नेपाल राष्ट्र बैंक
भुक्तानी प्रणाली विभाग

भु.प्र.वि./नीति/सूचना/०१/०८०/८१   मिति :- २०८०/०५/१०

श्री भुक्तानीसम्बन्धी कार्य गर्ने अनुमतिपत्रप्राप्त संस्थाहरु ।

विषय :- **Cyber Resilience Guidelines** जारी गरिएको सम्बन्धमा ।

विद्युतीय कारोबारमा आएको व्यापकतासंगै बृद्धि भएको साइबर जोखिमको पहिचान, विश्लेषण र व्यवस्थापनलाई प्रभावकारी र व्यवस्थित बनाउनका लागि **Cyber Resilience Guidelines** जारी गरिएको व्यहोरा अनुमतिपत्रप्राप्त बैंक तथा वित्तीय संस्था एवं भुक्तानी प्रणाली सञ्चालक र भुक्तानी सेवा प्रदायक संस्थाहरुको जानकारीका लागि अनुरोध छ ।

भवदीय,

(गुरुप्रसाद पौडेल)
कार्यकारी निर्देशक

बोधार्थ:

१. श्री नेपाल राष्ट्र बैंक, गभर्नरको कार्यालय ।
२. श्री नेपाल राष्ट्र बैंक, बैंक तथा वित्तीय संस्था नियमन विभाग ।
३. श्री नेपाल राष्ट्र बैंक, बैंक सुपरिवेक्षण विभाग ।
४. श्री नेपाल राष्ट्र बैंक, वित्तीय संस्था सुपरिवेक्षण विभाग ।
५. श्री नेपाल राष्ट्र बैंक, सूचना प्रविधि विभाग ।
६. श्री नेपाल बैंकर्स एसोशियसन ।
७. श्री डेभलपमेन्ट बैंकर्स एसोशियसन ।
८. श्री नेपाल वित्तीय संस्था संघ ।
९. श्री लघुवित्त वित्तीय संस्था संघ ।

NEPAL RASTRA BANK

Payment Systems Department

Cyber Resilience Guidelines

August, 2023

Contents

Acronyms

BFIs	Banks and Financial Institutions
BIS	Bank for International Settlements
COBIT	Control Objectives for Information and Related Technology
CPMI	Committee on Payments and Market Infrastructure
CRG	Cyber Resilience Guidelines
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
FMI	Financial Market Infrastructure
GCR	Guidelines on Cyber Resilience
ICT	Information Communications Technology
IOSCO	International Organization of Securities Commission
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LI	Licensed Institution by Payment Systems Department
NRB	Nepal Rastra Bank
PFMI	Principles for Financial Market Infrastructures
RTO	Resumption within two hours
SIEM	Security Information and Event Management
SOC	Security Operations Center
TLP	Traffic Light Protocol
TTE	Table Top Exercise
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

A. Introduction

Financial stability and public confidence in the financial system might both be significantly impacted by a cyber-attack on the financial system. In order to ensure financial stability, it is essential that financial market infrastructures (FMIs) operate safely and effectively. FMIs have the potential to spread financial shocks across national and international financial markets if they are not effectively managed, having a negative effect on the economy. In this regard, the security and effectiveness of the financial system depend on the cyber resilience of FMIs.

To provide guidance for FMIs to enhance their cyber resilience *Committee on Payments and Market Infrastructures (CPMI)* and the *International Organization of Securities Commissions (IOSCO)* has published *Guidance on cyber resilience for financial market infrastructures* (GCR) in June 2016. The GCR supplements *The Principles for Financial Market Infrastructures (PFMI)*, which was released in April 2012 by the *Committee on Payment and Settlement Systems* and *IOSCO*, by providing more information about the steps that FMIs should take to increase their level of cyber resilience.

Given the breadth and complexity of the cyber threat landscape and the dynamic nature of the technology, it is vital to adapt by enhancing and developing cyber resilience procedures while taking into consideration all pertinent advancements. The *Cyber Resilience Guidelines* (CRG) has been published by NRB pursuant to its monetary policy of fiscal year 2022/23, policy number 128, which states "*Cyber and Information Security Guideline will be issued for the institutions licensed to carry out payment-related transactions*". This document is created by NRB as a tool to support the GCR and express its expectations for cyber resilience to overseers and institutions licensed by the Payment Systems Department i.e., A, B, C, D class BFIs along with Payment System Operators (PSO) and Payment Systems Providers (PSP). ***Nepal Rastra Bank may also designate FMIs to implement the CRG as per its need.***

This document may be subject to review/amendment in regular interval or as and when necessary to incorporate required changes to ensure its alignment with the future development.

I. Purpose

The GCR issued by Bank for International Settlements (BIS) is intended to provide supplemental guidance to the PFMI regarding cyber resilience, primarily in the context of those principles listed below:

Key PFMI principles informing the guidance

Principle 2: Governance – *An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.*

Principle 3: Framework for the comprehensive management of risks – *An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other risks.*

Principle 8: Settlement finality – *An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.*

Principle 17: Operational risk – *An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.*

Principle 20: FMI links – *An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.*

The GCR is informed, in particular, by two important elements included in the PFMI relating to the systemic importance of FMIs: (i) the importance of assuring settlement when obligations are due and the finality of those transactions; and (ii) the ability of an FMI to resume operations within two hours following a disruption.

Principle 8 on settlement finality states: "An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time." The finality of settlement is important for the stability of the financial system. Credit, liquidity, market and legal risks are allocated among the parties to payments and securities transactions based on the principle of finality. The liquidity condition of financial institutions and their customers depends on the certainty of the assumption that transactions that are considered final will remain as such.

Since financial stability may indeed depend on FMIs to process transactions and settle obligations when they are due, the PFMI impose stringent expectations on FMIs in the area of operational risk. Of significant importance is an FMI's ability to resume critical operations rapidly. Specifically, Key Consideration 6 of Principle 17 on operational risk establishes an expectation that an FMI's business continuity plan "should be designed to ensure that" it can "resume operations within two hours following disruptive events and enable the FMI to complete settlement by the end of the day of the disruption, even in the case of extreme circumstances".

The CRG supplements the GCR. This document gives licensed institution (LI) and overseer more information that is transparent and clear on how to use the GCR to continuously increase an LI's cyber resilience. The CRG will give NRB the ability to express expectations to all LIs in a clear and uniform manner. This will ensure that financial stability is maintained and contribute to the proper management of cyber threats throughout the Nepalese financial system.

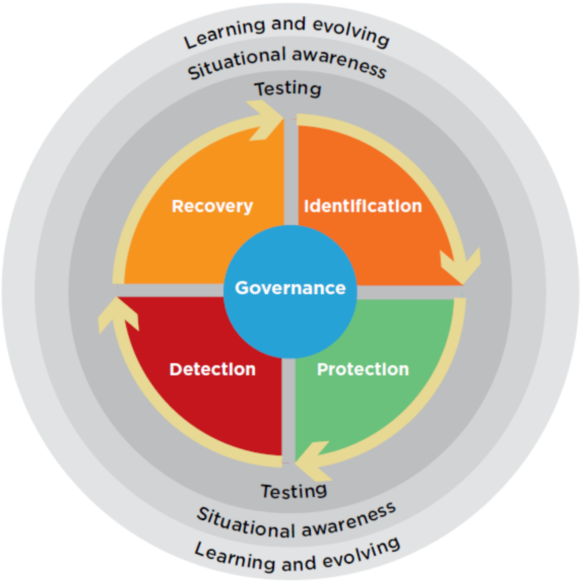
Due to the dependency and interconnectedness between LI and other LIs, FMIs, service providers and participants, LI should ensure that those entities also adhere to the cyber resilience requirements by counterparts as prescribed in this document through contractual obligation or any other means deemed necessary.

II. Approach

To implement the stated policy "*Cyber and Information Security Guideline will be issued for the institutions licensed to carry out payment-related transactions*" in policy number 128 of Monetary Policy of fiscal year 2022/23, NRB formulated a taskforce, which conducted a review of leading international standards (e.g., ISO/IEC 27001/27002, COBIT 2019) to identify areas that are relevant for LIs and consistent with the expectations of the GCR. NRB also utilized additional guidelines published by international regulatory bodies, particularly the *"Cyber Resilience Oversight Expectations for Financial Market Infrastructures", December 2018* of the European Central Bank (ECB), *"Cyber Resilience for Financial Market Infrastructure", November 2019* prepared by the Financial inclusion Global Initiative (FIGI) launched by World Bank Group, International Telecommunication Union (ITU) and the Committee on Payment Market Infrastructure (CPI) and the *"Expectations of Cyber Resilience of Financial Market Infrastructure (FMI)", October 2021* of the Bank of Canada. In order to ensure a current and effective cyber resilience program, the assessment also analyzed and evaluated recent developments that should be considered. NRB also consulted with the relevant stakeholders including Nepal Bankers' Association, PSOs and PSPs to seek their feedback on the content of the document before finalizing it.

III. Design and Organization of Cyber Resilience Guidelines

Similar to the BIS's Guidance on Cyber Resilience's chapters, the CRG is presented in sections. These sections outline five primary risk management categories as well as three overarching components that should be addressed throughout an LI's framework for cyber resilience.



Source: CPMI-IOSCO Guidance, 2016

The **risk management categories** are as follows:

a. Governance

b. Identification

c. Protection

d. Detection, and

e. Response and Recovery.

The **overarching components** are as follows:

a. Testing

b. Situational awareness

c. Learning and Evolving

A numbered list of discrete expectations is included in each subsection, outlining specific actions that LI's can take to put the CRG into practice.

IV. Applicability of Cyber Resilience Guidelines

Nepal Rastra Bank anticipates that all LIs will adhere strictly to the GCR and comply with the standards outlined in the CRG when putting it into practice. The LI must ensure that cyber risk is successfully managed in accordance with the LI's objectives and plan for cyber resilience, as well as in conjunction with the associated entity. Therefore, the LI and any associated entity that the LI relies on to operate its cyber resilience architecture shall comply with the standards set forth in this document. The CRG should be used by the LI as a tool to adhere to the GCR's rules and achieve the level of cyber resilience required to ensure financial stability.

To adopt risk-reducing measures appropriate to the various degrees of cyber risk it encounters, an LI is expected to use a risk-based strategy and prioritize its risk mitigation efforts while applying GCR. The CRG is not meant to serve as a check list for technical requirements or control requirements. Based on the LI's own risk-based methodology and its criticality within the Nepalese financial system, NRB will assess whether the LI is complying with the requirements outlined in the CRG.

LIs should continuously work to increase their degree of cyber maturity, especially by enhancing their capacity to carry out critical activities and recover from successful cyberattacks. This evolution and improvement should be the result of conversations between the LI and NRB over an extended period of time and in proportion to the criticality of the particular LI.

The GCR is based on principles because it understands that changing mitigation techniques are needed due to the dynamic nature of cyber threats. Although the CRG outlines detailed expectations for LIs to implement the GCR, NRB will permit flexibility in the approaches taken to achieve the requirements. The LI's cyber risk assessments should serve as the basis for the choice and use of cyber resilience measures. Additionally, because of the speed at which information technology is evolving and changes in the threat environment, cyber resilience measures may alter over time.

The size, organizational and operating structure, business model, and infrastructure design of LIs will all vary due to their heterogeneity. Therefore, it is possible that LIs could use various procedures, technologies, and approaches to meet the underlying expectations.

V. Managing Cyber Risks from Interconnections

The links between LIs and other organizations, including participants, linked FMIs, service providers, vendors, and vendor products, have grown during the past few years. LIs frequently put into practice solutions from outsourced service providers, like suppliers of financial technology, as they modernize and update their fundamental business processes. These linkages provide LIs numerous advantages, including improved creativity and access to cutting-edge technologies, operational efficiency, customized goods and services, and cost savings, but they could also pose more difficulties for managing cyber risk.

LIs must effectively identify, assess, and put into place preventive measures to mitigate the cyber risks that their interconnected stakeholders pose to them. Each component of the CRG includes information on how an LI can manage this risk (governance, identification, protection, detection, response and recovery, testing, situational awareness, learning and evolving). NRB expects LIs to take a risk-based approach when implementing its guidance on managing risks stemming from interconnections.

B. Governance

This section offers recommendations on the fundamental components that should be part of an LI's cyber resilience plan and framework, as well as how the governance arrangements within an LI should support those parts.

I. Preamble

Cyber governance refers to the arrangements an LI 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 prioritizes the security and efficiency of the LI's operations, and supports financial stability objectives. The framework should be guided by an LI's cyber resilience strategy, define how the LI'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 LI 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 LI's board (or equivalent) and its management, and it is incumbent upon its board and management to create a culture which recognizes that staff at all levels have important responsibilities in ensuring the LI's cyber resilience.

Strong cyber governance is essential to an LI'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 chapter provides guidance on what basic elements an LI's cyber resilience framework should include and how an LI's governance arrangements should support that framework.

II. Cyber Resilience Strategy

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

1. The LI should establish an internal, cross-disciplinary steering committee comprised of senior management and appropriate staff (employees and/or contractors) from multiple business units (e.g., business, finance, risk management, internal audit, operations, cybersecurity, information technology (IT), communications, legal and human resources, some of which may be external), to collectively develop a cyber resilience strategy and framework. The steering committee should provide multiple views and perspectives to ensure that the cyber resilience strategy and framework is holistic and focuses on all elements related to people, processes and technology.

2. The LI should ensure that the following aspects are addressed in the strategy:

   a. The LI's cyber resilience vision and mission;

b. The strategic cyber resilience goals, objectives and intended outcomes that the LI will work toward;

c. The importance of cyber resilience to the LI and its key internal and external stakeholders;

d. The LI's cyber risk tolerance (to ensure that it remains consistent with the LI's overall risk tolerance, business objectives and corporate strategy);

e. The cyber risks that the LI bears from and poses to its participants, other LIs 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 of cyber resilience initiatives, including the budgeting process and organizational capabilities; and

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

3. The board of the LI should approve the cyber resilience plan and make sure that it is reevaluated and updated on a regular basis in accordance with the LI's threat landscape.

III. Cyber Resilience Framework

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

Cyber resilience framework

4. The LI should have a cyber resilience framework that clearly sets out how it determines its cyber resilience objectives and risk tolerance, as well as how it effectively identifies, mitigates, and manages its cyber risks to support its objectives.

5. The LI's cyber resilience framework should be approved by the LI board to ensure that it is consistent with the organization's developed cyber resilience strategy.

6. The LI's cyber resilience framework should be regularly reviewed and updated.

7. In particular when there are changes to the LI's cyber resilience strategy or objectives, the cyber resilience framework (containing all policies, technological standards, processes, and controls) should be reviewed and updated. The LI should create a process for review that could consider the factors like:

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

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

c. critical functions, key roles, procedures, information assets, third-party service providers, and linkages of the LI as determined by risk assessments;

d. direct cyber-attacks that have affected the LI or indirect cyber incidents that have affected a component of the ecosystem surrounding the LI;

e. remarks or lessons learnt from audits or other forms of test on the cyber resilience framework;

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

g. new business developments and future strategic objectives.

Cyber is more than just ICT

8. The LI's cyber resilience framework should include requirements for timely communication and coordination mechanism so that the LI can work with the relevant parties to successfully respond to and recover from cyberattacks.

Enterprise risk management

9. The LI's cyber resilience framework should be aligned with its enterprise operational risk management framework and enterprise architecture.

An LI's ecosystem

10. The LI's cyber resilience framework should consider the cyber risks the LI faces from and poses to its participants, other LIs, suppliers, vendor goods, and its service providers, which are together referred to as an LI's ecosystem.

International and national standards

11. The LI's cyber resilience framework should employ leading industry-level standards, guidelines, or recommendations (such as the ISO/IEC 27000 series) as benchmarks when developing a framework for cyber resilience and incorporating the best cyber resilience solutions.

Risk management governance

12. The LI's cyber resilience framework should clearly define roles and responsibilities, including accountability for decision making within institutions for identifying, mitigating and managing risks.

13. The LI's cyber resilience framework should systematically incorporate the requirements (i.e., policies, technological standards, and controls) related to governance, identification, protection, detection, reaction, and recovery, testing, situational awareness, and learning and evolution.

Audit and compliance

14. Through independent compliance programs and audits carried out by qualified staff, the LI shall periodically evaluate and measure the sufficiency and effectiveness of its cyber resilience framework (including all security controls) and adherence to it. The LI is encouraged to apply relevant metrics, maturity models, and the results of its testing programs in this process. The LI should routinely order an external audit.

15. The LI should monitor its development of its cyber resilience capabilities on a continuous basis as it progresses from a current state to a defined future state (i.e., a target maturity level).

16. The LI should have a strategy for reaching its target level that outlines roadmaps for how it will be resourced and delivered.

IV. Role of the Board and Senior Management

Board and senior management responsibilities

17. The board of the LI is ultimately responsible for making sure that cyber risk is properly managed. The board should establish the LI's cyber risk tolerance and cyber resilience strategy, specify roles and duties for dealing with cyber risk, and endorse the cyber resilience framework.

18. 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 LI's risk management framework.

19. The LI 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.

20. The board and senior management should ensure that the LI's cyber risks and management of those risks are regularly evaluated during board meetings.

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

    a. allocating resources and setting priorities for cyber resilience deliverables based on the findings of cyber resilience assessments, key performance indicators, key risk indicators, overall business goals, and progress toward target maturity;

    b. periodically assessing the LI's cyber maturity through self-assessments of cyber resilience;

    c. assessing the self-evaluation and lesson learnt from the test results, and taking the appropriate decisions to improve the effectiveness of cyber activities;

d. ensuring that employees who are responsible for implementing the LI's cyber resilience framework have the necessary training, skills, knowledge, experience, expertise, and resources and are sufficiently informed, as well empowered to make prompt decisions; and

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

22. Senior management should make sure that every employee is aware of their responsibility for reducing cyber risk and has access to the necessary training.

23. For high-risk employees (e.g., senior management, system administrators, software developers and critical system operators), the board and senior management should create succession plans as necessary. In accordance with established succession plans, they should also create recruitment criteria for critical cyber roles that comprise the necessary cyber skills, expertise, and experience.

24. Senior management should help plan and participate in industry-wide drills that test and improve the cyber resilience of the LI's ecosystem.

Culture

25. In order to foster a culture where workers at all levels are aware that they have important responsibilities for ensuring the LI's cyber resilience, the board and senior management should cultivate a strong level of awareness of and commitment to cyber resilience.

26. The senior management of the LI should make sure that everyone within the institution has a better understanding of cyber risk. Training curriculum should be revised frequently to reflect the evolving threat landscape of the ecosystem.

27. The LI should create policies outlining the repercussions for staff members and contractors who don’t abide by cyber security regulations. The regulations must be precise and appropriate for the risk and situational context involved.

28. The senior management of the LI should ensure that situational awareness materials are made available to relevant employees when prompted by highly visible cyber incidents, changes to the threat landscapes and the impacts of these threats to the LI. For instance, the LI could send internal emails about cyber events or post articles in their intranet site.

Skills

29. The board and senior management of the LI should be comprised of individuals who have the right mix of expertise, knowledge, and experience to comprehend and control the cyber risks that the LI faces in order to effectively carry out their duties in relation to the cyber resilience strategy and framework. The board should be well-informed to challenge the suggestions and decisions made by the designated senior management in a credible manner. In order to do so, the LI should:

a. appoint at least one board member with cyber security expertise; and

b. ensure that the board of directors and senior management are aware of their responsibilities regarding cyber resilience (including their role in managing cyber risk) and, if necessary, receive appropriate training.

Accountability

30. A senior executive, such as a Chief Information Security Officer, responsible for carrying out the organization's cyber resilience architecture should be appointed by the board and senior management.

31. The senior management of the LI should ensure that the employees and contractors with privileged accounts who have access to sensitive assets and information need to receive additional cyber resilience training according to the criticality to the business.

32. The LI should ensure that this senior executive has:

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

    b. access to directly report to the board;

    c. operational independence from other IT operations; and

    d. the necessary skills and knowledge to successfully plan and execute the LI's cyber resilience initiatives.

C. Identification

This section describes how an LI should categorize business processes, information assets, and external dependencies, as well as how to identify risks.

I. Preamble

Given that an LI operational failure can negatively impact financial stability, it is crucial that LIs identify which of their critical operations and supporting information assets should, in order of priority, be protected against compromise. The ability of an LI 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 LI to know its information assets and understand its processes, procedures, systems and other dependencies to strengthen its overall cyber resilience posture.

II. Identification and Classification

It is important that the LI 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.

Identification of business functions and processes

33. The LI should identify and document all its critical functions, key roles and processes that support those functions, and update this information on a regular basis.

34. The LI should identify and document all processes that are dependent on third-party service providers and identify its interconnections, and update this information on a regular basis.

35. The LI should perform a business impact analysis to quantify the impact of disruptions on its critical operations.

36. The LI should have an enterprise risk management framework to identify risks and conduct risk assessment on a regular basis.

37. The LI should classify its functions and business processes according to their criticality; this information should be used for prioritizing its protective, detective, response and recovery measures.

38. The LI should create and maintain a simplified network map of network resources with an associated plan addressing IPs which locate routing and security devices and servers supporting the LI's critical functions which identify links with the outside world.

39. The LI should compulsorily conduct the needed risk assessments before deploying new and updated technologies, products, services and connections to identify potential threats and vulnerabilities.

Identification of information assets and related access

40. An LI should be able to identify the information assets (includes assets under the direct ownership of the LI and assets that the LI relies on for its critical business operations but are not owned by the LI itself) supporting its business processes. It should:

    a. establish a standard for categorizing information and information systems in accordance with the LI's security policy (its level of concern for availability, confidentiality and integrity);

    b. identify and maintain an up-to-date and centrally managed inventory of its information assets and system configurations in order to know the assets that support its business functions and processes; and

    c. develop and maintain an up-to-date network diagram, that includes:

        i. network resources (including IP addresses and subnets);
        ii. connected components; and
        iii. internal and external service links (including interconnections with other stakeholders, internet-facing services, cloud services and any other third-party systems).

41. The LI should adopt and apply a cyber security risk assessment process and maintain a risk register to document and monitor risks. The criteria for conducting and/or updating assessments should be specified in the risk assessment process (e.g., system development and renewal, emerging threats, and recognized vulnerabilities inside the LI's systems or infrastructure). The risk register should identify and categorize the risks according to their criticality.

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

43. LI should consult and update its risk register based on the outcome or progress of risk assessment results. These results should drive the selection and implementation of security controls, prioritizing them according to the risks faced by the LI.

44. The LI should maintain a central repository of individual and system accounts and permissions. The repository should:

    a. identify access rights to information assets;

    b. contain applicable information that will help the LI to identify any anomalous activities; and

    c. be protected from unauthorized access and modification.

Regular review and update

45. An LI should integrate identification efforts with other relevant processes, such as acquisition and change management. So that it could facilitate a regular review of LI's

list of critical business processes and functions, individual and system credentials, and inventory of information assets so that they remain current, accurate and complete.

III. Interconnections

The identification of an LI's critical business processes and the information assets supporting them should extend to the entities in its ecosystem. An LI's systems and processes are directly or indirectly interconnected with the systems and processes of the entities within its ecosystem, e.g., participants, linked FMIs, settlement banks, liquidity providers, service providers, critical infrastructure such as energy and telecommunications, vendors and vendor products. The cyber resilience of those entities could therefore have significant implications in terms of the cyber risk that the LI faces, particularly since the significance of the risks they may pose is not necessarily proportionate to the criticality of their business relationship with the LI.

46. The LI should identify the cyber risks that it bears from or poses to entities in its ecosystem and coordinate with relevant entities, as appropriate. In order to increase the ecosystem's overall resilience, this may involve identifying vulnerabilities and threats that they share and taking appropriate action to mitigate those risks collectively.

47. The LI should take into account a wide range of potential threat vectors and risks that could lead to a potential breach of the LI's essential business functions to identify and assess the risks to the LI from participants' interconnections. 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 LI. The LI should also assess potential risks to the LI's ecosystem that could arise from participant interconnections.

48. The LI must know the services and business operations of the third-party service provider, including details of the services provided by it and the manner in which those services will be delivered, in order to identify and evaluate the risks posed by interconnections with it. The LI may need to rely on various sources to gather this information. For e.g., publicly available data, self-assessments, and third-party assessments to understand, identify, and assess the risks.

D. Protection

In accordance with best practices for cyber resilience and security, this section offers advice on how the LI should adopt appropriate and efficient protections to prevent, reduce, or mitigate the effects of a potential cyber risk.

I. Preamble

Cyber resilience depends on effective security controls and system and process design that protect the confidentiality, integrity and availability of an LI's assets and services. These measures should be proportionate to an LI's threat landscape and systemic role in the financial system, and consistent with its risk tolerance. This chapter provides guidance on how LIs should implement appropriate and effective measures in line with leading cyber resilience and information security practices to prevent, limit or contain the impact of a potential cyber event.

II. Protection of Processes and Assets

LIs must implement a resilience by design strategy, put up robust information and communication technology (ICT) controls, and use layered defenses to protect their processes and assets.

Controls

49. The LI should implement appropriate protective controls that are in line with leading-practice cyber resilience standards such as ISO standards to minimize the likelihood and impact of a successful cyber-attack on identified critical business functions, information assets and data. The current LI standards are not intended to be replaced by the CRG.

50. The LI should implement these controls in accordance with the risk analysis completed during the identification phase based on the identification of its critical operations, key roles, procedures, information assets, third-party service providers, and interconnections.

51. Protective controls should be proportionate to the LI's threat landscape and systemic role in the financial system, and consistent with its risk tolerance.

52. The LI should implement multiple independent security controls necessary for protecting its systems, processes and data, at the earliest possible stage.

Resilience by design

An LI should take into account cyber resilience from the very beginning of the design and development of the system all the way through its life cycle. This will reduce software and hardware vulnerabilities and guarantee that the proper security measures are built into systems and processes from the beginning. If the system or any of its components are acquired from, or operated by, a third-party supplier, the LI should obtain assurance that the vendor has applied the appropriate security controls.

53. The LI should:

a. when designing, building, acquiring, or modifying its systems, processes, and products, implement a system development methodology that incorporates the resilience by design approach. at each step of development, the LI should manage its cyber risk and incorporate resilience based on the findings 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 (physically and/or logically) the development, testing and production environments for reducing operational risks. Each environment should be properly secured in accordance with the security standards of the LI;

e. assess the effectiveness of the its security controls regularly to adapt them to its evolving threat landscape. It should be monitored and audited regularly to ensure that they remain effective and have applied to all assets where they might be needed;

f. apply a defense-in-depth strategy in line with a risk-based approach, i.e. it should implement multiple independent security controls so that if one control fails or a vulnerability is exploited, alternative controls will be able to protect targeted assets and/or processes;

g. make sure the testing environment closely resembles the production environment as much as possible and practical, especially in terms of the software, network configurations, and hardware supporting essential systems;

h. thoroughly examine and test the business-critical software, systems, and networks against the LI's security requirements to make sure there is no adverse impact on organizational operations or security. Boundary testing, robustness and fault tolerance testing, performance and load testing, data flow testing, and use-case testing are some examples of rigorous testing that can be used to evaluate whether essential systems and software operate as intended. For new information systems, upgrades, and new versions, make sure security testing is integrated into the system's acceptance testing methods;

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

j. ensure that the change control processes and procedures are used to regulate changes to systems during the development life cycle.

Strong ICT Controls

These subsections offer a non-exhaustive list of significant controls that an LI should take into account. A number of LI-specific factors will be reflected in the controls that an LI decides to use.

Protecting information—data and information protection controls

54. To ensure the confidentiality, integrity and availability (CIA) of the LI's data and information at rest and in use, the LI should implement strong data and information protection controls. That includes, but are not limited, to:

    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 LI should update malicious code protection mechanisms as per its change and configuration management policies and procedures. LI personnel should be trained on the effective use of anti-malware software;

    b. protection against phishing attacks: The protection mechanism should include detection and mitigation of phishing attacks. LI personnel should be aware of phishing threats;

    c. integrity verification tools to detect unauthorized changes to critical files from internal and external sources (e.g., participating entities);

    d. data encryption commensurate with the LI's criticality, sensitivity and risk assessment processes;

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

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

    g. regular vulnerability assessment of its production environment. Controls and additional defense layers should be implemented and tested to protect unsupported or vulnerable systems;

    h. validation of all information inputs in applications, in particular, for web-facing applications. The validation should at least include valid syntax, data types, length, ranges and acceptable values;

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

    j. secure disposal of media when no longer required, using defined formal procedures of the institution;

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

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

m. policy to avoid unauthorized access to the confidential and sensitive information in paper as well as screens while working in the desk;

n. removable storage media should be stored in accordance with policy.

Protecting information - Communications and network security controls

55. The LI should implement strong communications and network security controls. That includes, but are not limited, to:

a. implementation of secure network protocols and encryption 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 LI may use intrusion detection or prevention systems, end-point security solutions or any other relevant solutions, in particular, on devices and in environments used for accessing the LI network remotely;

c. controls that manage or prevent unauthorized/unregistered devices from connecting to the LI'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 LI'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 LI's critical services. The LI 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. scan its legacy technologies regularly to identify potential vulnerabilities and seek upgrade opportunities. Control and additional defense layers should be implemented and tested in order to protect unsupported and vulnerable systems;

f. assurance that protection extends to the LI's entire attack surface and that sup- porting or extended infrastructure (e.g., non-core system, backup) that may be used as an attack vector into the critical infrastructure is also formally authorized, monitored and controlled;

Configuration and change management

56. The LI should have a configuration and change management policy, process and procedures in place. The configuration and change management process should be based on well-established and industry-recognized standards and best practices (e.g., an

information technology infrastructure library-ITIL). Among measures to put in place, the LI could/should:

a. approve and prioritize the changes from its Board of Directors (BoD) or Change Advisory Board (comprised of key stakeholders such as business and IT Management) 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, 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 unauthorized changes and installation of patches on the information system;

e. establish baseline system and security configurations (defined in the security policy) for information systems and system components (including devices used for accessing the LI network remotely) that:

    i. are documented, formally reviewed and regularly updated to adapt to the LI'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 and accurate;
    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 as per the software installation policy. For critical systems, the LI should employ software whitelisting capabilities configured with a deny-all, permit-by-exception policy;

g. implement the change management procedure (that includes scheduling change implementation, communicating to those impacted prior to implementation and consulting them, if necessary);

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

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

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

k. 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 fallback plan, when applicable.

Security settings consistent with levels of protection

57. The LI should configure ICT systems and devices with security settings that are consistent with the level of protection defined in its security policy. 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 mobile devices within the ICT environment. The LI's baseline system security configuration standards should prescribe the technical IT security controls, parameters, features and specifications required to achieve the LI's cyber security goals for the protection of information assets and technology-based solutions;

    b. application of industry-level 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.

Layered protection that facilitates response and recovery

58. The LI's protective controls should enable monitoring and detection of anomalous activity. The LI 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 regular network traffic patterns, account usage and access patterns) and the system’s business activities (such as participants’ regular 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 systems or application’s business logic to detect unusual transactions (for e.g., transactions that are unusually large or small, frequent or infrequent, out of sequence, etc.) or behavior (for e.g., activities conducted by unusual persons, at unusual times, from unusual locations), or implementing advanced data analytics of trends and notifying the LI when events occur outside of the normal trend;

c. implement SIEM (Security Information and Event Management) solution or equivalent tools (that utilize traffic flows, alerts, and correlated log analysis) to proactively take the necessary actions to increase its cyber resilience capabilities;

59. Where it is feasible and practical, the LI should develop the necessary capabilities to block suspected activity at the application and/or network in order to contain anomalous activity;

60. To segregate systems and data of varying criticality, the LI should:

a. establish a secure boundary that protects its network infrastructure by using tools such as a router, firewall, Intrusion Prevention System (IPS) or Intrusion detection system (IDS), Virtual Private Network (VPN), Demilitarized Zone (DMZ) or proxies, etc. The secure boundary should identify trusted and untrusted zones (DMZ) 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. For e.g., a virtual local area network (VLAN) segment and internet protocol (IP) subnet;

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 LI 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, where possible.

III. Interconnections

Third-party security management ensures protection of the LI's assets that are accessible by participants, service providers, linked FMIs, vendors or other entities in its ecosystem, while maintaining an agreed level of information security and service delivery in line with service agreements to ensure disruptions to the LI are minimized.

Risks from interconnections

61. The LI should implement protective measures to mitigate risks arising from the entities in its ecosystem. The results of the risk assessment from the identification phase,

incorporating the risk posed by the connected entity and the nature of the LI's relationship with the entity, will determine the appropriate controls for each entity.

Participation requirements

62. If necessary, an LI should specify participation requirements to ensure that it can meet its cyber resilience objectives. The LI should impose rules in the following areas, but are not limited, to:

    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.

63. The LI should obtain assurance from its participants that they meet the LI's cyber resilience requirements. The assurance can be in the form of participant self-attestations or external third-party certifications of the participant’s resilience.

Third-party cyber resilience

64. The LI should request confirmation that its third-party vendors and service providers, including ICT suppliers, meet its requirements for cyber resilience. The LI should make sure that clauses supporting the LI's goals for cyber resilience are agreed upon and recorded when negotiating or renewing its contracts with third parties.

    Contracts should cover matters such as:

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

    b. information security requirements for mitigating the risks associated with third party access to the LI’s information assets. Information assets include assets under the direct ownership of the LI and assets that the LI relies on for its critical business operations but are not owned by the LI itself;

    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.

65. The LI should update its risk profile component related to third-party, as appropriate, upon notification of changes to third party service levels or security functionality.

IV. 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 LI's employees, customers, assets, reputation and interests at risk.

Security analytics

66. The LI should implement measures to monitor anomalous behavior by users of its systems. It should use data loss identification and prevention techniques in order to prevent removal of sensitive and confidential data from its network.

Changes in employment status

67. In order to reduce insider threats, an LI should screen and background-check new employments. Similar checks should be performed on every employee periodically throughout their employment, commensurate with access to critical systems by the staff. The LI should set up processes and controls to mitigate risks associated with employees quitting their jobs or changing their responsibilities.

68. The LI should incorporate cyber security at every stage of the employment life cycle, outlining the security-related steps that must be taken during each employee's onboarding, ongoing management, and termination. This includes:

    a. conducting pre-employment background security checks on all successful candidates (employees and/or contractors) based on their potential roles as well as the importance of the resources and information they might need to perform their duties. Contractual agreements with employees and contractors should specify their responsibilities for information security of the institution;

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

    c. making sure that all access rights related to an employee's previous position that are not required for their new responsibilities are promptly revoked when an employee's responsibilities change. Employees who are assigned critical/sensitive roles (such as those requiring privileged access to critical systems or who become high-risk staff);

    d. putting in place processes to promptly revoke all access privileges to the information assets from departing/unrelated employees. Staff should be required to return all LI-owned property, including critical records, upon termination of employment.

69. All employees, contractors, and outside parties should be required to wear identity card issued by the institution. Security personnel should be alerted right away if they encounter anyone not wearing the identity card issued by the institution.

70. Access to secure areas or confidential information processing facilities, including for outside support staff, should only be granted only when necessary. Such access should be authorized and monitored.

Access control

Logical access

71. The LI should ensure the following:

    a. prior to account creation and authorization, each user's identity has been confirmed. The LI should make sure that identity verification is carried out by the participating entity and is stipulated as a requirement in the participant agreement if users are members of an external participating entity;

    b. all internal (e.g., employees and contractor) as well as external users (e.g., LI participants) have been uniquely identified and authenticated so that actions and activities can be attributed to individual users;

    c. the authentication mechanism (such as passwords, tokens, biometrics, public key infrastructure certificates or key cards) should be set as per the criticality of the information system, processes, and/or user roles to ensure sufficient level of protection in their intended use;

    d. the critical systems, processes, and roles should all require multi-factor authentication, wherever supported. The LI should set and enforce password complexity requirements (e.g., minimum length, types of characters, etc.) for password-based authentication;

    e. a formal access control model (for e.g., role-based access control, rule-based access control or attribute-based access control) that enforces an access control policy is used to establish and manage user access to resources. The access control 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). The selected model should make sure that only authorized people are granted access to resources. When a person is no longer authorized, the access control policy should include procedures to revoke access to resources;

    f. the principle of separation of duties has been applied to application processes and/or transactions that may be at risk of fraud or misuse for e.g., high-value and/or high-volume transactions. This principle requires that no single person should be permitted to perform all parts of these processes and/or transactions for e.g., application of four-eyes principle, six-eyes principle, etc.;

    g. procedures have been established to control the creation, modification, and deletion of user accounts and access rights. Such actions must be submitted to and authorized by the proper staff. This should be recorded for periodic review;

h. the maximum number of unsuccessful login attempts is set and enforced. And proper instructions should be provided to let the user know what to do after the allotted number of tries has been reached;

i. an up-to-date record of all individual and system accounts (in particular, privileged and remote access accounts) and their associated access rights is maintained;

j. automated mechanisms are implemented to support the management of information system access accounts, wherever applicable. 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;

k. the concerned staff are automatically notified when user access has been elevated to privileged access;

l. specific procedures have been implemented to allocate privileged access on a need-to-use or an event-by-event basis;

m. automated mechanisms are employed that allow continuous monitoring and auditing of enabling, disabling and removal actions (related to user account creation and modification in critical systems) in order to notify concerned staff to detect potential malicious behavior or suspicious activity. The LI's authentication mechanisms follow industry best practices and are aligned with relevant standards (for e.g., ISO 27001/27002).

Physical access

72. The LI should ensure the following:

a. information processing facilities and areas containing sensitive and/or critical information are protected by defined security perimeters;

b. access to secure areas is restricted to authorized personnel only by means of the proper entry controls;

c. reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, critical computing equipment is situated and safeguarded. Critical computing equipment should be physically protected with features like water damage protection, fire suppression systems, temperature and humidity controls, and emergency power and lighting,

d. wireless access points, power cables, and telecommunications cabling related to critical systems should be protected from tampering and damage;

e. equipment is properly maintained to ensure its continuous availability and integrity.

V. Training

73. Information security should be complied by all employees (including senior management and board members) and contractors in accordance with the LI's established cyber resilience policies, technical standards, and procedures.

LI staff

74. The LI should:

a. make sure that all employees, whether they are full-time or temporary, receive training to help them develop and maintain the necessary awareness and skills for identifying 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 staff members are well-versed in the cyber risks they may encounter while performing their duties, as well as their roles and responsibilities in protecting the LI's assets, especially critical systems;

d. include a course on cyber security awareness in the program for onboarding new employees;

e. train the relevant staff before go live of new systems or applications;

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

g. assess the training's effectiveness to see if the awareness and training have a positive impact on behavior and adjust the training as necessary.

High-risk groups

75. The LI should identify staff members and subcontractors in high-risk groups, such as those with privileged system access or in delicate business roles, and give them specialized information security training.

E. Detection

This section lists the protections and tools that an LI needs to be able to identify unusual activity, cyber events, and incidents.

I. Preamble

An LI's ability to recognize 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 LI 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 LI should maintain effective capabilities to extensively monitor for anomalous activities. This chapter outlines monitoring- and process-related guidance aimed at helping LIs detect cyber incidents.

II. Detecting a Cyber Attack

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).

76. The LI should implement continuous monitoring against the baseline profile of system activities discussed in the title ***Layered protection that facilitates response and recovery*** (Page No. 20) of sub-section: ***II. Protection of processes and assets*** under the section: ***D. Protection***.

77. The LI should:

    a. develop and implement automated detection systems (for e.g., a security information and event management system) that correlate all network and system alerts with any other unusual activity across all of 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.

    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 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 routinely reviewed, tested, and updated appropriately in a controlled and authorized manner.

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.

78. The LI should:

a. collect, monitor and analyze patterns and behavior (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 recognize known threats, improve the chance of identifying threats trying to exploit recently discovered (zero-day) vulnerabilities, and threats using recently discovered attack chains, methods, and techniques;

d. ensure that it understands and has anticipated the use cases of 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 in place to monitor activities that are not in accordance with its security policy and may result in the loss of confidentiality, integrity, data theft, or destruction.

Layered detection

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

79. The LI should use detection capabilities by implementing multi-layered detection controls that cover people, processes, and technology with each layer serving as a safety net for preceding layer. As a cyber-attack typically progresses in a sequence of stages before attaining its end objective, LIs should also apply approaches that enable them to delay or disrupt the attackers’ ability to advance within the attack sequence. An effective intrusion detection capability could help an LI identify flaws in its protective measures and correct them as soon as possible.

80. The LI should constantly investigate new technologies and techniques to prevent lateral movement. These technologies and techniques should trigger alerts and notify the LI of any potential malicious activity.

81. The LI should ensure its detection capabilities are periodically reviewed, tested and updated appropriately.

Incident response

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

82. The monitoring and detection capabilities of the LI should send a notification to the concerned staff.

83. To facilitate forensic investigation, the LI should ensure that:

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

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

    c. the logs' content includes the necessary information to support investigation (e.g., event type, time, user/address, and so on);

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

84. The LI should ensure that its logs are backed up in a secure location and that controls are in place to mitigate the risk of alteration.

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

Security analytics

86. The LI 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 center (SOC), network operations center or equivalent.

F. Response and Recovery

This section provides guidance on an LI's capabilities to respond to and recover from Cyber-attacks.

I. Preamble

Financial stability may depend on an LI's ability to settle obligations when they are due. Therefore, an LI'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 in meeting related objectives. This chapter provides guidance on an LI's capabilities to respond to and recover from cyber-attacks.

II. Incident Response, Resumption and Recovery

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

Incident response planning

87. The LI should have a comprehensive cyber incident response capability that includes detection and analysis as well as containment, elimination, and recovery; and post-incident activity. This capability could include direct cooperative or contractual agreements with incident response organizations or providers to help with mitigation efforts as quickly as possible.

88. The LI should also have the resources, policies, and procedures in place to conduct a thorough investigation of a cyber-attack including root cause analysis. The LI may use internal resources and/or third-party service providers with whom it has contractual agreements to ensure that the investigation begins as soon as a cyber-attack is detected.

89. When a successful or attempted cyber-attack is detected and confirmed, the LI should deploy its investigative capability to determine the nature and extent of the attack, as well as the damage inflicted.

90. While the investigation is ongoing, the LI should take immediate action to contain the cyber-attack or attempted cyber-attack to prevent further damage and begin efforts to resume operations based on its response planning.

91. Based on the potential impact and criticality of the risk, the LI should establish criteria and procedures for escalating cyber incidents to the board and senior management.

92. The LI should also have procedures to escalate investigations to law enforcement agencies as needed.

93. The LI should ensure that its incident response team has the requisite skills and training to address cyber incidents.

94. The LI should train its employees so that they understand their roles and responsibilities in handling digital evidence and ensuring that it is not compromised and remains valid in accordance with the requirements of the local jurisdiction.

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

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

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

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

96. Planning to enable resumption within two hours of a cyber incident requires a detailed and comprehensive understanding of the LI's functions and processes. No single solution will work for all LIs. An LI should involve both the technical and business teams to carefully plan for risks specific to the LI's design, critical functions and processes. Despite having the capability to resume critical operations within two hours, the LI should exercise judgment (in agreement with regulatory/supervisory authorities and relevant stakeholders) when resuming operations so that risks to itself or its ecosystem do not thereby escalate, while considering that completion of settlement by the end of day is crucial.

Contingency planning

97. While the LI should aim to resume critical operations safely within two hours of a disruption, it should also prepare for scenarios in which this objective is not achieved. The LI should analyze critical functions, transactions, and interdependencies to prioritize resumption and recovery actions that, depending on the LI's design, may assist it in processing critical transactions while remediation efforts are ongoing. The LI 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.

98. The LI should devise a backup plan based on scenarios in which resumption within two hours is not possible. This strategy should include:

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

    b. define roles and responsibilities; and

    c. set out options for rerouting or substituting critical functions and/or services that may be affected for an extended period of time by a successful cyber-attack.

99. Based on their relative priorities and reliable information related to resumption possibility, the LI must plan for how to operate in a reduced capacity or how to safely restore services over time.

Planning and preparation

100. To manage cyber security incidents, the LI should develop comprehensive cyber incident response, resumption, and recovery plans (these can be part of the Business Continuity Plan or as a separate document). These plans should aim to limit damage and prioritize resumption and recovery actions that facilitate critical transaction processing while reducing recovery time and costs. Following should be considered while developing these plans.

    a. the response plan should specify actions to be taken as soon as a cyber incident is detected;

    b. the resumption plan should include actions to restore and resume the LI's critical business operations, possibly in a reduced capacity, as soon as it is safe and practicable to do so (and with two hours as the target objective);

    c. the recovery plan should outline the steps that must be taken in order for the LI to safely return to a fully functional normal operating state, which may take some time.

101. 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.

102. In developing its plans, the LI should:

    a. include a range of extreme but plausible scenarios to assess the potential impact of such scenarios on the LI and the broader ecosystem; and

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

103. The LI 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 previous cyber incidents, including root cause analysis findings

104. The LI should test its response, resumption, and recovery plans against a variety of scenarios on a regular basis.

105. The LI should consult with relevant external stakeholders (e.g., participants, service providers and other LIs) within the ecosystem to improve its response, resumption, and recovery plans.

106. The LI should put in place processes to improve its response, resumption, and recovery plans on a continuous basis, considering cyber threat intelligence sources (e.g., feeds) and information shared within its ecosystem.

107. The LI's cyber incident response, resumption and recovery processes should be closely integrated with crisis management, business continuity, and disaster recovery planning and operations.

III. Design Elements

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

Design and business integration

108. System and process design and controls for critical function and operation should support incident response activities as much as possible.

109. The LI should design systems and processes to minimize the impact of any cyber incident, to resume critical operations within two hours of a disruption, to complete settlement by the end of the day, and to maintain transaction integrity.

110. When designing its systems and processes, the LI should consider a variety of scenarios and potential response actions, as well as their implications.

111. The objective of resuming operations within two hours necessitates careful selection and implementation techniques and methods of settlement, as well as technologies and tools for recovering system configuration and data. The solutions chosen will be determined by several factors, including the system's design and complexity, the frequency and volume of transactions, and the system's life-cycle stage (The life-cycle stage of a LI'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 challenges, the LI should nonetheless seek solutions that incrementally reduce the resumption time as much as possible). There is no single solution that fits all Lis and critical systems.

Data integrity

112. The LI should define and identify data that is critical for the resumption of services which should 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 LI should be able to recover these data in a reasonable amount of time.

113. The LI should have plans in place to quickly determine the status of all transactions and member positions in the event of a disruption, backed up by recovery point objectives. As a result, the LI should design and test its systems and processes to ensure recovery of accurate data following a breach. Stringent protection and detection controls should be used to protect information and data.

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

115. Recovery point objectives and data recovery options should be established in close collaboration with the business and IT functions. This close collaboration can assist an organization in answering fundamental questions about how to conduct critical business processes in the face of corruption.

116. The backup solutions provided by the LI should be configured to align with the frequency and volume of transactions. Because an LI processes thousands of transactions per hour, a solution that only backs up once per day will not provide adequate protection unless additional database transaction recovery solutions are implemented.

117. The backup and recovery methods and strategies should be integrated into LI's system infrastructure at the development and/or acquisition phase.

118. The LI should back up its information system by maintaining a redundant secondary system that is not located in the same place as the primary system and that can be activated without information being lost or operations disrupted.

119. Data recovery measures should be included in the LI's cyber resilience framework. The LI should consider a variety of options for data recovery. The LI should choose these options based on a detailed analysis of what data are critical to the LI's operations, including what data the LI would need to resume operations within two hours and how various cyber scenarios, including data loss and manipulation of data, could impact the integrity of these data.

120. Backups should be protected both at rest and in transit to ensure data confidentiality, integrity, and availability. Backups should be tested on a regular basis to ensure their availability and integrity.

121. The range of data recovery options that the LI should consider include, but are not limited, to:

    a. implementing database record recovery mechanisms, such as record rollback and logging or rolling forward to correct corrupted data;

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

    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. For e.g., 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.

IV. Interconnections

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

Data-sharing agreements

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

123. The LI should review information-sharing rules, agreements, and protocols on a regular basis in order to control the publication and distribution of such information and to prevent the disclosure of sensitive information that could have adverse consequences if disseminated improperly.

Contagion

124. In the event of a large-scale cyber incident, an LI may pose or be exposed to contagion risk (i.e., the spread of malware or corrupted data) to or from its ecosystem. The LI should develop policies and procedures outlining how it will collaborate with relevant interconnected entities to resume operations (with the first priority being its critical functions and services) as soon as it is safe and practicable to do so without putting the broader sector or the financial system at risk.

Crisis communication

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

126. The incident response plan for the LI should identify internal and external stakeholders who must be notified, decision-making responsibilities and authorities, and information that must be shared and reported, as well as when this should take place.

127. Any cyber incident that could be material or systemic should be immediately reported to relevant oversight and regulatory authorities by the LI. The LI should follow the requirements of NRB's related directive/guideline when reporting cyber incidents to the NRB.

128. When there are indications of criminal intent (e.g., fraud, extortion), the LI should have procedures in place to escalate investigations to law enforcement agencies.

Responsible disclosure policy

129. The LI should have a policy and procedures in place to allow for the responsible disclosure of potential vulnerabilities and risks within its ecosystem as it responds in real time to a cyber-attack or incident.

130. The LI should prioritize disclosures that will assist participants and other stakeholders in responding quickly and mitigating their own risk, which will benefit the ecosystem and overall financial stability.

Forensic readiness

131. The LI should develop the capability to support or assist in forensic investigations. This capability should include the ability to design protective and detective controls to aid in the investigation process. The LI should establish relevant system logging policies, such as required audit log content, log and event time synchronization, and log file retention periods.

132. The LI should establish procedures for securely handling, collecting, and preserving digital evidence while ensuring its authenticity and integrity, so that forensic investigations can be conducted after the event or after critical operations resume.

133. The LI should closely integrate plans for forensic readiness with plans for incident management and other related business planning activities.

134. The LI should train its staff so that all those involved in the particular incident understand their responsibilities related to handling the digital evidence, ensuring it is not compromised and valid as per the local jurisdiction.

G. Testing

This section provides guidance on what should be included in a LI's testing program and how testing results can be used to continuously improve the LI's cyber resilience posture. Vulnerability assessments, scenario-based testing, penetration tests, and red team tests are all part of the testing scope.

I. 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 LI, 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 LI and its environment is essential in determining the residual cyber risk to the LI'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 LI'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 chapter provides guidance on areas that should be included in an LI's testing and how results from testing can be used to improve the LI's cyber resilience posture on an ongoing basis. The scope of testing for the purpose of this guidance includes vulnerability assessments, scenario-based testing, penetration tests and tests using red teams.

II. Comprehensive Testing Program

An LI should have a comprehensive testing program to validate the effectiveness of its cyber resilience framework. Testing is a tool that LIs 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.

135. As part of its cyber resilience framework, the LI should establish and maintain a comprehensive testing program. The testing program should be developed using a risk-based approach and include a wide range of methodologies, practices, and tools for monitoring, assessing, and evaluating the effectiveness of the cyber resilience framework's core components.

136. The testing program should be reviewed and updated on a regular basis, taking into account the evolving threat landscape and the criticality of information assets.

137. When implementing its testing program, the LI should develop appropriate capabilities and involve all relevant internal stakeholders (including business lines and operational

units). These tests should include business continuity and incident and crisis response teams, where applicable.

138. To improve its cyber resilience stance, the LI should also collaborate with entities in its ecosystem. This collaboration helps to strengthen the LI's ecosystem's resilience.

139. The LI should involve its board and senior management appropriately (e.g., as members of crisis management teams) and inform them of test results.

140. To continuously improve its cyber resilience stance, the LI should establish policies and procedures to prioritize and resolve issues identified during the various tests, as well as perform subsequent validation to determine whether gaps have been addressed sufficiently.

141. The LI should ensure that the tests are carried out by independent parties, whether internal or external.

Methodologies, practices and tools

142. The LI should use a wide range of testing methodologies, practices, and tools, such as vulnerability assessments, scenario-based testing, penetration tests, and red team tests (which may overlap partly or be combined).

Vulnerability assessment

143. The LI should develop and regularly update a vulnerability management process to classify, prioritize, and resolve potential vulnerabilities identified in vulnerability assessments, as well as perform subsequent validation to determine whether gaps have been addressed sufficiently.

144. The vulnerability management process of the LI should help identifying exploitable weakness (which is a susceptibility or flaw in a system that an attacker can access and exploit to compromise system security) in critical systems and technologies, as well as conditions that allow for human error and accidents in critical functions, supporting processes, and information assets.

145. The LI should conduct vulnerability scanning of its external-facing services as well as internal systems and networks on a regular basis. These scans should rotate between environments to ensure that they reach all environments throughout the year.

146. The LI should conduct vulnerability assessments to identify bugs and weaknesses before deploying or redeploying new or existing services supporting critical functions, applications, and infrastructure components. These assessments should be performed on a regular basis, with change and release management processes in place.

147. The LI should conduct vulnerability assessments on running services, applications, and infrastructure components on a regular basis. It should monitor and evaluate the effectiveness of security controls to address identified vulnerabilities, as well as check for compliance with regulations, policies, and configurations.

148. As part of its vulnerability management process, the LI should develop and implement a variety of effective practices and tools (for e.g., a bug bounty program or static and dynamic code reviews), as well as appropriate safeguards to manage them.

Scenario-based testing

149. To evaluate and improve its incident detection capability, as well as response, resumption, and recovery plans, the LI should conduct various scenario-based tests, including extreme but plausible scenarios. The latter should be reviewed and tested on a regular basis. Scenarios-based tests can be tabletop exercises (sometimes abbreviated TTX or TTE-is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios) or simulations.

150. The LI should design tests that:

    a. address a sufficiently broad range of scenarios, such as simulation of extreme but plausible cyber-attacks;

    b. are intended 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. its response, resumption and recovery plans against cyber-attack scenarios which include data destruction, data integrity corruption, data loss, and system and data availability.

    e. cover breaches affecting multiple components of the LI's ecosystem in order to identify and analyze potential complexities, interdependencies, and potential contagion at the business and operational levels

151. The LI should use cyber threat intelligence (CTI) and cyber threat modelling to imitate the unique characteristics of cyber threats, to the extent possible.

152. In order to achieve greater operational resilience, the LI should also conduct exercises to test processes and staff's ability to respond to unfamiliar scenarios.

153. The LI should collaborate with the ecosystem to develop cybersecurity incident scenarios involving significant financial loss and use them for stress tests to understand potential spill overs and contagion risk to the ecosystem. With the help of the stress tests, it will improve its cyber resilience postures contributing to the improvement if the ecosystem's resilience as a whole.

154. When appropriate, the LI's board of directors and senior management should involve in scenario-based testing.

Penetration tests

155. Penetration tests should be performed by the LI to identify vulnerabilities that may affect its systems, networks, applications, people, or processes. These tests should simulate actual attacks on the LI's systems in order to provide an in-depth evaluation of their security.

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

157. The LI should include all critical internal and external stakeholders in penetration testing exercises, as appropriate. Application and system owners, as well as business continuity and incident and crisis response teams, could be among these stakeholders.

158. The LI should incorporate testing practices into its enterprise risk management process in order to identify, analyze, and fix cyber security vulnerabilities caused by new products, services, or interconnections.

159. The LI should perform security assessments and tests at all stages of the system development life cycle and at any level (business, application, and technology) for the entire application portfolio, including mobile applications.

160. The LI should implement best practices and automated tools to support processes and procedures for fixing technical and organizational weaknesses identified during testing exercises and ensuring compliance with approved policies and configurations.

Red team testing

161. The LI should use so-called red teams to introduce an adversary perspective in a controlled setting to challenge its own organization and ecosystem. Red teams test potential vulnerabilities as well as the effectiveness of an LI's mitigating controls, which include people, processes, and technology.

162. A red team can be made up of LI employees as well as outside experts who are, in either case, independent of the function being tested. The red team should conduct regular exercises and collaborate with its cyber defense team (e.g., blue team) to share findings and improve the LI's cyber resilience stance.

163. The LI should also use appropriate cyber threat intelligence (CTI) to inform its testing methods, such as by designing tests to simulate advanced threat agent capabilities and extreme but plausible scenarios. The LI should conduct red team exercises based on specific and plausible threat scenarios, using reliable and valuable CTI.

164. The LI should proactively engage in industry-wide exercises in order to test cooperation and coordination protocols and communication plans. These exercises should foster the LI's awareness on cross-sector cooperation and third-party risks.

III. Coordination

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

165. To the extent practicable and feasible, the LI should promote, organize, and manage exercises designed to test its response, resumption, and recovery plans and processes. Such exercises should include LI participants, critical service providers, and linked FMIs, as appropriate.

166. The LI should take part in industry-wide tests and exercises organized by the 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 carrying out their operations as usual.

167. Testing should include scenarios that cover breaches affecting multiple components of the LI's ecosystem.

H. Situational Awareness

This section provides guidance to the institutions on identifying sources of threat, using the information, sharing it with stakeholders so that the potential threat in the current payment market infrastructure could be timely identified and mitigated.

I. Preamble

Situational awareness refers to an LI'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 LI'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 LI better understand the vulnerabilities in its critical business functions, and facilitate the adoption of appropriate risk mitigation strategies. It can also enable an LI 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 LI and its ecosystem is an LI's active participation in information-sharing arrangements and collaboration with trusted stakeholders within and outside the industry. This chapter provides guidance for LIs to establish a cyber threat intelligence process, analysis and sharing processes.

II. 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.

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors. Threat intelligence enables LI to make faster, more informed, data-backed security decisions and change its behavior from reactive to proactive in the fight against threat actors.

Identification of potential cyber threats

168. The LI should identify cyber threats that could materially affect its ability to operate or provide services as expected, or that may have a significant impact on its ability to meet its own obligations or have knock-on effects within its own ecosystem. The LI should include in its threat analysis those threats that could cause extreme but plausible cyber events, even if they are thought unlikely to happen or have never happened before. This analysis should be regularly reviewed and updated.

Threat intelligence process

169. The LI should:

   a. create a process for gathering and analyzing relevant cyber threat information. The LI should include internal and external business and system information in its analysis to provide a business-specific context. This will turn information into usable CTI that provides timely insights and informs enhanced decision-making by enabling the LI to anticipate a cyber attacker's capabilities, intentions and modus operandi.

   b. have the ability to analyze collected data and assess the potential impact on its cyber resilience framework.

   c. gather and analyze cyber threat information and the production of cyber threat intelligence that are reviewed and updated regularly.

   d. use multiple sources of intelligence from internal and external sources (e.g., application, system and network logs; security products such as firewalls and intrusion detection systems; trusted threat intelligence providers; and publicly available information), correlated log analyses, alerts, traffic flows, cyber events in other sectors, and geopolitical events. This will allow the LI to better understand the evolving threat landscape and proactively take the appropriate measures to improve its cyber resilience capabilities.

Scope of cyber threat intelligence gathering

170. To acquire threat information, the LI should belong or subscribe to a threat and vulnerability information-sharing source and/or information-sharing and analysis center that provides information on cyber threats and vulnerabilities, where available.

171. The LI's cyber threat information should include analysis of real-world attackers' tactics, techniques, and procedures, as well as information on geopolitical developments that may trigger cyber-attacks on any entity within the LI's ecosystem.

172. The LI should use the threat information (for e.g., identified potential threat actors) collected from different sources, while considering its own business and technical characteristics, to:

   a. determine threat actors' motivations and capabilities (including their tactics, techniques, and procedures), as well as the extent to which the LI is vulnerable to a targeted attack from them;

   b. reassess the risk of technical vulnerabilities in operating systems, applications, and other software that could be exploited to launch attacks on the LI;

   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 LI's business processes and its reputation that could arise from such attacks; and

e. share information with relevant stakeholders in the ecosystem to achieve broader cyber resilience situational awareness, including promoting each other's approach to achieve cyber resilience;

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

Effective use of information

173. The LI should continuously use the CTI it has developed to assess and manage security threats and vulnerabilities in order to implement threat-informed cyber security controls in its systems and, more broadly, to continuously improve its cyber resilience framework and capabilities.

174. The LI should:

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

b. integrate and align its CTI process with that of its SOC. The LI should use information from its SOC to improve its CTI, and vice versa, it should use its CTI to inform its SOC;

c. use CTI to help inform and update its testing program to ensure it is up-to-date with the latest threat landscape, attackers' tactics, and vulnerabilities.

III. 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.

Planning ahead

175. The LI should define:

a. its information-sharing objectives in line with its business objectives and cyber resilience framework. At the very least, its objectives should include timely gathering and exchanging information that could facilitate in the detection, response, resumption, and recovery of its own systems and those of its participants during and after 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,
iii. those with whom the information can and should be shared.

c. how information provided to the LI will be acted upon (e.g., by employing the Traffic Light Protocol- TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP only has four colors; any designations not listed in this standard are not considered valid by FIRST).

176. The LI should establish and review its information-sharing rules and agreements on a regular basis. It should implement procedures that allow information to be shared promptly and in accordance with the objectives and scope define in the information-sharing rules and agreements, while also meeting its obligations to protect potentially sensitive data, the improper disclosure of which could have adverse consequences.

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

Information-sharing groups

178. The LI 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.

179. The LI should consider exchanging information on its cyber resilience framework with trusted stakeholders, as needed, to promote understanding of each other's approach to securing systems that are linked or interfaced. Such information exchange would help an LI and its stakeholders coordinate their respective security measures in order to achieve greater cyber resilience.

180. The LI should participate in efforts to identify and address gaps in current information-sharing mechanisms in order to facilitate an ecosystem-wide response to large-scale incidents.

181. In the event of an incident, the LI should plan for information-sharing through trusted channels, 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 LI's ecosystem during and after a cyber-attack.

I. Learning and Evolving

This section provides insights to the institution on how to increase the knowledge of staff about cyber threats in an ongoing basis, use the lesson learnt from occurred incidents to review and update the existing cyber resilience framework of the institution for strengthening its cyber resilience capability.

I. Preamble

An LI'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 LI should implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the LI to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. An LI should aim to instill a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

II. Ongoing Learning

An LI 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.

Lessons from cyber events

182. To enhance its cyber resilience capabilities, the LI should identify and categorize lessons learned (strategic, tactical, and operational) from real-life cyber incidents, both internal and external to the LI.

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

184. When highly visible cyber events or regulatory alerts occur, the LI should ensure that cyber security awareness materials are made available to staff.

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

Acquiring new knowledge and capabilities

186. The LI should:

   a. confirm that it has a program for continuous cyber resilience training. This training program should be conducted to board members and senior management at least once a year. Incident response, current cyber threats, and emerging issues (e.g., spear phishing, social engineering and mobile security) should all be covered in the annual cyber resilience training;

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

c. should have capabilities in place to use multiple sources of intelligence, correlated log analysis, alerts, traffic flows, cyber events across other sectors and geopolitical events to better understand the evolving threat landscape and proactively take the appropriate measures to improve its cyber resilience capabilities;

d. investigate new security approaches and technological capabilities that may improve the company's security posture. For example, in response to a mobile workforce and mobile devices, the adoption of cloud-based services, insider threats, and breaches in network perimeter security, some organizations are considering a zero-trust approach.

Predictive capacity

187. The LI's cyber risk management practices should include proactive protection against future cyber events in addition to reactive controls. The LI should strive for predictive capabilities by collecting data from multiple internal and external sources, defining a baseline for behavioral and system activity, and analyzing activities that deviate from the baseline.

III. Cyber Resilience Benchmarking

Metrics

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

188. Metrics and maturity models enable an LI to assess its cyber resilience maturity in relation to a set of predefined criteria, typically its operational reliability objectives. The LI must analyze and correlate findings from audits, vulnerability assessments, management information, incidents, near misses, tests, and exercises with external and internal intelligence for this benchmarking. Metrics can assist the LI in identifying gaps in its cyber resilience framework for remediation, as well as allowing the LI to systematically evolve and achieve more mature states of cyber resilience.

189. To assess the performance and effectiveness of its testing program, the LI should develop, monitor, and analyze metrics. The LI should use the results of the analysis to improve its testing program.

190. The LI should create a set of indicators and management information to measure and monitor the effectiveness of the cyber resilience strategy and framework, as well as its evolution over time. Relevant information and indicators could include, for example:

a. the percentage of the LI's employees that have received cyber security training;

b. the percentage of incidents reported within the required time frame for each incident category;

c. the percentage of vulnerabilities that were mitigated within a specified time period after discovery; and

d. yearly reports monitoring progress of indicators, etc.

J. Glossary

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 LI. A smaller attack surface means that the LI is less exploitable and an attack less likely. However, reducing attack surfaces does not necessarily re- duce 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
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.

Term	Definition
	Source: NIST Glossary
Breach	Compromise of security that leads to the accidental or un- lawful destruction, loss, alteration, unauthorized 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 LI's stakeholders. A business process may comprise several assets, including information, ICT resources, personnel, logistics and organizational 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 LI'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 unauthorized 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 LI, 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 per- sons, 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) jeopardizes the cybersecurity of an information system or the information the system processes, stores or transmits; or ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. Source: FSB Cyber Lexicon
Cyber resilience	An LI'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 LI has established to identify, protect, detect, respond to and re- cover from the plausible sources of cyber risks it faces. Source: CPMI-IOSCO
Cyber resilience strategy	An LI'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 LI 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 LI's cyber risk should support the business processes and be integrated in the LI's overall risk management framework. Source: CPMI-IOSCO

Term	Definition
Cyber risk profile	The cyber risk actually assumed, measured at a given point intime. Source: CPMI-IOSCO
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, analyzed, 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
Defense 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 (DemilitarizedZone) 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 authorized access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorized 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 organization's ability to perform its critical operations. Source: CPMI-IOSCO
Distributed denial of service(DDoS)	A denial of service that is carried out using numerous sources simultaneously.

Term	Definition
attack	Source: FSB Cyber Lexicon
Ecosystem	A system or group of interconnected elements formed linkages and dependencies. For an LI, this may include participants, linked FMIs, service providers, vendors and vendor products. Source: CPMI-IOSCO
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 LI to maximize the use of digital evidence to identify the nature of a cyber-attack. Source: CPMI-IOSCO
Governance (CRG risk management category)	The set of relationships between an LI's owners, board of directors (or equivalent), management, and other relevant parties, including participants, authorities, and other stake- holders (such as participants' customers, other interdependent LIs, and the broader market). Governance provides the processes through which an LI 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

Term	Definition
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
Information asset	Any piece of data, device or other component of the environment that supports information-related activities. In the con- text 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 as- sets 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 do- main) 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 acomponent of a system, the property of not having been modified or destroyed in an unauthorized manner. Source: CPMI-IOSCO
Internet Protocol security (IP-Sec)	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 LI applies multiple detection controls rather than relying on a single control. See layered protection and defense in depth. Source: Bank of Canada

Term	Definition
Layered protection	As relying on any single defense against a cyber threat may be inadequate, an LI can use a series of different defenses 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 "defense 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
Licensed Institution (LI)	Institution licensed by Payment Systems Department of Nepal Rastra Bank.
Malware	Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of mal- ware include computer viruses, worms, Trojans, spyware, and adware. Source: CCCS
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 LI 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

Term	Definition
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 circum- vent 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
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 re-sources 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 organization to test its defenses and improve its effective- ness. A red team views the cyber resilience of an LI from an adversary’s perspective. Source: CPMI-IOSCO

Term	Definition
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 conceptualization 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 LI 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
	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

Term	Definition
Risk tolerance	The acceptable level of variation (from the organization's risk appetite) relative to achievement of a specific objective. In set- ting 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 LIs identify, assess and understand therisks 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 protectthe 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 center	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 downloading and executing files that appear to be benign butare 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

Term	Definition
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 behavior of a *threat actor*. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior 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 orunintentionally exploit one or more vulnerabilities in an LI's systems, resulting in a loss of confidentiality, integrity or availability. Source: CPMI-IOSCO
Threat actor	An individual, a group or an organization believed to be operating with malicious intent. Source: FSB Cyber Lexicon
Threat assessment	Process of formally evaluating the degree of threat to an in- formation system or enterprise and describing the nature ofthe threat. Source: NIST Glossary
Threat vector	A path or route used by the *threat actor* to gain access to thetarget. Source: FSB Cyber Lexicon
Transport layer security (TLS)	An authentication and encryption protocol widely implemented in browsers and web servers. HTTP traffic transmit- ted using TLS is known as HTTPS. 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
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

Term	Definition
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

K. References

Bank of Canada, “Expectations of Cyber Resilience of Financial Market Infrastructure (FMI)”, October 2021. Available at https://www.bankofcanada.ca/wp-content/uploads/2021/10/expectations-cyber-resilience-financial-market-infrastructures.pdf.

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).

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 Inclusion Global Initiative (FIGI), World Bank Group, International Telecommunications Union (ITU), “Cyber Resilience for Financial Market Infrastructures,” November2019.Available at https://thedocs.worldbank.org/en/doc/189821576699037673-0130022019/original/FIGIECBOperationalCyberFinalWeb1213.pdf