective measures for early remediation.

5. The FMI should continuously explore new technologies and techniques to inhibit lateral movement. These technologies and techniques should trigger alerts and inform the FMI of potential malicious activity.

4.5 Incident response

An FMI's monitoring and detection capabilities should facilitate its incident response process and support information collection for the forensic investigation process.

6. The FMI's monitoring and detection capabilities should trigger a notification to appropriate staff.

7. To facilitate forensic investigation, the FMI should ensure that:

    a. detected anomalies and events are recorded in event or system logs;

    b. the content of the logs includes the necessary information to support investigation (e.g., event type, time, user/address, etc.);

    c. there is enough storage capacity for the necessary logs; and

    d. audit information and tools are protected against unauthorized access, modification and deletion.

8. The FMI should ensure that its logs are backed up at a secure location with controls in place to mitigate the risk of alteration.

9. The FMI should implement a time synchronization capability to ensure that correlated logs have consistent times.

10. The FMI should have a process to collect, centralize and correlate event information (including anomalous activity) from multiple sources and log analysis to continuously monitor the IT environment (e.g., databases, servers and end points, etc.). This capability could be achieved through a security operations centre (SOC), network operations centre or equivalent.

---

[36] Examples of such controls include the following as applied to (1) people—audits and reconciliations, behavioural analytics, job rotation, logging and monitoring; (2) processes—auditing, deviation analysis, logging and monitoring; and (3) technology—continuous security monitoring, endpoint detection and response, intrusion detection system, intrusion protection system, malware detection system.

5 Response and recovery

5.1 Preamble

Financial stability may depend on an FMI's ability to settle obligations when they are due. Therefore, an FMI's arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them. Continuity planning is essential for meeting related objectives.

This section provides guidance on an FMI's capabilities to respond to and recover from cyber attacks.

5.2 Incident response, resumption and recovery

FMIs are expected to develop robust cyber incident handling capabilities to reduce the impact that a cyber incident could have on the FMI and its ecosystem. FMIs should have plans that detail appropriate actions for the FMI to take at various stages of its management of a cyber incident, which include response, resumption and recovery.

5.2.1 Planning and preparation

1. The FMI should develop comprehensive cyber incident response, resumption and recovery plans to manage cyber security incidents.[37] These plans should aim to limit damage and prioritize resumption and recovery actions that facilitate the processing of critical transactions and reduce recovery time and costs. The response plan sets out actions to be conducted immediately upon detection of a cyber incident. The resumption plan incorporates actions to restore and resume the FMI's critical business operations, possibly in a state of diminished capacity, that would be taken as soon as it is safe and practicable to do so (and with two hours as the target objective). The recovery plan sets out actions that allow the FMI to safely return to a fully functional normal operating state, which may take some time.

2. Response, resumption and recovery plans should define policies and procedures as well as roles and responsibilities for escalating, responding to and recovering from cyber incidents.

3. In developing its plans, the FMI should:

    a. incorporate a range of extreme but plausible scenarios to assess the potential impact such scenarios may have on the FMI and the broader ecosystem; and

    b. consult and coordinate with all relevant business units and external stakeholders.

[37] An FMI may not have separate plans for response, resumption and recovery, but its plan(s) should, nevertheless, separately detail the steps required to respond to a cyber incident, resume operations and recover.

4. The FMI should regularly update its plans. This includes:

    a. reviewing its range of scenarios;

    b. conducting business impact assessments in line with the evolving threat landscape; and

    c. incorporating lessons learned from past cyber incidents, including findings from root cause analyses.

5. The FMI should regularly test its response, resumption and recovery plans against a range of scenarios.

6. The FMI should consult with relevant external stakeholders (e.g., participants, service providers and other FMIs) within the ecosystem to further enhance its response, resumption and recovery plans.

7. The FMI should implement processes to continuously improve its response, resumption and recovery plans, considering cyber threat intelligence sources (e.g., feeds), information shared within its ecosystem and lessons learned from previous events.

5.2.2 Resumption within two hours (i.e., two-hour RTO)

8. Objectives for resuming operations should be planned for and tested. In line with key consideration 17.6 of the PFMI, an FMI should design and test its systems and processes to enable:

    a. the safe resumption of critical business operations within two hours of a cyber disruption; and

    b. completion of settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios.

9. Planning to enable resumption within two hours of a cyber incident requires a detailed and comprehensive understanding of the FMI's business functions and processes. No single solution will work for all FMIs. An FMI should involve both the technical and business teams to carefully plan for risks specific to the FMI's design, critical functions and business processes. Despite having the capability to resume critical business operations within two hours, the FMI should exercise judgment (in agreement with regulatory/supervisory authorities and relevant stakeholders) when resuming operations. The FMI must consider whether resuming operations has the potential to escalate risks to the FMI or its ecosystem, while taking into account that completion of settlement by the end of day is crucial.

5.2.3 Contingency planning

10. While the FMI should plan to safely resume critical business operations within two hours of a disruption, it should also plan for scenarios in which this objective is not achieved. The FMI should analyze critical functions, transactions and interdependencies to prioritize

resumption and recovery actions that may, depending on the design of the FMI, help it to process critical transactions while remediation efforts continue. The FMI should also plan for situations in which critical people, processes or systems may be unavailable for significant periods—for example, by potentially reverting (where feasible, safe and practicable) to manual processing if automated systems are down.

11. The FMI should develop a contingency plan, based on the scenarios in which resumption within two hours is not achievable. This plan should:

    a. address how the FMI could achieve recovery objectives and restoration priorities;

    b. define roles and responsibilities; and

    c. set out options to reroute or substitute critical functions and/or services that may be affected for a significant period by a successful cyber attack.

12. The FMI must plan for how to operate in a diminished capacity or how to safely restore services over time, based on their relative priorities, and with accurate data.

5.2.4 Incident response and investigation

13. The FMI should have a comprehensive cyber incident response capability that includes detection and analysis; containment, eradication and recovery; and post-incident activity. Having this capability should allow the FMI to analyze cyber security incidents immediately upon their detection, while minimizing service disruption and allowing resumption, containment and recovery efforts to commence. This capability might include direct cooperative or contractual agreements with incident response organizations or providers to rapidly assist with mitigation efforts. It may also include direct involvement of the FMI business units to assist in prioritizing activities.

14. The FMI should also have capabilities, policies and procedures to perform a thorough investigation of a cyber attack, including root cause analysis and forensics. The FMI may use internal resources and/or third-party service providers with whom it has contractual agreements to ensure the investigation gets underway quickly upon detection of a cyber attack.

15. Upon detection and confirmation of a successful or attempted cyber attack, the FMI should deploy its investigative capability to determine the nature and extent of the attack as well as the damage inflicted.

16. While the investigation is ongoing, the FMI should take immediate actions to contain the cyber attack or attempted cyber attack to prevent further damage and commence efforts to resume operations based on its response planning. Investigation activities may extend over a medium- or longer-term period and are distinct from more immediate incident response activities, which focus on limiting damage, prioritizing resumption and allowing for completion of settlement by end of day.

17. The FMI should establish criteria and procedures for escalating cyber incidents to the board and senior management based on the potential impact and criticality of the risk.

18. The FMI should also have procedures to escalate investigations to law enforcement, as appropriate.

19. The FMI should train its staff so that they understand their role and responsibilities related to handling the digital evidence, ensuring it is not compromised and remains valid as per the requirements of the local jurisdiction.

5.2.5 Forensic readiness

20. The FMI should develop the capability to support or assist in forensic investigation. This capability should include engineering protective and detective controls to facilitate the investigative process. The FMI should establish relevant system logging policies that include required audit log content, time synchronization of logs and events, and log file retention periods.

21. The FMI should establish procedures for securely handling, collecting and preserving digital evidence, ensuring its authenticity and integrity so that forensic investigations may be performed after the event or after resumption of critical operations.

5.3 Design elements

In designing new systems and processes the FMI should consider how these systems and processes can support incident response activities. The design of business processes, information systems, and response and recovery controls has a significant influence on the FMI's ability to resume critical operations within two hours.

5.3.1 Design and business integration

22. System and process design and controls for critical functions and operations should support incident response activities as much as possible. The FMI should design systems and processes to limit the impact of any cyber incident, resume critical operations within two hours of a disruption, complete settlement by end of day and preserve transaction integrity.

23. The FMI should consider a range of scenarios and potential response actions and their implications when designing its systems and processes. The objective of resuming operations within two hours requires careful selection and implementation of techniques and methods for completing settlement and the technologies and tools for recovering system configuration and data. The solutions selected will depend on several factors, such as the design and complexity of the system, the frequency and volume of transactions and the life-cycle stage of the systems.[38] No single solution fits all FMIs and all critical systems.

---

[38] The life-cycle stage of an FMI's systems may be the most significant factor in the selection of solutions that facilitate rapid resumption. For those systems that are in early development and/or undergoing transformation or renewal, solutions may be built in throughout the system: in the business processes and human interface; applications; system software; and computing, storage and network infrastructures. For legacy systems, however, the selection of solutions may be severely limited and, in some cases, cost prohibitive. While recognizing these

5.3.2 Data integrity

24. The FMI should define and identify data critical for resumption of services that needs to be backed up. The data types that are necessary for resumption include not only transactional data but also other critical data, such as source code, business reference data and configuration data. The FMI should be able to recover these data within a predictable period.

25. The FMI should have plans to identify, in a timely manner, the status of all transactions and member positions at the time of a disruption, supported by corresponding recovery point objectives. Therefore, the FMI should design and test its systems and processes to enable recovery of accurate data following a breach. Information and data should be safeguarded by stringent protection and detection controls.

26. Recovery point objectives to support data integrity efforts should be consistent with the FMI's resumption time objective for critical operations.

27. Recovery point objectives and data recovery options should be established through close collaboration with the business and IT functions. This close collaboration can help an organization answer fundamental questions about how to conduct critical business processes under corruption scenarios.

28. The FMI's backup solutions should be configured to align with the frequency and volume of transactions. As an FMI performs thousands of transactions per hour each day, a solution that backs up only once per day will not provide adequate protection unless additional database transaction recovery solutions are also implemented.

29. The FMI's cyber resilience framework should include data recovery measures. The FMI should consider a range of options that could be used to recover data. The FMI should select these options based on detailed analysis of what data are critical to the FMI's operations, including what data the FMI would require to resume operations within two hours and how various cyber scenarios could impact the integrity of these data, including both loss and manipulation of data.

30. Backups should be protected at rest and in transit to ensure the confidentiality, integrity and availability of data. Backups should be tested regularly to verify their availability and integrity.

31. Examples of the range of data recovery options that the FMI should consider include, but are not limited, to:

    a. implementing database record recovery mechanisms, which might include record rollback and logging or rolling forward to correct corrupted data;

    b. conducting more frequent independent reconciliation of participants' positions;

---

challenges, the FMI should nonetheless seek solutions that incrementally reduce the resumption time as much as possible.

c. keeping a copy of all received and processed data and related information; and

d. using secure storage technologies to store the most critical files for resuming operations, which include critical transaction and reference data, configuration files and logs. Examples include data vaults (data storage that can be written to but not read without additional strong authentication and management tools) and write-once-read-many times drives.

5.4 Interconnections

An FMI's cyber incident response activities should be coordinated with its interconnected entities and stakeholders. The FMI should implement measures to facilitate such coordination and plan for how it will communicate and coordinate in the event of a cyber attack.

5.4.1 Data-sharing agreements

32. The FMI should have a data-sharing agreement with third parties and/or participants, where appropriate, to facilitate obtaining uncorrupted data from them, if necessary, for resuming its business operations in a timely manner and with accurate data.

33. The FMI should regularly review information-sharing rules, agreements and protocols to control the publication and distribution of such information and to prevent the disclosure of sensitive information that may have adverse consequences if disseminated improperly.

5.4.2 Contagion

34. In the event of a large-scale cyber incident, it is possible for an FMI to pose contagion risk (i.e., propagation of malware or corrupted data) to, or be exposed to contagion risk from, its ecosystem. The FMI should develop policies and procedures that define how it should work together with relevant interconnected entities to enable the resumption of operations (the first priority being its critical functions and services) as soon as it is safe and practicable to do so without causing unnecessary risk to the broader sector or the financial system.

5.4.3 Crisis communication

35. The FMI should develop a communication plan and procedures to communicate with participants, linked FMIs, authorities and others (e.g., service providers and media, where relevant). The FMI's communication plan should be informed by scenario-based planning and analysis as well as previous experience.

36. The FMI's incident response plan should identify internal and external stakeholders that must be notified, decision-making responsibilities and authorities, and information that must be shared and reported, and when this should take place.

37. The FMI should immediately notify relevant oversight and regulatory authorities of any cyber incident that could be material or systemic. In reporting cyber incidents to the Bank

of Canada, the FMI should follow the requirements of the Bank of Canada's Guideline for Cyber and Information Technology Incident Reporting.

38. The FMI should also have procedures to escalate investigations to law enforcement when there are indications of criminal intent (e.g., fraud, extortion).

5.4.4 Responsible disclosure policy

39. The FMI should have a policy and procedures to enable responsible disclosure of potential vulnerabilities and risks within its ecosystem as it responds in real time to a cyber attack or incident. In particular, the FMI should prioritize disclosures that could help participants and other stakeholders respond promptly and mitigate their own risk, which could benefit the ecosystem and overall financial stability.

6 Testing

6.1 Preamble

Testing is an integral component of any cyber resilience framework. All elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an FMI, and regularly thereafter. This includes the extent to which the framework is implemented correctly, operating as intended and producing desired outcomes. Understanding the overall effectiveness of the cyber resilience framework in the FMI and its environment is essential in determining the residual cyber risk to the FMI's operations, assets and ecosystem.

Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the FMI's cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cyber resilience posture and reduce or eliminate identified gaps.

This section provides guidance on what should be included in an FMI's testing program and how results from testing can be used to improve the FMI's cyber resilience posture on an ongoing basis. The scope of testing includes vulnerability assessments, scenario-based testing, penetration tests and tests using red teams.

6.2 Comprehensive testing program

An FMI should have a comprehensive testing program to validate the effectiveness of its cyber resilience framework. Testing is a tool that FMIs can use to identify flaws in security controls. However, due to the practical limitations of conducting security tests, passing such a test is not an indication that no flaws exist or that the system adequately satisfies security objectives related to confidentiality, integrity, authentication, availability, authorization and non-repudiation.

1. The FMI should establish and maintain a comprehensive testing program as an integral part of its cyber resilience framework. The testing program should be developed using a

risk-based approach and consist of a broad spectrum of methodologies, practices and tools for monitoring, assessing and evaluating the effectiveness of the core components of the cyber resilience framework.

2. The testing program should be regularly reviewed and updated, taking into account the evolving landscape of threats and the criticality of information assets.

3. The FMI should develop appropriate capabilities and involve all relevant internal stakeholders (including business lines and operational units) when implementing its testing program. Where applicable, these tests should include business continuity and incident and crisis response teams.

4. The FMI should also collaborate with the entities in its ecosystem to further improve its cyber resilience posture. This collaboration contributes to strengthening the resilience of the FMI's ecosystem.

5. The FMI should involve its board and senior management appropriately (e.g., as part of crisis management teams) and inform them of test results.

6. For continuous improvement of its cyber resilience posture, the FMI should establish policies and procedures to prioritize and resolve issues identified during the various tests and perform subsequent validation to assess whether gaps have been fully addressed.

6.2.1 Methodologies, practices and tools

7. The FMI should employ a variety of testing methodologies, practices and tools, including vulnerability assessments, scenario-based testing, penetration tests and red team tests (which may overlap partly or be combined).

6.2.1.1 Vulnerability assessment

8. The FMI should develop and regularly update a vulnerability management process to classify, prioritize and resolve potential weaknesses identified in vulnerability assessments and perform subsequent validation to assess whether gaps have been fully addressed.

9. The FMI's vulnerability management process should help identify exploitable weaknesses[39] in critical systems and technologies, and conditions that enable human error and accidents in critical functions, supporting processes and information assets.

10. The FMI should regularly conduct vulnerability scanning of its external-facing services and internal systems and networks. These scans should rotate among environments to reach all environments throughout the year.

11. The FMI should perform vulnerability assessments before any deployment or redeployment of new or existing services supporting critical functions, applications and

[39] An exploitable weakness is a susceptibility or flaw in a system that an attacker can access and exploit to compromise system security.

infrastructure components for fixing bugs and weaknesses. These assessments should be done consistently with change and release management processes in place.

12. The FMI should periodically conduct vulnerability assessments on running services, applications and infrastructure components. It should check for compliance with regulations, policy and configurations and monitor and evaluate the effectiveness of security controls to address the identified vulnerabilities.

13. The FMI should develop and adopt a range of effective practices and tools[40] as part of its vulnerability management process and have appropriate safeguards to manage them.

6.2.1.2 Scenario-based testing

14. The FMI should perform different scenario-based tests, including extreme but plausible scenarios, to evaluate and improve its incident detection capability as well as response, resumption and recovery plans. The latter should be subject to periodic review and testing. Scenario-based tests can take the form of tabletop exercises or simulations.

15. The FMI should design tests that:

    a. address an appropriately broad scope of scenarios, including simulation of extreme but plausible cyber attacks;

    b. are designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans;

    c. include data destruction, data integrity corruption, data loss, and system and data availability and

    d. cover breaches affecting multiple portions of the FMI's ecosystem in order to identify and analyze potential complexities, interdependencies and possible contagion at both the business and operational levels.

16. The FMI should use cyber threat intelligence (CTI) and cyber threat modelling to imitate the unique characteristics of cyber threats. It should also conduct exercises to test processes and the ability of staff to respond to unfamiliar scenarios, with a view to achieving stronger operational resilience.

17. The FMI's board and senior management should be engaged in the scenario-based testing, when appropriate.

6.2.1.3 Penetration tests

18. The FMI should carry out penetration tests to identify vulnerabilities that may affect its systems, networks, applications, people or processes. To provide an in-depth evaluation

[40] For example, a bug bounty program or static and dynamic code reviews.

of the security of the FMI's systems, these tests should simulate actual attacks on the systems.

19. Penetration tests should be conducted regularly and whenever there are major updates to or deployment of systems.

20. The FMI should involve all critical internal and external stakeholders in the penetration-testing exercises, as appropriate. These stakeholders could include application and system owners and business continuity and incident and crisis response teams.

21. The FMI should integrate testing practices in its enterprise risk management process with the aim of identifying, analyzing and fixing cyber security vulnerabilities stemming from new products, services or interconnections.

22. The FMI should perform security assessments and tests when applicable at all phases of the system development life cycle and at any level (business, application and technology) for the entire application portfolio, including mobile applications.

23. The FMI should adopt best practices and automated tools to support the processes and procedures to fix technical and organizational weaknesses identified during the testing exercises and to check for compliance with approved policy and configurations.

6.2.1.4 Red team testing

24. The FMI should challenge its own organization and ecosystem using so-called red teams to introduce an adversary perspective in a controlled setting. Red teams test for possible vulnerabilities and the effectiveness of an FMI's mitigating controls, including its people, processes and technology. A red team may consist of an FMI's own employees and/or outside experts, who are, in either case, independent of the function being tested. The red team should regularly conduct exercises and engage with its cyber defence team (e.g., blue team) to share its findings and make improvements to the FMI's cyber resilience posture.

25. The FMI should also employ appropriate cyber threat intelligence to inform its testing methods—for example, by designing tests to simulate advanced threat agent capabilities and extreme but plausible scenarios. The FMI should perform red team exercises using reliable and valuable CTI, based on specific and plausible threat scenarios.

6.3 Coordination

Identifying plausible complexities, dependencies and weaknesses in an FMI's response, resumption and recovery plans requires that the FMI coordinate with the entities in its ecosystem in testing these plans. This will help the FMI to improve its plans and ultimately the resilience of both the FMI and its ecosystem.

26. The FMI should, to the extent practicable and possible, promote, design, organize and manage exercises designed to test its response, resumption and recovery plans and processes. Such exercises should include FMI participants, critical service providers and linked FMIs, as appropriate.

27. The FMI should participate in industry-wide tests and exercises organized by relevant authorities. Achieving timely resumption of operations market-wide calls for an added dimension to testing exercises. Traditional isolated testing implicitly assumes that all other players are operating as usual. Removing that assumption helps an FMI identify plausible complexities, dependencies and weaknesses that may have been overlooked in its response, resumption and recovery plans. Accordingly, testing should include scenarios that cover breaches affecting multiple portions of the FMI's ecosystem.

7 Situational awareness

7.1 Preamble

Situational awareness refers to an FMI's understanding of the cyber threat environment within which it operates, and the implications of being in that environment for its business and the adequacy of its cyber risk mitigation measures. Strong situational awareness acquired through an effective cyber threat intelligence process can make a significant difference in the FMI's ability to pre-empt cyber events or respond rapidly and effectively to them. Specifically, a keen appreciation of the threat landscape can help an FMI better understand the vulnerabilities in its critical business functions and facilitate the adoption of appropriate risk mitigation strategies. It can also enable an FMI to validate its strategic direction, resource allocation, processes, procedures and controls with respect to building its cyber resilience. A key means of achieving situational awareness for an FMI and its ecosystem is an FMI's active participation in information-sharing arrangements and collaboration with trusted stakeholders within and outside the industry.

This section provides guidance for FMIs to establish a cyber threat intelligence process, analysis and sharing processes.

7.2 Cyber threat intelligence

Cyber threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted or enriched to provide the necessary context for decision-making processes.

1. The FMI should identify cyber threats that could materially affect its ability to operate or provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its own ecosystem. The FMI should include in its threat analysis those threats that could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. This analysis should be regularly reviewed and updated.

2. The FMI should:

    a. establish a process to gather and analyze relevant cyber threat information. To provide a business-specific context, the FMI should include internal and external business and system information in its analysis. This will turn information into usable

CTI that provides timely insights and informs enhanced decision-making by enabling the FMI to anticipate a cyber attacker's capabilities, intentions and modus operandi.

b. have the capabilities to analyze the information gathered and assess the potential impact on its cyber resilience framework.

c. use multiple sources of intelligence from internal and external sources,[41] correlated log analyses, alerts, traffic flows, cyber events across other sectors and geopolitical events. This will allow the FMI to better understand the evolving threat landscape and proactively take the appropriate measures to improve its cyber resilience capabilities.

3. To acquire threat information, the FMI should belong or subscribe to a threat and vulnerability information-sharing source and/or information-sharing and analysis centre that provides information on cyber threats and vulnerabilities. Cyber threat information gathered by the FMI should include analysis of the tactics, techniques and procedures of real-life attackers and information on geopolitical developments that may trigger cyber attacks on any entity within the FMI's ecosystem.

4. The FMI should use the threat information collected from different sources, while considering its own business and technical characteristics, to:

   a. determine the motivation and capabilities of threat actors (including their tactics, techniques and procedures) and the extent to which the FMI is at risk of a targeted attack from them;

   b. reassess the risk of technical vulnerabilities in operating systems, applications and other software, which could be exploited to perform attacks on the FMI;

   c. analyze cyber security incidents experienced by other organizations, including types of incidents, origin of attacks, targets of attacks, preceding threat events and frequency, and determine the potential risk these pose;

   d. analyze the likelihood of attack from these threat actors and the impact on the confidentiality, integrity and availability of the FMI's business processes and its reputation that could arise from such attacks; and

   e. analyze the impact of attacks already conducted by such threat actors on the ecosystem.

5. The FMI should continuously use the CTI that it has produced to assess and manage security threats and vulnerabilities in order to implement threat-informed cyber security controls in its systems and, more generally, enhance its cyber resilience framework and capabilities on an ongoing basis.

---

[41] For example, application, system and network logs; security products such as firewalls and intrusion detection systems; trusted threat intelligence providers; and publicly available information.

6. The FMI should:

    a. ensure that CTI is made available to appropriate staff who are responsible for mitigating cyber risks at the strategic, tactical and operational levels within the FMI.

    b. integrate and align its CTI process with that of its SOC. The FMI should use information gathered from its SOC to further enhance its CTI; and conversely, it should use its CTI to inform its SOC.

    c. use CTI to help inform and update its testing program to ensure it is in line with the latest threat landscape, attackers' modus operandi and vulnerabilities.

7.3 Information sharing

Information sharing is the voluntary act of exchanging data between various organizations, people and technologies, making information possessed by one entity available to another entity.

7. The FMI should define:

    a. its objectives for information sharing, in line with its business objectives and cyber resilience framework. At the very least its objectives should include collecting and exchanging information in a timely manner that could facilitate detection, response, resumption and recovery of its own systems and those of its participants during and following a cyber attack.

    b. the scope of information-sharing activities, including:

        i. the types of information available to be exchanged,

        ii. the circumstances under which sharing this information is permitted, and

        iii. those with whom the information can and should be shared.

    c. how information provided to the FMI will be acted upon (e.g., by employing the Traffic Light Protocol).

8. The FMI should establish and regularly review its information-sharing rules and agreements. It should implement procedures that allow information to be shared promptly and in line with the objectives and scope established above, while at the same time meeting its obligations to protect potentially sensitive data, the improper disclosure of which may have adverse consequences.

9. The FMI should establish and implement protocols with employees for sharing information relating to threats, vulnerabilities and cyber incidents, based on their specific roles and responsibilities.

10. The FMI should participate actively in existing information-sharing groups and facilities, including cross-industry, cross-government and cross-border groups, to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators related to cyber threats.

11. As appropriate, an FMI should consider exchanging information on its cyber resilience framework with trusted stakeholders to promote understanding of each other's approach to securing systems that are linked or interfaced. Such information exchange would facilitate an FMI's and its stakeholders' efforts to dovetail their respective security measures to achieve greater cyber resilience.

12. The FMI should participate in efforts to identify the gaps in current information-sharing mechanisms and seek to address them in order to facilitate an ecosystem-wide response to large-scale incidents.

13. The FMI should plan for information-sharing through trusted channels in the event of an incident, collecting and exchanging timely information that could facilitate the detection, response, resumption and recovery of its own systems and those of other entities within the FMI's ecosystem during and following a cyber attack.

8 Learning and evolving

8.1 Preamble

An FMI's cyber resilience framework needs to achieve continuous cyber resilience amid a changing threat environment. To be effective in keeping pace with the rapid evolution of cyber threats, an FMI should implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the FMI to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. An FMI should aim to instil a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

8.2 Ongoing learning

An FMI can strengthen its cyber resilience posture by incorporating learning from past cyber incidents, acquiring new knowledge and capabilities on an ongoing basis and assessing its capabilities with the appropriate metrics and maturity models.

8.2.1 Lessons from cyber events

1. The FMI should identify and categorize lessons learned (strategic, tactical and operational) from real-life cyber incidents, internal to the FMI and external, to advance its cyber resilience capabilities.

2. The FMI should incorporate these key lessons learned from real-life cyber incidents and/or from results of testing on the FMI and/or other organizations to improve its risk mitigation capabilities as well as its cyber response, resumption, recovery and contingency plans.

3. The FMI should ensure that cyber security awareness materials are available to staff when prompted by highly visible cyber events or by regulatory alerts.

4. The FMI should incorporate lessons learned into staff training, awareness programs and materials, on an ongoing and dynamic basis, and validate their effectiveness. The FMI should utilize industry and authority initiatives related to awareness and training, where possible.

8.2.2 Acquiring new knowledge and capabilities

5. The FMI should:

   a. ensure that it has a program for continuing cyber resilience training. This training program should be offered to board members and senior management and should be conducted at least annually. The annual cyber resilience training should include incident response, current cyber threats and emerging issues.[42]

   b. continuously review its skills, competencies and training requirements to ensure that staff have the right set of skills as technologies and risks evolve. This includes the ability to operate and implement any information technologies that the FMI acquires.

   c. explore new security approaches and technology capabilities that could improve its security posture. For example, some organizations are considering a zero-trust approach in response to a mobile workforce and mobile devices, adoption of cloud-based services, insider threats and breaches in network perimeter security.[43]

8.2.3 Predictive capacity

6. The FMI's cyber risk management practices should go beyond reactive controls and include proactive protection against future cyber events. The FMI should work toward achieving predictive capabilities by capturing data from multiple internal and external sources, defining a baseline for behavioural and system activity and analyzing activity that deviates from the baseline.

8.3 Cyber resilience benchmarking

8.3.1 Metrics

A cyber resiliency metric is derived from or relatable to some element of the Cyber Resilience Framework.

7. Metrics and maturity models allow an FMI to assess its cyber resilience maturity against a set of predefined criteria, typically its operational reliability objectives. This benchmarking requires an FMI to analyze and correlate findings from audits, vulnerability assessments, management information, incidents, near misses, tests and exercises[44] with external and

[42] For example, phishing, spear phishing, social engineering and mobile security.

[43] NIST, Zero Trust Architecture, Special Publication 800-207, August 2020.

[44] For example, penetration testing and red team testing.

internal intelligence. The use of metrics can help an FMI to identify gaps in its cyber resilience framework for remediation and allow an FMI to systematically evolve and achieve more mature states of cyber resilience.

8. The FMI should develop, monitor and analyze metrics to assess the performance and effectiveness of its testing program. The FMI should use the analysis conducted to further improve its testing program.

9. The FMI should develop a range of indicators and management information to regularly measure and monitor the effective implementation of the cyber resilience strategy and framework and its evolution over time. For example, relevant information and indicators could be:

    a. the percentage of the FMI's staff that have received cyber security training,

    b. the percentage of incidents reported within the required time frame per applicable incident category,

    c. the percentage of vulnerabilities mitigated within a defined time period after discovery, and

    d. yearly reports monitoring progress of indicators, etc.

Annex A: Glossary

The Glossary contains a set of terms used in the ECR that are defined in industry standards or in regulatory publications. A complete list of sources is found at the end of the Glossary. Within the ECR a number of these terms that qualified by the word "cyber", have broader applicability. In recognition of this, the Glossary may drop the qualifier. For example, the Glossary refers to risk appetite and risk tolerance rather than cyber risk appetite and cyber risk tolerance.

Term	Definition
Access control	Means to ensure that access to assets is authorized and restricted based on business and security requirements. Source: FSB Cyber Lexicon
Activity	Set of cohesive tasks of a process Source: NIST Glossary
Anomalous activity	Any actions that are outside of what is expected, as measured against what "normally" should be happening, occur. Source: UCF Compliance Dictionary
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: FSB Cyber Lexicon
Attack surface	The sum of an information system's characteristics in the broad categories (software, hardware, network, processes and human) which allows an attacker to probe, enter, attack or maintain a presence in the system and potentially cause damage to an FMI. A smaller attack surface means that the FMI is less exploitable and an attack less likely. However, reducing attack surfaces does not necessarily reduce the damage an attack can inflict. Source: CPMI-IOSCO
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Source: NIST Glossary
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. Source: NIST Glossary
Authorization	Access privileges granted to a user, program, or process. Source: CCCS

Term	Definition
Availability	Property of being accessible and usable on demand by an authorized entity. Source: FSB Cyber Lexicon
Baseline configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. Source: NIST Glossary
Breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed. Source: FSB Cyber Lexicon
Business impact analysis (BIA)	The process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs) and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions and plans. Source: Gartner Information Technology Glossary
Business process	A collection of linked activities that takes one or more kinds of input and creates an output that is of value to an FMI's stakeholders. A business process may comprise several assets, including information, ICT resources, personnel, logistics and organisational structure, which contribute either directly or indirectly to the added value of the service. Source: CPMI-IOSCO
Capabilities	People, processes and technologies used to identify, mitigate and manage an FMI's cyber risks to support its objectives. Source: CROE
Compromise	Violation of the security of an *information system*. Source: FSB Cyber Lexicon
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. Source: FSB Cyber Lexicon
Configuration management	The activity of managing the configuration of an information system throughout its life cycle. Source: CROE
Critical operations	Any activity, function, process, or service, the loss of which, for even a short period of time, would materially affect the continued operation of an FMI, its participants, the market it serves, and/or the broader financial system. Source: CPMI-IOSCO

Term	Definition
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Source: FSB Cyber Lexicon
Cyber attack	The use of an exploit by an adversary to take advantage of a weakness(es) with the intent of achieving an adverse effect on the ICT environment. Source: CPMI-IOSCO
Cyber event	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring. Source: FSB Cyber Lexicon
Cyber incident	A cyber event that: i) jeopardises 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. Source: FSB Cyber Lexicon
Cyber resilience	An FMI's ability to anticipate, withstand, contain and rapidly recover from a cyber-attack. Source: CPMI-IOSCO
Cyber resilience framework	Consists of the policies, procedures and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces. Source: CPMI-IOSCO
Cyber resilience strategy	An FMI's high-level principles and medium-term plans to achieve its objective of managing cyber risks. Source: CPMI-IOSCO
Cyber risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Source: NIST Glossary
Cyber risk management	The process used by an FMI to establish an enterprise-wide framework to manage the likelihood of a cyber-attack and develop strategies to mitigate, respond to, learn from and coordinate its response to the impact of a cyber-attack. The management of an FMI's cyber risk should support the business processes and be integrated in the FMI's overall risk management framework. Source: CPMI-IOSCO
Cyber risk profile	The cyber risk actually assumed, measured at a given point in time. Source: CPMI-IOSCO

Term	Definition
Cyber security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. Source: FSB Cyber Lexicon
Cyber threat intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Source: FSB Cyber Lexicon definition for "Threat Intelligence"
Data Integrity	A property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored. Source: NIST Glossary
Defence in depth	The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another. Source: NIST Glossary See layered protection and layered detection.
Demilitarized zone (DMZ)	Also referred to as a perimeter network, the (Demilitarized Zone) DMZ is a less-secure portion of a network, which is located between the Internet and internal networks. An organization uses a DMZ to host its own Internet services without risking unauthorized access to its private network. Source: Adapted from CCCS
Denial of service (DoS)	Prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users. Source: FSB Cyber Lexicon
Detect (function)	Development and implementation of the appropriate activities in order to identify the occurrence of a cyber event. Source: NIST CSF
Disruption	An event affecting an organisation's ability to perform its critical operations. Source: CPMI-IOSCO
Distributed denial of service (DDoS) attack	A denial of service that is carried out using numerous sources simultaneously. Source: FSB Cyber Lexicon
Ecosystem	A system or group of interconnected elements formed linkages and dependencies. For an FMI, this may include participants, linked FMIs, service providers, vendors and vendor products. Source: CPMI-IOSCO

Term	Definition
Enterprise architecture (EA)	The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture Source: NIST Glossary
Exploit	A technique to breach the security of a network or information system in violation of security policy. Source: NIST Glossary
Financial Market Infrastructure (FMI)	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions. Source: CPMI-IOSCO
Forensic investigation	The application of investigative and analytical techniques to gather and preserve evidence from a digital device impacted by a cyber-attack. Source: CPMI-IOSCO
Forensic readiness	The ability of an FMI to maximise the use of digital evidence to identify the nature of a cyber-attack. Source: CPMI-IOSCO
Governance (ECR risk management category)	The set of relationships between an FMI's owners, board of directors (or equivalent), management, and other relevant parties, including participants, authorities, and other stakeholders (such as participants' customers, other interdependent FMIs, and the broader market). Governance provides the processes through which an FMI sets its cyber resilience objectives, determines the means for achieving those objectives, and monitors performance against those objectives. Source: CPSS-IOSCO PFMI. Adapted from Principle 2: Governance, Explanatory Note 3.2.1
Identify (function)	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Source: NIST CSF
Identity and access management (IAM)	Encapsulates people, processes and technology to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. Source: FSB Cyber Lexicon
Incident response team (IRT) [also known as CERT or CSIRT]	Team of appropriately skilled and trusted members of the organization that handles incidents during their life cycle. Source: FSB Cyber Lexicon
Indicators of compromise (IoCs)	An artifact that serves as forensic evidence of potential intrusions on a host system or network. IoCs enable information security professionals and system administrators to detect intrusion attempts or other malicious activities. IOCs also provide actionable threat intelligence that can be shared within the ecosystem. Source: Adapted from Trend Micro

Term	Definition
Information asset	Any piece of data, device or other component of the environment that supports information-related activities. In the context of this report, information assets include data, hardware and software. Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services. Source: CPMI-IOSCO
Information system	Set of applications, services, information technology assets or other information-handling components, which includes the operating environment. Source: FSB Cyber Lexicon
Insider threat	An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. Source: NIST Glossary
Integrity	With reference to information, an information system or a component of a system, the property of not having been modified or destroyed in an unauthorised manner. Source: CPMI-IOSCO
Internet Protocol security (IPSec)	An OSI Network layer security protocol that provides authentication and encryption over IP networks. Source: NIST Glossary
Layered detection	An approach to cyber resilience in which the FMI applies multiple detection controls rather than relying on a single control. See layered protection and defense in depth. Source: Bank of Canada
Layered protection	As relying on any single defence against a cyber threat may be inadequate, an FMI can use a series of different defences to cover the gaps in and reinforce other protective measures. For example, the use of firewalls, intrusion detection systems, malware scanners, integrity auditing procedures and local storage encryption tools can serve to protect information assets in a complementary and mutually reinforcing manner. May also be referred to as “defence in depth”. Source: CPMI-IOSCO
Leading standards, guidelines and practices	Standards, guidelines and practices which reflect industry best approaches to managing cyber threats, and which incorporate what are generally regarded as the most effective cyber resilience solutions. Source: CPMI-IOSCO
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware. Source: CCCS

Term	Definition
Maturity model	A mechanism to have cyber resilience controls, methods and processes assessed according to management best practice, against a clear set of external benchmarks. Source: CPMI-IOSCO
Multi-factor authentication	The process of using two or more factors to achieve authentication. Factors include something you know (e.g., password or personal identification number); something you have (e.g., cryptographic identification device or token); and something you are (e.g., biometric). Source: NIST Glossary
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities. Source: FSB Cyber Lexicon
Operational resilience	The ability of an FMI to: (i) maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and (ii) recover to effective operational capability in a time frame consistent with the provision of critical economic services. Source: CPMI-IOSCO
Patch management	The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs. Source: NIST Glossary
Penetration testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an *information system*. Source: NIST Glossary
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. Source: NIST Glossary
Policy	Statements, rules or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component. Source: NIST Glossary
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of cyber incidents. Source: FSB Cyber Lexicon

Term	Definition
Recover (function)	Develop and implement appropriate activities and programs to maintain plans for cyber resilience, including to be able to restore any capabilities that were impaired due to a cyber security incident. Source: Adapted from NIST CSF
Recovery point objective (RPO)	The measurement of data loss that is tolerable to an organization. Source: CCCS
Recovery time objective (RTO)	Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations. Source: DRII Glossary for Resilience
Red team	An independent group that challenges the cyber resilience of an organisation to test its defences and improve its effectiveness. A red team views the cyber resilience of an FMI from an adversary's perspective. Source: CPMI-IOSCO
Red team testing	A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. Source: G-7 Fundamental Elements for Threat-led Penetration Testing
Resilience by design	The embedding of security in technology and system development from the earliest stages of conceptualisation and design. Source: CPMI-IOSCO
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. Source: NIST Glossary
Restore	To bring back to a former, original, or normal condition, as a system or data. Source: Bank of Canada
Resume	To recommence functions following a cyber incident. An FMI should resume critical services as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability. The plan of action should incorporate the use of a secondary site and be designed to ensure that critical ICT systems can resume operations within two hours following a disruptive event. Source: CPMI-IOSCO
Risk Appetite	The broad-based amount of risk an enterprise is willing to accept in pursuit of its mission/vision. Source: Adapted from NIST Glossary
Risk Assessment	The process of identifying, estimating, and prioritizing information security risks. Assessing risk requires the careful analysis

Term	Definition
	of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur. Source: Managing Information Security Risk, p. 6.
Risk register	A central record of current risks, and related information, for a given scope or organization. Current risks are comprised of both accepted risks and risks that have a planned mitigation path. Source: NIST Glossary
Risk tolerance	The acceptable level of variation (from the organization's risk appetite) relative to achievement of a specific objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite. Source: Adapted from COSO, Understanding and Communicating Risk Appetite
Risk-based approach	An approach whereby FMIs identify, assess and understand the risks to which they are exposed and take measures commensurate with these risks. Source: CPMI-IOSCO
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. Source: NIST Glossary
Security controls	A management, operational, or technical high-level security requirement prescribed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls are implemented using various types of security solutions that include security products, security policies, security practices, and security procedures. Source: CCCS
Security operations centre	A function or service responsible for monitoring, detecting and isolating incidents. Source: CPMI-IOSCO
Situational awareness	The ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. Source: CPMI-IOSCO
Social engineering	A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as

Term	Definition
	downloading and executing files that appear to be benign but are actually malicious. Source: NIST Glossary
Standard operating procedure (SOP)	A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event. Source: NIST Glossary
System development life cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. Source: NIST Glossary
Tactics, techniques and procedures (TTPs)	The behaviour of a *threat actor*. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly-detailed description in the context of a technique. Source: FSB Cyber Lexicon
Threat	A circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in an FMI's systems, resulting in a loss of confidentiality, integrity or availability. Source: CPMI-IOSCO
Threat actor	An individual, a group or an organisation believed to be operating with malicious intent. Source: FSB Cyber Lexicon
Threat assessment	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. Source: NIST Glossary
Threat vector	A path or route used by the *threat actor* to gain access to the target. Source: FSB Cyber Lexicon
Transport layer security (TLS)	An authentication and encryption protocol widely implemented in browsers and web servers. HTTP traffic transmitted using TLS is known as HTTPS. Source: NIST Glossary
Voice Over Internet Protocol (VOIP)	A term used to describe the transmission of packetized voice using the internet protocol (IP) and consists of both signaling and media protocols. Source: NIST Glossary
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Source: NIST Glossary

Term	Definition
Vulnerability assessment	Systematic examination of an information system and its controls and processes to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. Source: FSB Cyber Lexicon
Whitelisting	An implementation of a default deny all or allow by exception policy across an enterprise environment, and a clear, concise, rapid and efficient process for adding exceptions when required for mission accomplishments. Source: NIST Glossary
Zero-day attack	An attack that exploits a previously unknown hardware, firmware, or software vulnerability. Source: NIST Glossary

Sources (the shortened version or acronym used in the glossary is shown in parentheses):

Canadian Centre for Cyber Security, "Glossary," 2021. Available at https://cyber.gc.ca/en/glossary. (CCCS)

Committee on Payment and Settlement Systems and International Organization of Securities Commissions, "Principles for financial market infrastructures," April 2012. Available at https://www.bis.org/cpmi/publ/d101a.pdf. (CPSS-IOSCO PFMI)

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (CPMI-IOSCO), "Guidance on cyber resilience for financial market infrastructures," June 2016. Available at https://www.bis.org/cpmi/publ/d146.pdf. (CPMI-IOSCO)

Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Understanding and Communicating Risk Appetite," January 2012. Available at https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf. (COSO)

Department of Finance Canada, "G-7 Fundamental Elements for Threat-led Penetration Testing," October 2018. Available at https://www.canada.ca/content/dam/fin/documents/g7/G7-penetration-testing-tests-penetration-eng.pdf. (G-7 Fundamental Elements for Threat-led Penetration Testing)

Disaster Recovery Institute International (DRII), "Glossary for Resilience," 2020. Available at https://drii.org/resources/viewglossary. (DRII Glossary for Resilience)

European Central Bank (ECB), "Cyber resilience oversight expectations for financial market infrastructures," December 2018. Available at https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf. (CROE)

Financial Stability Board (FSB), "Cyber Lexicon," November 2018. Available at https://www.fsb.org/wp-content/uploads/P121118-1.pdf. (FSB Cyber Lexicon)

Gartner, "Information Technology Glossary," 2021. Available at https://www.gartner.com/en/information-technology/glossary. (Gartner Information Technology Glossary)

National Institute of Standards and Technology (NIST) Information Technology Lab Computer Security Resource Centre, "Glossary," May 2021. Available at https://csrc.nist.gov/glossary. (NIST Glossary)

National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 2018. Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. (NIST CSF)

National Institute of Standards and Technology (NIST), "Managing Information Security Risk," March 2011. Available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf. (NIST Managing Information Security Risk)

Trend Micro, "Definition," 2021. Available at https://www.trendmicro.com/vinfo/us/security/definition/a. (Trend Micro)

Unified Compliance Framework (UCF), "Compliance Dictionary," 2021. Available at https://compliancedictionary.com/. (UCF Compliance Dictionary)