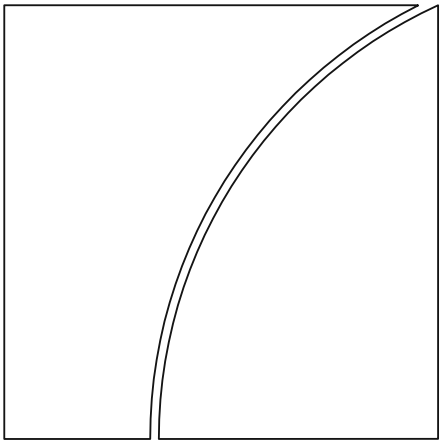
Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions



Cyber resilience toolkit: practical considerations for FMIs

September 2026

BIS

IOSCO

This publication is available on the BIS website (www.bis.org) and the IOSCO website (www.iosco.org).

ISBN 978-92-9259-968-3 (online)

Contents

Introduction

In April 2012, the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published the *Principles for financial market infrastructures* (PFMI). The PFMI set standards for the design and operation of key financial market infrastructures (FMIs) in order to enhance their safety and efficiency and, more broadly, to limit systemic risk and foster transparency and financial stability. The PFMI apply to all systemically important payment systems, central securities depositories , securities settlement systems , central counterparties (CCPs) and trade repositories (referred to collectively as FMIs). These FMIs clear, settle and record transactions in financial markets.

In 2016, CPMI-IOSCO published guidance to the PFMI to enhance FMIs' cyber resilience, primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20). The *Guidance on cyber resilience for financial market infrastructures* (Cyber Guidance) is not intended to impose additional standards on FMIs beyond those set out in the PFMI.

Cyber risks to financial institutions, such as FMIs, are intensifying. The volume of cyber attacks on financial institutions has more than doubled since 2020, and two thirds of phishing schemes between August 2023 and July 2024 targeted financial institutions and their clients.[1,2] Furthermore, artificial intelligence (AI) models and tools are reshaping cyber security across industries. The 2022 CPMI-IOSCO *Implementation monitoring of the PFMI: Level 3 assessment on financial market infrastructures' cyber resilience* (L3 assessment) identified a number of areas where FMIs' implementation of the PFMI, informed by the Cyber Guidance, could be enhanced.[3] The L3 assessment's findings and the evolving threat environment highlight the need for practical, adaptable resources to support effective, real-world implementation of the Principles.

While the PFMI and Cyber Guidance remain highly relevant and fit for purpose, CPMI-IOSCO member discussions and workshops with industry have recognised that additional practical, targeted support may assist FMIs in enhancing their cyber resilience. This cyber resilience toolkit has been jointly developed by CPMI and IOSCO, informed by the findings of the L3 assessment, the evolving threat environment and by the work of other bodies on cyber resilience,[4] to support FMIs as they seek to strengthen their cyber resilience frameworks and implement operational resilience-related components of the PFMI, as informed by the Cyber Guidance. The intended audience for this toolkit includes authorities, FMI board members, senior management and personnel with operational and cyber risk- and resilience-related responsibilities.

The toolkit is not intended to alter or replace any part of the PFMI or cyber guidance. Instead, it provides supplemental detail related to the preparations and measures that FMIs may undertake to enhance their cyber resilience capabilities, with the objective of limiting the escalating risks that cyber threats pose to financial stability.

1 F Natalucci, M Qureshi and F Suntheim, "Rising cyber threats pose serious concerns for financial stability", *IMF Blog*, 9 April 2024.

2 J Leydon, "11 biggest financial sector cyber security threats", *CSO*, 20 November 2024.

3 The L3 assessment, which considers consistency in the outcomes of FMIs' implementation of the PFMI, identified one serious issue of concern regarding the consistency of FMIs' cyber response and recovery plans and four issues of concern regarding FMIs' cyber resilience planning and testing.

4 See Annex 2B.

The cyber resilience toolkit

This toolkit comprises a set of voluntary, non-binding tools which contain practical considerations across four topics relevant to enhancing the cyber resilience of FMIs, consistent with the PFMI as informed by the Cyber Guidance: (i) governance of cyber risk and resilience; (ii) scenario identification and design; (iii) response, resumption and recovery plans; and (iv) testing and exercising (Table 1).[5] The individual tools can be used in isolation or in combination with each other. The toolkit has not been designed, and is not suitable to be used, for measuring or assessing an FMI's compliance with or liability under any law or regulation. The practical considerations are intended to be technology neutral and applicable to a wide range of FMIs. They are not intended to provide exhaustive coverage of a given topic.

Key features of the cyber resilience toolkit — Table 1

Tool		Key features
1.	**Governance of cyber risk and resilience at FMIs**	Tool 1 provides practical considerations which may assist FMIs in strengthening the governance of FMIs' cyber resilience frameworks by providing practical considerations on the following: ● The appraisal of the board's collective cyber-related skills and training programmes. ● Management of risks arising from an FMI's ecosystem. ● Cyber resilience maturity models for gauging the adequacy and effectiveness of an FMI's cyber resilience framework. ● Examples of cyber resilience metrics which may be useful when reporting to board members, senior management and key persons in control functions.
2.	**Scenario identification and design**	Tool 2 provides practical considerations for the construction of extreme but plausible scenarios by outlining potential strategies and methodologies for their design using a risk-based approach, including: ● Designing scenarios that test an FMI's cyber resilience framework according to an FMI's specific needs. ● Supporting strategies, methodologies and resources which may be useful in scenario design. ● Identifying challenges posed to FMIs by extreme cyber scenarios.
3.	**Response, resumption and recovery plans**	Tool 3 provides practical considerations which may assist FMIs in the design of resumption and recovery planning, including: ● Identifying the critical operations and information assets required to resume operations within two hours following disruptive events. ● Identifying the key design elements of response, resumption and recovery plans. ● Handling disconnection and subsequent safe reconnection of ecosystem entities (eg service providers, participants and linked FMIs) facing cyber incidents. ● Implementing infrastructure and data resilience measures to support safe and rapid recovery from cyber incidents. ● A questionnaire FMIs could use to assist self-assessment of their cyber resilience posture.
4.	**Cyber resilience testing and exercising**	Tool 4 provides practical considerations for FMIs in designing cyber resilience testing programmes, including: ● Categories of testing and exercising to assess resilience posture at various stages of development and after significant system changes. ● Tailoring a test programme to an FMI's needs by combining the various categories of testing and exercising. ● Conducting (and benefiting from) advanced testing and exercising such as red team tests and threat-lead penetration testing. ● Learning and evolving from the results of cyber resilience testing and exercising or from real or simulated cyber incidents to identify enhancements to an FMI's cyber resilience framework.

[5] This is without prejudice to legal and regulatory requirements. Other considerations may be appropriate depending on an FMI's specific needs and legal or regulatory requirements.

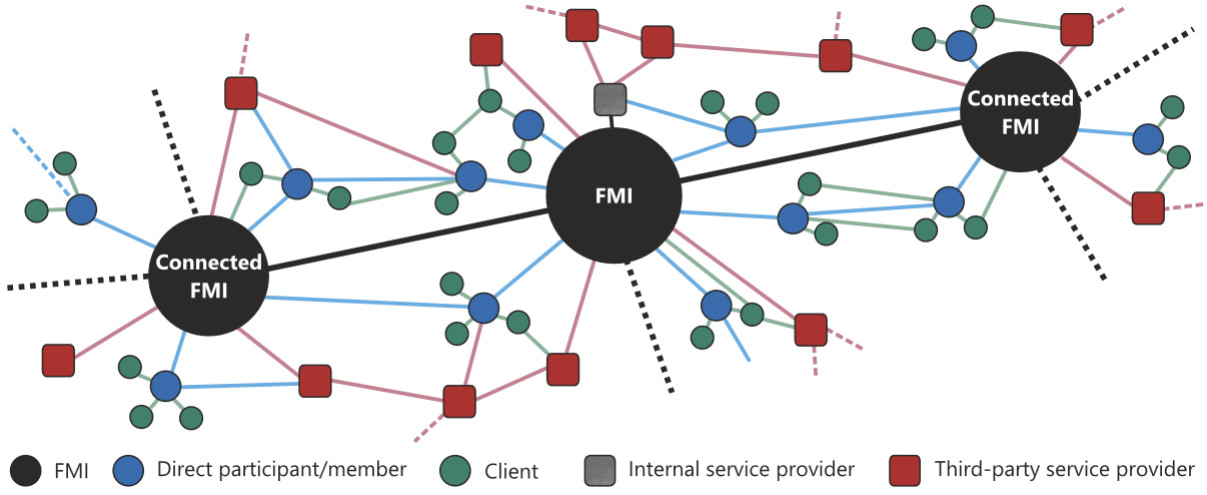
The toolkit is intended to be used with due consideration to an FMI's risk profile and the scale, complexity and nature of the activity it undertakes. An FMI may use the materials within the toolkit individually or in combination depending on its specific needs and priorities. They are designed to enable consideration of an FMI's specific threat landscape, ecosystem and ICT requirements.[6]

Ecosystem considerations in the toolkit

FMIs are digitally connected and interdependent with a larger ecosystem of entities, such as FMIs' participants, linked FMIs, internal and third-party service providers, vendors and critical infrastructures, collectively referred to as "ecosystem entities" (Figure 1).[7] Given the central role FMIs play in the financial system, vulnerabilities in ecosystem entities or the FMI itself can create channels for contagion, with cascading impacts. These risks can manifest through malicious cyber attacks, system failures or human errors affecting any entity within the ecosystem.

Stylised view of an FMI's ecosystem

Figure 1



Source: CPMI

Each tool in this toolkit provides some considerations for identifying, managing and mitigating the cyber risks that FMIs face from (and pose to) the entities in their ecosystems. This approach recognises that cyber resilience cannot be achieved in isolation and reminds FMIs to consider the bidirectional interdependencies present in each aspect of their cyber resilience frameworks.

Developments in artificial intelligence

Developments in AI models and tools are reshaping cyber security, requiring FMIs to adapt their defences against the speed, volume and complexity of AI-driven threats. Where traditional security

[6] ICT = information and communications technologies. ICT can also be read as IT (information technology) in this document.

[7] Annex A of the Cyber Guidance defines ecosystem as "A system or group of interconnected elements, formed linkages and dependencies. For an FMI, this may include participants, linked FMIs, service providers, vendors and vendor products." Section 3.3 of the Cyber Guidance describes the entities within an FMI's ecosystem as including "participants, linked FMIs, settlement banks, liquidity providers, service providers, critical infrastructures such as energy and telecommunications, vendors and vendor products". For the purposes of this toolkit, service providers could include third-party and nth-party providers.

processes relied on detection, analysis and remediation cycles measured in days or weeks, AI-driven threats can now identify vulnerabilities and craft exploits in hours.

Developments in AI models and tools have also lowered the barrier to entry for malicious actors and increased the number of threat actors with sophisticated capabilities. The continued rapid improvement of AI capabilities may require FMIs to adapt their defensive measures and the policies, procedures and controls that support their cyber resilience frameworks to meet the evolving threat landscape.

In response to these developments, the toolkit contains a number of practical considerations for adapting to the risks from and leveraging the benefits of ongoing developments in AI.[8]

[8] See also FSB, *Sound Practices for Responsible Adoption of Artificial Intelligence (AI): consultation report*, 2026, www.fsb.org/uploads/P100626.pdf.

1 Governance of cyber resilience at FMIs

1.1 Introduction

Robust cyber governance enables an FMI to adopt a more comprehensive and forward-looking approach to addressing dynamic and evolving cyber threats and helps to embed cyber risk management throughout the organisation.

This tool is intended to assist in strengthening the governance of an FMI's cyber resilience framework and provides practical considerations for the training and assessment of board members and senior management with responsibilities for cyber risk and cyber resilience. It also provides considerations for managing risks arising from an FMI's ecosystem as well as insight into the use of risk management metrics and maturity models to appraise and report on the adequacy and effectiveness of an FMI's cyber resilience framework (CRF).[9]

1.2 Practical considerations for the governance of cyber risks

1.2.1 Board member cyber skills and training

A baseline level of cyber knowledge equips all board members to provide effective challenge, evaluate management recommendations and respond effectively during cyber incidents.

Board members who are not cyber risk experts may consider appropriate training to improve their cyber risk management and cyber resilience-related skills. Examples of the forms of training which may help include:

- Periodic workshops on key cyber resilience issues and emerging trends. These may include dedicated sessions focusing on the analysis of specific threats, attacks, trends or technologies relevant to the FMI. Such initiatives may help to increase the level of cyber resilience knowledge and, at the same time, provide insights into the primary current and emerging risks.
- Awareness and security training sessions by internal or external providers, new director induction training, regular ICT/cyber briefings (eg on emerging risks), dedicated cyber workshops, etc.
- Discussions of real-life case studies regarding operational or cyber incidents affecting the FMI itself or any entity belonging to its ecosystem or incidents that have occurred at other FMIs or in other financial or economic sectors.
- Training on the FMI's AI deployments, AI provider concentration and AI-enabled adversary capabilities.
- Participation in cyber security simulations where the scenario requires the involvement of board members for decision-making according to the response, resumption and recovery plans adopted by the FMI.

Techniques for maximising the effectiveness of training include aligning training with business objectives and outcomes (eg efficiency, service availability, confidentiality, etc), fostering open discussions and exercises/simulations.

[9] Annex A in the Cyber Guidance defines a CRF as consisting of "the policies, procedures and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces".

The board may consider supplementing the cyber risk expertise of its members through continuing professional education, maintaining experienced staff or engaging external independent organisations or consultants to report to or advise the board. [10]

1.2.2 Board and senior management considerations for managing risks arising from an FMI's ecosystem

Board and senior management engagement in strategy development, oversight and coordination activities strengthens an FMI's ability to manage cyber risks across its ecosystem. Examples of practical considerations with respect to board and senior management for addressing risk arising from an FMI's ecosystem which could be incorporated in the FMI's Cyber Resilience Strategy (CRS) and CRF may include :[11]

- Incorporating ecosystem-related risk considerations into the FMI's CRF. For example, it could outline how ecosystem-related risks are identified, monitored and managed from an end-to-end perspective, given the interconnected nature of its technology and processes.
- Actively involving the board and senior management in overseeing ecosystem-related risk management as part of the FMI's cyber resilience strategy and CRF.
- Including board and senior management participation in planning and executing testing exercises that assess interdependencies and response coordination across entities in the FMI's ecosystem.
- Integrating the CRF with the broader enterprise-wide risk management framework, to facilitate incorporation of evolving and emerging ecosystem-related risks.

1.3 Cyber resilience benchmarking

Maturity models are used to help identify gaps in an FMI's CRF for the remediation and evolution of its maturity level.[12] Maturity models may aid an FMI's board and senior management in assessing and measuring the adequacy and effectiveness of the FMI's CRF. The use of maturity levels within a maturity model provides a benchmark against which an FMI can measure progression and establish priority areas for improvement.

The use of metrics can assist an FMI in pinpointing shortcomings in its CRF and enable it to methodically measure progress towards more advanced maturity levels.

[10] Relevant certifications for senior managers include eg COBIT (Control Objectives for Information and Related Technologies), ISACA Certified Information Systems Auditor (CISA), ISACA Certified in Risk and Information Systems Control (CRISC), Society of Corporate Compliance and Ethics Certified Compliance & Ethics Professional (CCEP), ISC2 Certified Governance Risk and Compliance (CGRC), Institute of Internal Auditors Certification in Risk Management Assurance (CRMA), and ISACA Certified in the Governance of Enterprise IT (CGEIT). A relevant reference framework for cyber security roles and competencies may be the ENISA European Cybersecurity Skills Framework.

[11] Annex A in the Cyber Guidance defines a CRS as "An FMI's high level principles and medium term plans to achieve its objective of managing cyber risks."

[12] Annex A in the Cyber Guidance defines cyber maturity model as "A mechanism to have cyber resilience controls, methods and processes assessed according to management best practice, against a clear set of external benchmarks."

1.3.1 Cyber maturity levels

Many financial institutions, including FMIs, use a maturity model that uses defined tiers introduced by a sector-agnostic model then maps sector-specific requirements onto that scale.[13] Some cyber resilience maturity models are tailored to FMIs, some to depository institutions and others to jurisdiction-specific banking sectors.[14]

Different models use maturity levels that are not always directly comparable, but they generally align in their objectives. While models vary in terminology and detail, they typically describe a similar progression. This starts with basic or ad hoc practices (eg initial, baseline, evolving), moves to risk-informed, standardised execution (eg intermediate, advancing) and culminates in intelligence-led, data-driven continuous improvement. Box 1 provides examples of practical considerations for inclusion in the different tiers of a maturity model, and Annex 1A provides a comparison of common cyber resilience maturity models.

Box 1

Example of cyber resilience maturity levels applied to an FMI: learning and evolving

An FMI may use levels of expectations/maturity levels such as the following to assess the current level of its maturity, measure progression and define steps for future enhancements.

Initial/baseline/evolving: essential capabilities are established; performance of practices is monitored and managed

- Establish information-gathering capabilities on vulnerabilities, threats, events and incidents occurring both within and outside the FMI.
- Analyse gathered information and assess potential impacts on the FMI's cyber resilience framework.
- Classify and incorporate lessons learned, identify the key stakeholders to whom these apply, incorporate them to improve the FMI's cyber resilience framework and capabilities, and convey them to each relevant stakeholder on an ongoing basis.
- Implement annual cyber resilience training for all staff, including senior management.
- Provide up-to-date cyber security awareness materials when prompted by highly visible cyber or operational incidents or by regulatory alerts.
- Incorporate lessons learned into training programmes.
- Develop indicators to measure cyber resilience strategy effectiveness.

Intermediate/advancing: advanced tools are integrated across the FMI's business lines and have been improved over time to proactively manage the cyber risks that the FMI is exposed to

- Validate the effectiveness of incorporating lessons learned into the employee training and awareness programmes on a regular basis.
- Monitor technological developments (such as the development of AI capabilities) and acquire new cyber risk management policies and processes to manage the associated risks.

[13] The US NIST Cybersecurity Framework (CSF) is an example of a sector-agnostic model. This framework provides functions, categories and subcategories with four implementation tiers: partial, risk-informed, repeatable, adaptive. These tiers are widely used as a maturity scale in finance. See www.nist.gov/cyberframework.

[14] Annex 1A provides examples from different jurisdictions of financial institution- and FMI-specific maturity models that an FMI may use or tailor to its own context (eg when an FMI's board sets objectives for maturity levels to be reached and maintained within a certain time frame).

- Analyse and correlate findings from audits, incidents, tests and intelligence to enhance and improve cyber resilience capabilities.
- Incorporate lessons from real-life cyber or operational incidents and testing results to improve risk mitigation capabilities, as well as cyber contingency, response, resumption and recovery plans.
- Track progress using a maturity model.
- Participate in information-sharing arrangements promoting awareness and sharing of best practices.

Advanced/innovating: enhanced capabilities driving ecosystem-wide innovation to manage cyber risks and enhance cyber resilience

- Utilise multiple intelligence sources (eg correlated log analysis, alerts, traffic flows, cyber events across other sectors and geopolitical events) to understand the evolving threat landscape.
- Proactively improve cyber resilience capabilities based on comprehensive analysis.
- Participate in industry-wide or cross-sector exercises, enabling testing of cooperation arrangements and assessment of resilience at the ecosystem level based on realistic scenarios.

1.3.2 Examples of quantitative cyber resilience metrics

Tracking quantitative measures and metrics can help an FMI to monitor and assess operations against cyber resilience and cyber risk tolerance thresholds. Maintaining both historical and predictive metrics may provide insights into trends, patterns and causes of specific outcomes; may help inform decision-making; and serves as a benchmark for future performance.

Broadly, different metrics may be of interest to board members, senior management and key persons in control functions. Board members require high-level, strategic metrics to align cyber resilience with business objectives and risk appetite, whereas senior management may be more focused on operational metrics to track the implementation of the cyber resilience framework and ensure readiness for threats. Key persons in control functions typically use metrics to validate the effectiveness of controls processes, ensure compliance and identify areas for improvement.

Table 2 provides a non-exhaustive list of example metrics for measuring cyber risk and resilience.

Cyber resilience framework example metrics — Table 2

Reporting category/description	Examples of metrics
Strategic metrics	
Cyber risk management and posture Ensure that cyber risks are identified, assessed and addressed effectively; provide a high-level view of the organisation's cyber risk exposure and mitigation efforts.	• Residual risk rating • Count of open high-risk findings • Critical vulnerability remediation time • Third-party cyber risk status • Business-critical system coverage • Number of risk assessments conducted • Percentage of critical risks mitigated for critical assets • Percentage of risks within risk appetite
Strategic progress Assess progress in implementing cyber resilience strategies and improving board awareness.	• Percentage of initiatives completed or on track • Risk reduction achieved • Resilience enhancement progress • Critical capability gaps closed • Budget-to-progress alignment • Results of board-level cyber training

Resource allocation Monitor the adequacy and efficiency of resource allocation for cyber resilience initiatives.	• Percentage of budget utilised for cyber resilience • Ratio of cyber resilience to ICT spending • Cyber budget allocation by risk area • Staffing levels versus target operating model • Open cyber roles/vacancy rate • Critical services support coverage • Third-party security spend
Training and awareness Assess the organisation's efforts to build a cyber-resilient culture and improve employee awareness.	• Percentage of phishing simulation click-through • Mandatory cyber training completion rate (per cent) • Role-based training completion rate (per cent) • Training assessment scores • Awareness campaign engagement • Reduction in human-error incidents
Operational metrics	
Incident trends and response Measure the readiness and effectiveness of incident response capabilities.	• Number of significant cyber or operational incidents • Mean time to detect (MTTD), respond (MTTRes) and recover (MTTRec) • Number of incident response drills • Incident volume by severity • Escalation timeliness • Repeat incident rate • Number of open incident remediation items • Number of open incident remediation actions past due
Recovery and resumption Track resilience and readiness for recovery following an incident.	• Frequency of disaster recovery exercises (number of times per year) • Percentage of successful restorations from backups • Critical services resumed within tolerance • Disaster recovery and business continuity exercise results
Vulnerability Evaluate the effectiveness of vulnerability management and operational controls.	• Percentage of vulnerabilities remediated • Percentage of IT assets covered by vulnerability scanning • Critical/high vulnerability count • Median time to remediate critical vulnerabilities • Average vulnerability age
Risk posed to an FMI by its ecosystem Monitor and mitigate risks arising from ecosystem entities.	• Percentage of vendors assessed for cyber risks • Number of ecosystem-related incidents • Vendor remediation timeliness • Vendor incident notification timeliness • Critical service provider concentration
Threat intelligence Track the organisation's ability to anticipate and respond to emerging threats.	• Number of actionable insights generated • Volume and types of detected threats • Threat-informed detection coverage
Control and effectiveness metrics	
Control effectiveness Evaluate the effectiveness of cyber resilience controls.	• Percentage of key controls tested and effective • Deviations from security configurations or baselines • Key control pass/fail rate • Control exception rate • Preventive versus detective control coverage • Control coverage (people/process/technology) for critical assets • Repeat control failures
Cyber security controls	• Malware stopped or detected • Phishing sites identified

Measure the organisation's ability to prevent and detect malicious activities, ensuring operational security.	• Blocked malicious connections
Effectiveness of monitoring and detection Assess the effectiveness of monitoring tools and processes.	• Number of alerts generated and investigated • False positive/negative rates in detection systems • Detection coverage across critical assets • Alert volume by severity • Log source coverage • Escalation rate to incident response
Effectiveness of cyber security programme over time Measure the overall efficiency and maturity of the organisation's cyber resilience programme over time.	• Residual risk trend • Control maturity score and trend • Vulnerability remediation trend • Incident severity trend • Detection and response improvement
Compliance metrics	
Audit and compliance Verify the effectiveness of controls and adherence to regulatory requirements.	• Number of internal audits completed • Percentage of compliance gaps remediated • Audit finding volume and severity • Audit finding remediation timeliness • Audit control failures
Regulatory reporting and compliance Ensure timely and accurate reporting to regulators and avoid compliance issues.	• Status of compliance with regulations • Timeliness of reports submitted to regulators • Number of regulatory inquiries or penalties • Results of regulatory audits • Regulatory finding inventory status • Cyber incident notification readiness

Annex 1A Comparison of cyber resilience maturity models

The objectives of cyber maturity models are generally in broad alignment. While terminology and the level of granularity may vary, all models describe a similar maturation arc from foundational or ad hoc practices through to risk-informed, standardised execution, arriving at intelligence-led, data-driven and continuous improvement. Table 1A.1 sets out a high-level description of cyber maturity levels from CRF examples.

Comparison of cyber resilience maturity models[15] Table 1A.1

Framework (jurisdiction)	Number of tiers/levels	Terminology	Progression through tiers (low → high)
NIST CSF **(Global)**	Four	Tier 1–4: partial; risk-informed; repeatable; adaptive	Ad hoc/limited awareness → risk-informed practices → documented and consistently applied → continuously improved, intel-driven, integrated with ERM
ECB CROE **(European Union)**	Three (staged expectations)	Commonly referred to as: baseline/evolving; advancing; innovating	Evolving: essential capabilities are established; performance of practices is monitored and managed → Advancing: advanced tools are integrated across the FMI's business lines and have been improved over time to proactively manage cyber risks posed to the FMI. → Innovating: enhanced capabilities drive ecosystem-wide innovation to manage cyber risks and enhance cyber resilience
HKMA CFI – C RAF **(Hong Kong SAR)**	Three (applies to 26 components across seven domains)	Baseline; intermediate; advanced	Core controls and foundational governance → risk-based, standardised and consistently applied practices (baseline + intermediate control principles) → integrated with ERM, threat-informed, automated (baseline + intermediate + advanced control principles)
SAMA CSF **(Saudi Arabia)**	Five	L1 initial/ad hoc; L2 managed/repeatable; L3 defined; L4 quantitatively managed; L5 optimised	Fragmented/reactive → basic and repeatable → enterprise-defined and comprehensive → data-driven/performance managed → continuously improved, predictive/intel-driven

Table 1A.2 provides an approximate alignment among the individual tiers of the models in Table 1A.1.

Approximate alignment of maturity models' tiers Table 1A.2

NIST CSF	ECB CROE	HKMA C-RAF	SAMA CSF
Tier 1: partial	Baseline/evolving	-	Level 1: initial
Tier 2: risk-informed	Evolving → advancing (transition)	Baseline	Level 2: managed/repeatable
Tier 3: repeatable	Advancing	Intermediate	Level 3: defined
Tier 4: adaptive	Innovating	Advanced	Level 4–5: quantitatively managed/optimised

[15] CSF = cyber security framework; CROE = cyber resilience oversight expectations; CFI = cybersecurity fortification initiative; C RAF = cyber resilience assessment framework; ERM = enterprise risk management.

2 Extreme but plausible cyber scenario identification and design

2.1 Introduction

This tool is intended to assist an FMI in developing extreme but plausible cyber scenarios. These scenarios can be used when: (i) designing the FMI's ICT architecture and business/IT processes; (ii) designing business continuity plans (as well as response, resumption and recovery plans); and (iii) conducting related cyber resilience tests and exercises. Scenarios help an FMI to build resilience capabilities and assess the effectiveness of processes and technical capabilities put in place to identify, protect, detect, respond to and recover from cyber attacks that are not prevented.

Since the cyber threat landscape is dynamic and evolving, benchmark scenarios may change over time as new threats and risks emerge. Updating scenarios may help an FMI and its ecosystem entities prepare for these emerging threats and maintain the resilience of their ICT infrastructures and operational processes.

This tool provides practical considerations for developing these cyber scenarios, beginning with identifying the objectives and scope, and then understanding the landscape and situation specific to the FMI. It also provides factors to consider in designing scenarios and adding complexity.

A set of resources that may aid an FMI in designing scenarios is included as Appendix 2B.

2.2 Blueprint for building extreme but plausible scenarios

This section provides a practical blueprint detailing strategies and methodologies that can be used to identify and design extreme but plausible cyber scenarios. The blueprint contains four elements that provide a step-by-step approach to developing scenarios and two boxes that provide additional considerations for tailoring scenarios to an FMI's unique business context.

2.2.1 Define objectives and scope

Defining the objectives and scope can help to calibrate the development of scenarios based on an FMI's unique needs and business context. The following considerations and questions can help with this process:

- Define objectives: What are the strategic decisions the FMI is trying to inform and who are the key decision-makers? What are the risks the FMI seeks to assess and which ecosystem entities should be considered?
- Identify the scope and boundaries: What are the FMI's critical assets and systems, risk appetite, critical operations and processes, ecosystem entity interconnections and relevant past incidents? What is most relevant to the FMI's context? What is within scope and out of scope?
- Establish procedures for scenario formulation: What are the FMI's structured procedures to guide scenario development, considering various attack vectors and potential impact factors?[16]
- Follow an established governance framework: How does the FMI's governance framework and independent review function contribute to the integrity and consistency of the scenario development process? In particular, who in the organisation reviews and approves the development of scenarios? Does the FMI have a dedicated scenario development group? Is there an independent group positioned to provide effective challenge in the scenario development process? Does the scenario development function take a cross-divisional

[16] Details on potential failure scenarios may also be captured as part of the ICT business continuity policy.

approach to incorporate knowledge of other business functions (eg finance, risk, legal, operations, etc) into cyber scenarios?

2.2.2 Gather scenario inputs

The following scenario inputs help to tailor the scenarios based on the current threat landscape and the FMI's ICT infrastructure:

- Identify information assets: Identifying and understanding information assets enables an FMI to better understand how a cyber incident may affect its systems.[17] One way to identify information assets is to map infrastructure components and ICT assets, including dependencies on third parties for critical operations (see sections 3.2 and 3.3 for additional information). This analysis may consider interconnections and interdependencies with internal or external ICT systems that might amplify impacts. See Box 2 for considerations on the identification of risks arising from the FMI's ecosystem.
- Incorporate lessons learned from previous cyber and operational incidents and testing to inform what aspects of the cyber scenarios require adjustment.
- Assess the impact that a disruption may have on an FMI's operations and risk profile.[18]
  - This assessment may include recognition of the role an FMI's critical operations play in the functioning of the financial system, and of its interconnectedness with entities in its ecosystem, especially those that may present implications to resumption and recovery.
- Develop and incorporate threat intelligence along three dimensions – strategic, tactical and operational – to inform FMIs' protection and detection controls, response plans and resumption (see Table 3).
  - Threat intelligence is collected, developed and updated by reviewing sources and conducting risk assessments to evaluate the likelihood and impact of risks materialising. Significant changes in the cyber threat landscape may warrant updating an FMI's cyber security procedures or risk tolerance. For example, AI-driven threats that craft exploits in hours may require FMIs to adapt their procedures and risk tolerance frameworks to implement incremental mitigations based on tactics, techniques and procedures (TTPs) identified by threat intelligence.
  - Considering the evolving cyber threat landscape, threat intelligence may be based on incidents that have occurred in other contexts outside the FMI community.

[17] The Cyber Guidance defines information asset as: "Any piece of data, device or other component of the environment that supports information-related activities. In the context of this report, information assets include data, hardware and software. Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services."

[18] This may be referred to as a business impact analysis (BIA). BIA is defined inter alia in ISO/TS 22317:2021, NIST IR 8286D, BSI Standard 200-4 (available in German). The NIST Glossary describes a BIA as a "Process of analyzing operational functions and the effect that a disruption might have on them" (https://csrc.nist.gov/glossary/term/business_impact_analysis). Further, the BSI describes a BIA as an analysis to identify critical business processes and resources as well as parameters for their recovery after interruptions. It is followed by a risk analysis to examine the risks that critical processes and resources are exposed to.

Threat intelligence dimensions Table 3

Dimension	Threat intelligence output	Scenario design element	Response, resumption and recovery
Strategic	Risk scenarios, summaries of the threat landscape, business impact assessments, resilience goals	Define big picture situations and what is most important to keep running (eg extortion malware affecting essential services, supplier disruption)	Set policies and structure: separate critical networks, plan backup and recovery, manage access responsibly, assess supplier security and prepare crisis communications
Operational	Practical guides for likely attacks, ideas for what to search for, prioritised alerts, monitoring plans, step-by-step response procedures	Describe likely attackers, their methods, stages of an attack, possible entry points and conditions they rely on	Build procedures and alerts, make sure the right data are captured, define clear steps and handoffs between teams, set escalation paths
Tactical	Lists of warning signs, pattern-matching rules, blocking lists, update lists, standard configuration settings	Include concrete details like suspicious internet addresses, file fingerprints, known software flaws, weak settings and typical attack sequences	Set up blocks and alerts, apply updates quickly, tighten configurations and isolate affected systems when needed

- Predefined grading scales for the impact of a threat can help to calibrate extreme but plausible cyber scenarios against the FMI's risk appetite. These scales are designed to ensure that scenarios are neither arbitrary nor exaggerated in measuring impacts such as data integrity, service availability, participant disruption and ecosystem interdependencies.
- Horizon scanning of emerging risks for which no mitigation measures are in place may inform scenario design. Emerging risks may materialise in the medium to long term, ie beyond the time horizon (usually three to five years) where an FMI's budget and resources are generally allocated to mitigate the already identified risks. For example, an FMI may consider the following questions:

– Considering the FMI's nature and scale of operations, which prospective risks (in the financial sector and beyond it) pose the most significant threats to its core functions in the next three to five years?

– Have these risks materialised in other sectors and how are they being addressed there?

– How can these risks be incorporated in the FMI's CRF to effectively mitigate their impacts before an incident/outage?

2.2.3 Identify key influences and critical uncertainties

With the cyber landscape constantly evolving, the following considerations can help to ensure scenario development is informed by an FMI's current environment and possible future threats:

- Analyse vulnerabilities and critical assets: Identify assets that are most critical to the FMI's operations and mission (see section 3.2). Assess the attack surface, level and effectiveness of controls, vulnerabilities and exposure of these assets. In particular, identify weaknesses in their processes, systems, networks and applications, including any interdependencies that critical operations and core business lines may have, eg third parties. This may be done in various ways, including through modelling/simulation, continuous monitoring and the use of AI tools.
- Use threat intelligence: This can help an FMI to understand emerging threats, attackers' motives and capabilities, trends in recent events and the evolution of TTPs.
- Brainstorm: Consider external and internal factors that may influence the FMI's future (eg its exposure to changed or new cyber threats) or have an impact on critical operations of the FMI

and its ecosystem. These factors include political, economic, social, technological, environmental, legal and other factors.[19]

- Identify trends and uncertainties: Monitor consistent patterns of change as well as factors that may have unintentional consequences or open new attack paths.

Box 2

Considerations for identifying risks arising from an FMI's ecosystem

The following are additional considerations for identifying risks arising in the FMI's ecosystem when developing a cyber resilience strategy and framework:

- End-to-end mapping for the identification of business functions and processes: Map dependencies for all critical operations and services in an FMI's ecosystem to obtain an ecosystem-wide view. Conduct business impact analyses and risk assessments that consider disruptions originating from the ecosystem.
- Identification of information assets and related access: Develop network diagrams that illustrate interconnections between internal systems and external ecosystem entities to enable visibility into how information and processes flow between internal systems and the broader ecosystem.
- Risk and impact analysis: Conduct business impact analyses to assess the potential impact of disruptions on critical operations and cyber risk assessments that explicitly consider disruptions originating in the ecosystem (eg supply chain, shared technologies). Prioritise analysis for ecosystem entities that support critical services and operations.
- Cyber threat intelligence: Establish a process to gather and analyse cyber threat information from internal and external sources, including the ecosystem. Use this intelligence to anticipate and mitigate potential threats.

2.2.4 Scenario development

Based on the scenario inputs and key influences and uncertainties, the following approaches can be used to develop scenarios that will assess an FMI's resilience and the effectiveness of its processes and technical capabilities:

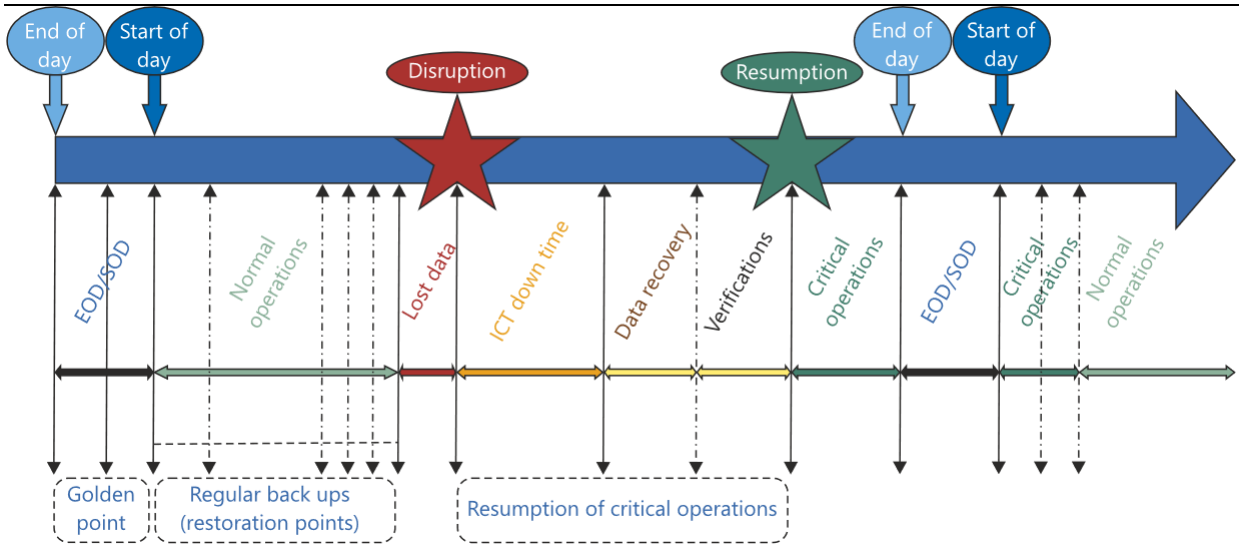
- Create diverse "what-if" scenarios: Develop a range of scenarios that encompass various threat levels, complexities and potential impacts on assets and operations (see Annex 2A for examples).
- Consider including complexity add-ons in existing scenarios to ensure that they consider both the FMI's role in the financial system and the growing severity and complexity of cyber attacks (see Box 3).
- Ensure realism and relevance: Tailor the scenarios to the FMI's unique environment and the specific threats it is most likely to face, as well as to the chain of events that may lead to a specific extreme event or impact. Designing credible and realistic scenarios helps to develop an accurate understanding of resilience against real-world threats. This includes determining, when defining the scenario, what constitutes a failure for the relevant controls. Engaging with ecosystem entities in building extreme but plausible scenarios, for example through an industry-wide effort, can help an FMI ensure its scenarios are as realistic as possible.

[19] The UK PESTLE framework may be a useful starting point for identifying influences and uncertainties. See Chartered Institute of Personal Development, "PESTLE analysis", 6 December 2021, www.cipd.org/globalassets/media/knowledge/knowledge-hub/factsheets/pestle-analysis-factsheet_20221230T092611.pdf.

- Develop detailed narratives, or a timeline, that describe the sequence of events (see Figure 2 for an example), the attacker's actions, the initial impact on systems and operations and, to the extent possible, some key aspects of the ensuing consequences (eg financial loss, legal repercussions).

Stylised timeline of cyber related outage

Figure 2



Source: CPMI.

- Leverage available scenario development frameworks: Using frameworks available in the financial sector, or in other sectors, may help to inform FMIs on how to develop and structure their scenarios. Referencing available frameworks can also provide a common language and understanding of adversary behaviours (see Annex 2B).
- Consider incorporating or generating a scenario library: Using a scenario library may aid an FMI in learning and developing through continuous benchmarking of its cyber resilience framework and strategy.

Box 3

Complexity add-ons

Implementing complex scenarios

Business continuity management processes and arrangements, included in an FMI's cyber resilience framework (CRF), are designed to allow the FMI to respond to and recover from most cyber or operational incidents (even in the case of extreme but plausible scenarios) with regularly tested and exercised incident response, crisis management and recovery capabilities. Therefore, under sufficiently complex scenarios, scenario testing will likely involve coordinated responses from multiple management, business and technical areas, as well as third parties.[20]

Realistic evaluation of the extent and duration of processes to respond to and recover from complex scenarios, especially integrity breaches, may require consideration of and planning for the following: stopping services, performing technical and verification steps to check the availability and integrity of backup copies, coordinating and communicating with all relevant parties, deciding on the best-suited recovery strategy, reconciling business context (eg by reclaiming missing transactions), reconnecting ecosystem entities and safely resuming operations.

Incorporating more complexity into scenarios

There are a variety of ways to incorporate more complexity into cyber scenarios:

- Simulate responding to coordinated or simultaneous attack vectors, including vectors designed to distract responders, affecting critical operations and/or multiple business lines, challenging incident management, governance and communication processes to key internal and external stakeholders.
- Consider an event that affects the technical aspects of an FMI's operations, including the extended use of alternative sites, contingency solutions such as non-similar facilities, or the use of non-standard procedures.
- Consider possible combinations of tactics, techniques and procedures that may be exploited by a threat actor, rather than just one.
- Assume the failure of multiple levels of control.
- Consider the timing of the disruption that would present the most challenges (eg close to the time of completion of settlement, when settlement funds are moving between participants or another critical deadline or cut-off).
- Consider that most severe scenarios may not be limited to the impact on the primary site/facility hosting the FMI's ICT resources, but may extend to multiple or all sites due to a threat element (eg

[20] Examples of structured approaches an FMI may use when designing extreme but plausible scenarios are available from ISO/IEC 27005:2022(E), EBIOS RM or the FAIR Institute in its guide to defining and refining cyber risk scenarios, ensuring that they accurately represent probable loss events. See Annex 2B.

an advanced persistent threat, supply chain attack or zero-day exploit[21]) which needs to be contained and eradicated across sites.

- Consider the emerging dimension of information warfare as part of geopolitical tensions or nation- or state-level open conflict. These may take the form of sophisticated cyber operations strategically deployed alongside disinformation campaigns aimed at undermining financial stability; eroding public trust; or disrupting, damaging or stealing from adversary nations' critical infrastructure to achieve geopolitical objectives.
  - Consider disinformation and influence operations, including deliberate manipulation of market-sensitive information, false financial narratives and strategically timed attacks coinciding with critical geopolitical developments.
- Consider hybrid threat scenarios. Examples include: (i) where compromised communication channels spread misleading information concurrent with system attacks; and (ii) where manipulated market data are released during an ongoing cyber or operational incident to trigger panic-driven financial decisions. Global tensions create environments where such coordinated campaigns targeting multiple financial institutions simultaneously become increasingly plausible.
- Consider simultaneous events, including tail risks, for example, a cyber attack coinciding with large-scale market stress or outages in key sectors (eg energy or telecommunications), affecting or limiting an FMI's ability to respond.
- Consider the possibility that the two-hour resumption objective cannot be achieved. In planning for such scenarios (especially if there is no guarantee that operations can be resumed safely), consider the use of specific non-standardised procedures to ensure completion of settlement by the end of the day and thus postpone the safe resumption of operations to the next business day (see section 3.3.4).
  - Consider that resumption of an FMI's critical operations within two hours after a disruptive cyber or operational incident would likely be conditional on the integrity of data.
- Consider the FMI's larger ecosystem (eg supply chain, other participants in the domestic and global financial system) including nth parties in the FMI's supply chain (see Box 2).
- Consider whether there are critical third parties and/or systems the FMI relies on that operate in a different time zone to the FMI and how this could affect recovery.

2.3 Considerations for testing and updating extreme but plausible scenarios

Processes to plan, test, analyse and update scenarios as well as to communicate details about them with relevant stakeholders can improve their realism, effectiveness and alignment with the evolving threat landscape. The following are practical considerations with respect to these processes.

Plan, test, analyse and update scenarios

- Perform an impact assessment: Analyse the implications of each scenario that the FMI developed, including potential risks and opportunities. Identify potential risk transmission channels, concentrations and vulnerabilities within critical operations and core business lines considering third-party risks.

[21] A zero-day exploit is a cyber attack that targets an unknown vulnerability in software, hardware or firmware. Developers have no prior knowledge of the flaw, leaving no time to create patches, making such exploits highly dangerous and systems vulnerable.

- Plan detailed responses: Outline the key elements of the plan the FMI would follow in response to each scenario, including incident management, governance and communication protocols. This can also include assigning clear roles and responsibilities to key internal and external stakeholders to ensure a coordinated response.
- Back-test scenarios: Validate scenarios by comparing them with past cyber or operational incidents at the FMI or significant incidents outside the FMI's context. Back-testing results can be used to refine scenarios and increase their realism and effectiveness.
- Conduct proactive tests and simulations (see section 4): Test existing strategies and response, resumption and recovery plans at regular intervals (eg annually or after significant changes to the FMI's infrastructure or threat landscape) against the developed scenarios to assess resilience and identify vulnerability gaps (eg tabletop exercises). Continually update scenarios and response plans to address new and emerging threats.
- Learn and adapt: Conduct root cause analysis and document lessons learned and gaps identified in the FMI's response, resumption and recovery through the tested scenarios. Use the insights gained from tests and exercises to refine response strategies and measures enhancing cyber security controls and recovery from cyber or operational incidents.

Communication and scenario application

- Share findings with stakeholders: Present the scenarios and their implications to relevant decision-makers and stakeholders. Proceed with care and exchange sensitive information only in trusted circles, eg among personnel knowledgeable in cyber risk designated by the FMI and its ecosystem entities.
- Review and update scenarios: As the threat landscape is constantly evolving, regular review and revision of scenarios to reflect new threats and vulnerabilities and the evolution of the FMI's broader context can help maintain the FMI's level of preparedness. For example, an FMI may be affected by regulatory, technological, business, environmental and geopolitical developments.

Annex 2A: Extreme but plausible scenarios – stylised examples

1. Cyber attack on a systemic central counterparty and securities settlement system /central securities depository

   Timing: Weekday, midday (not Friday).

   Threat: The attackers, a highly skilled group of cyber criminals, launched a multifaceted assault on the FMI. They began with a phishing campaign, sending meticulously crafted emails to employees, containing deepfake videos that impersonated senior executives. Simultaneously, the attackers targeted third-party service providers and market participants, exploiting vulnerabilities in their systems through supply chain attacks. While confirmation is needed, there is a suspicion that a critical subcontractor's service for which there is no substitute was compromised during a system update by a malicious insider who potentially installed the malware. Malware was deployed, infiltrating the FMI's network and gaining access to critical transaction records.

   Disruption: Settlement processes were disrupted with delays and erroneous settlements affecting market participants.

   Impacts: The attack led to significant data corruption, making it impossible for the FMI to resume operations within two hours. This resulted in transaction failures and incorrect intraday margin calculations, further exacerbating the market turmoil. Completion of settlement by the end of the day was at risk. The FMI had to consider using alternative arrangements for multiple critical operations/business lines.

2. Insider-enabled disruption of end of day (EOD) settlement

   Timing: EOD, on a high-volume settlement day.

   Threat: A privileged insider disables or corrupts reconciliation scripts/logic used to validate EOD settlement. Changes are hidden through log manipulation.

   Disruption: Settlement processes were disrupted with delays and erroneous settlements affecting market participants. The FMI cannot validate settlement results, and discrepancies appear across participants. No reliable audit trail is available.

   Impacts: The FMI cannot confirm that its records are accurate or can be trusted, and regulators require proof of data integrity before resumption. To achieve completion of settlement by the end of the day, the FMI may use non-standard procedures and conduct reconciliation of its records.

3. Malicious manipulation of settlement priority rules

   Timing: Overnight, discovered during EOD or start of day (SOD); midday, when settlement sequencing anomalies appear.

   Threat: An attacker alters static configuration files that control settlement sequencing, priority queues and liquidity optimisation algorithms.

   Disruption: Settlement sequencing becomes incorrect and the manipulation is discovered when EOD settlement produces unexpected liquidity shortfalls. Participants dispute the settlement order.

   Impacts: EOD settlement may fail and the FMI may halt the batch, and the recovery point objective rollback would then invalidate the day's settlement queue. Participants dispute the correct settlement order.

4. Ransomware encrypting production and backups

   Timing: Start of EOD batch, when systems are most vulnerable or overnight, discovered during SOD startup.

Threat: Time-triggered ransomware payload encrypts production systems and nearline backup and attempts to spread to a secondary site.

Disruption: Core clearing and settlement engines freeze and backups are unavailable. Only offline backups remain.

Impact: Breach of resumption time objective – the resumption time approaches EOD settlement time and manual fallback procedures are required. Participants face uncertainty about exposures as a multi-day outage is inevitable.

5. Cryptographic compromise hardware security module (HSM)/public key infrastructure (PKI)

   Timing: Intraday, during high-volume clearing or overnight, discovered during SOD authentication checks.

   Threat: Zero-day vulnerability in HSM or certificate authority is exploited. Digital signatures become unreliable and authentication tokens can be forged.

   Disruption: Participants cannot verify authenticity of messages and FMI cannot trust inbound settlement instructions. All digital signing operations are halted.

   Impact: Clearing and settlement may be suspended as contingency authentication channels are required and participants attest to system integrity. There is high risk of fraudulent instruction and reconnection is delayed until trust is restored.

Ecosystem-specific scenario examples

6. Systemically important financial institution is targeted by cyber criminals

   Timing: Any time during daily operation schedule.

   Threat: Initial investigation results confirm the cyber security incident. The FMI's regulator and relevant authorities are notified.

   Disruption: A major bank is the target of a distributed denial of service attack. The affected bank is the largest participant in terms of market share of transaction values in the large-value payment system and stops the submission of outgoing payments for four hours in the afternoon.

   Impact: Other banks stop outgoing payments to the affected bank two hours before the closing time. Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances.

7. Critical service provider (CSP) to financial sector experiences an outage due to a cyber attack

   Timing: Any time during daily operation schedule.

   Threat: A CSP is the target of an attack exploiting an application server.

   Disruption: The affected CSP provides data processing and information systems management services to the five largest banks, including its core banking activities.

   Impact: The CSP data breach affects the confidentiality and integrity of payment instructions. The five largest banks are unable to submit payment instructions for four hours in the afternoon before the closing time. Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances.

Annex 2B Scenario resources

The following resources may help FMIs develop extreme but plausible scenarios.

- Bank for International Settlements (BIS) – cyber resilience papers. The BIS publishes thematic papers on cyber risk, operational resilience and systemic risk propagation which can be useful for cross-border contagion and multi-FMI scenario design.
- Financial Services Information Sharing and Analysis Center (FS-ISAC).
- Financial Stability Board (FSB) – cyber incident reporting and systemic risk. The FSB's work on cyber incident reporting harmonisation helps shape realistic scenario triggers and escalation pathways. Its systemic risk analyses inform cross-FMI contagion scenarios.
- National computer emergency response teams (CERTs) and cyber security centres such as the Cybersecurity & Infrastructure Security Agency (CISA) in the United States, ENISA in Europe or BSI (Federal Office for Information Security) in Germany.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework and SP 800-Series: This is a widely used framework for improving cyber security risk management in critical infrastructure, eg threat modelling, control expectations and scenario realism. NIST SP 800 34 (contingency planning) and SP 800 61 (incident response) are especially relevant.

Other sources and publications

- Agence nationale de la sécurité des systèmes d'information (ANSSI) (2018): *EBIOS Risk Manager*.
- Bank of England (2024): *CBEST threat intelligence-led assessments: implementation guide for CBEST participants*.
- Cross Market Operational Resilience Group (CMORG) (2025): *Dynamic scenario library*.
- ——— (2025): *Guidance for firm operational resilience, version 3*.
- ENISA (2025): *ENISA threat landscape 2025*.
- European Central Bank (ECB) (2018): *Cyber resilience oversight expectations for financial market infrastructures*.
- FAIR Institute (2025): *A FAIR taxonomy for cyber risk scenarios*.
- Financial and Banking Information Infrastructure Committee (FBIIC) (2017): *Financial sector cyber exercise template*.
- G7 Cyber Expert Group (CEG) (2016): *G7 fundamental elements of cybersecurity for the financial sector*.
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2022): *Information security, cybersecurity and privacy protection – guidance on managing information security risks*, ISO/IEC 27005:2022.
- MITRE (2026): *ATT&CK Matrix for Enterprise*.
- Securities Industry and Financial Markets Association (SIFMA) (2025): *Quantum Dawn Cybersecurity Exercises*.

3 Developing response, resumption and recovery plans

3.1 Introduction

This tool is designed to support FMIs in developing response, resumption and recovery plans by providing practical considerations for FMIs in three key areas: (i) identification and prioritisation of critical operations and assets; (ii) capabilities to support response, resumption and recovery plans; and (iii) criteria for identifying conditions for safe resumption of operations, including when to disconnect from and reconnect to ecosystem entities.

Annex 3A provides further information on standard industry metrics used for measuring business continuity. References for disconnection and reconnection processes are listed in Annex 3B. A reference questionnaire is provided in Annex 3C to help FMIs assess their response, resumption and recovery plans and capacity to resume critical operations within two hours of major operational or cyber incidents.

3.2 Identifying critical operations and information assets

Identifying the operational features and key design elements that enable an FMI to achieve resumption of critical operations within two hours in the case of a major disruption, operational failure or cyber incident is critical to increasing the cyber resilience of an FMI and its ecosystem. Table 4 provides practical considerations for identifying information assets and related processes that are essential to facilitate the safe resumption of an FMI's critical operations.[22]

Identifying assets for the safe resumption of critical operations — Table 4

	Practical considerations
Identification and documentation of critical assets	• Define and implement a process to identify and document all critical operations, critical systems, critical functions, key roles, upstream and downstream dependencies, business processes and information assets that support those functions. • Identify and document dependencies on third-party service providers, interconnections and external systems, and ensure this information is regularly updated.
Inventory management	• Maintain a current, up-to-date and centrally managed inventory of: - critical operations, critical systems, critical functions, key roles, business processes and information assets; - third-party service providers, interconnections and dependencies; and - system configurations, individual accounts and system accounts (including privileged and remote access accounts). • Update the inventory regularly and when changes occur (eg new, relocated, repurposed, depreciated or retired assets). • Integrate inventory management with acquisition, change management and other relevant processes to ensure accuracy and completeness.
Network diagrams	• Develop and maintain comprehensive and current physical and logical network diagrams, which include:

[22] See Bank of Canada, *Expectations for cyber resilience of financial market infrastructures*, 2021, www.bankofcanada.ca/wp-content/uploads/2021/10/expectations-cyber-resilience-financial-market-infrastructures.pdf; European Central Bank, *Cyber resilience oversight expectations for financial market infrastructures*, 2018, www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf; and Monetary Authority of Singapore (MAS), "Notice on technology risk management", FSM-N21, 2024, www.mas.gov.sg/regulation/notices/notice-fsm-n21; and MAS, *Technology risk management guidelines,* 2021, www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines.

	- network resources, IP addresses and subnets:
	  - connected components and routing/security devices; and
	  - links to internal and external services, including interconnections with stakeholders, internet-facing services, cloud services and other third-party systems.
	• Use network diagrams to assess risks and implement appropriate controls.
	• Ensure access to network diagrams is closely controlled.
	• Create and maintain a simplified network map specifically for critical functions, including routing and security devices, servers and links to external systems.

Integration with other processes	• Align identification and risk management efforts with other processes, such as acquisition, change management and system development or renewal, to ensure a holistic approach to cyber resilience.

3.3 Key response, resumption and recovery capabilities

This section provides practical considerations for an FMI when designing, developing and implementing capabilities that its response, resumption and recovery plans may leverage when responding to an incident. These capabilities include and expand on the techniques detailed in the 2014 CPMI report *Cyber resilience in financial market infrastructures* (2014 cyber report).

Capabilities are grouped into four subsections: (i) ICT infrastructure design; (ii) data resilience; (iii) application resilience; and (iv) processes and procedures for handling incidents and crises. Each capability is intended to be technology neutral and applicable to a wide range of FMIs; however, other capabilities may be appropriate depending on an FMI's specific needs. In addition to these capabilities, any contractual or operational arrangements the FMI makes to facilitate its response, resumption and recovery plans may need to be agreed upon in advance with internal and external stakeholders.

Because the techniques below may affect the services that the FMI provides to its participants, such as when and how it provides these services, including the impact of the use of these techniques in the FMI's rulebook and contractual arrangements can help to mitigate the risk of litigation and provide transparency that will help participants and other relevant stakeholders manage related risks.

3.3.1 ICT infrastructure design

As set out in the 2014 cyber report, resumption of operations to a "normal" or "good enough" processing state is a key element of recovery. Under certain extreme but plausible scenarios, simply resuming operations, even if resumption occurs swiftly, may not be appropriate. For example, an FMI that simply resumes operations within two hours following a cyber attack may be resuming them to the same vulnerable state in which the attack occurred. Therefore, additional capabilities, as detailed below, may materially increase an FMI's ability to identify, protect, detect, respond to and recover from such scenarios in a safe state.

Adopting infrastructure as code

Infrastructure as code (IaC),[23] a method for managing infrastructure using machine-readable code instead of manual configuration, may enable an FMI's teams to automate the provision, configuration and management of servers, networks, databases and other resources, to ensure consistency, repeatability and scalability across environments. IaC may help an FMI to recover its ICT systems by

[23] IaC is an approach to managing ICT infrastructure through machine-readable configuration files, rather than manual processes or interactive tools. It represents an effective and auditable method to implement key security principles, such as controlled change management and traceability, to increase operational resilience.

limiting its reliance on otherwise manual and possibly error-prone processes for recovery to ensure safe resumption of critical operations.

By adopting IaC, FMIs may achieve higher operational resilience, faster incident response and improved compliance, while reducing costs and manual overhead. Key benefits for operational resilience include:

- Automation and consistency: IaC can eliminate manual errors and ensure that infrastructure is deployed and managed uniformly, reducing configuration drift and human-caused outages.
- Disaster recovery: Infrastructure can be quickly rebuilt or restored from version-controlled code, significantly reducing recovery time in the event of failures or disasters.
- Immutable infrastructure: IaC can encourage the replacement of resources rather than in-place changes, minimising the risk of configuration errors and improving system stability.
- Version control and auditability: All infrastructure changes can be tracked, documented and reversed, enabling transparency, compliance and rapid rollback if needed.
- Scalability and elasticity: IaC can allow for dynamic scaling of resources in response to demand or failure, ensuring continuous availability and performance.
- Continuous integration/continuous delivery (CI/CD):[24] IaC can be seamlessly automated through CI/CD pipelines that enable automated testing and deployment of infrastructure changes as code as well as application code, further enhancing reliability.

Layered architectures and recovering operations

Network architectures with layered defences seek to reduce the opportunity for a threat actor to move laterally from an ecosystem entity's systems to or within an FMI's systems. This is accomplished through the segmentation of an FMI's architecture and network into logical zones with carefully controlled boundaries between these zones. Layered architectures are especially relevant for firms that have connected formerly isolated critical infrastructure systems to internal and external networks to meet business objectives.[25]

The effective implementation of a layered architecture may include the use of one or more "demilitarised zones" (DMZs) to control the type of traffic that is forwarded to the FMI's more secure zones.[26] The use of virtual local area networks (VLANs) may allow for further segmentation of a physical network.[27] These network layers should utilise an access management system to perform multifactor authentication on the basis of user roles and least privileges. Together, DMZs and VLANs should allow for the immediate segmentation or isolation of external connections to prevent contagion or lateral movement following an attack. A layered architecture benefits from automated stop/start capabilities to

[24] See section 4.4.3 for further information.

[25] Layered architecture, also known as multi-tier architecture, is a structured approach that separates layers of operations from others, so that the functioning, or not functioning, of one will not affect the others. Layered architecture is an effective approach and industry best practice to ensuring clear separation of responsibilities, maintainability and operational resilience.

[26] NIST defines a DMZ as a "Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks." Demilitarized zone (DMZ) - Glossary | CSRC (Computer Security Resource Center).

[27] NIST defines a VLAN as "A broadcast domain that is partitioned and isolated within a network at the data link layer. A single physical local area network (LAN) can be logically partitioned into multiple, independent VLANs; a group of devices on one or more physical LANs can be configured to communicate within the same VLAN, as if they were attached to the same physical LAN." Virtual Local Area Network - Glossary | CSRC.

halt compromised services and communications preventing further contagion, which may also facilitate thorough analysis of an incident and corrective action.

The use of DMZs and VLANs does not come without risks. For example, should a computer in the DMZ become compromised, a threat actor could use that device to pivot to other connected devices, posing risks to an FMI's critical systems.[28] Network segmentation solutions should therefore be carefully structured with consideration of the benefits and drawbacks of a layered architecture.

Layered architectures can be further strengthened using enhanced authentication for critical systems, non-similar facilities or their equivalents as well as specific security requirements for vendor integrations governing connectivity, access control and vulnerability management.

Adopting a layered architecture can limit the scope of the impact of a cyber event, potentially allowing for partial resumption of services while still remediating any system components that have been compromised. For example, if an FMI cannot achieve intraday recovery of its critical components, it may consider extending operating hours with consideration of linked FMIs and other interdependencies. This allows FMIs to meet completion of settlement by the end of the day through non-standard procedures (see section 3.3.4), provided the FMI's participants are available to process transactions and the operations layer can be recovered.

To conduct monitoring within a layered architecture, the use of multi-layered detection controls may identify and disrupt potential threats to the FMI's ecosystem. This can be accomplished using a combination of multiple threat detection capabilities such as host-based and network-based intrusion detection systems (IDS). These systems may be further supplemented using an intrusion protection system (IPS) to monitor the FMI's network for malicious activity. The most robust monitoring solutions likely use multiple IDS and an IPS in tandem.[29]

Designing and utilising a non-similar facility or its equivalents

The use of a non-similar facility (NSF)[30] or its equivalents can provide additional infrastructure resilience and support an FMI's response, resumption and recovery plans. In the case of a cyber or operational incident that impacts the primary facility, an FMI can resume operations using the NSF (assuming it is not affected by the same incident).

However, it is important to note that while an NSF may allow for the FMI's critical operations to continue, it may not provide the full functionality of an FMI's primary facility and should not be fully relied on for handling non-critical operations. True non-similarity can be considered at both the operational level (ie processes, procedures and geographic separation) and the infrastructure level (ie network architecture, network resolution services, hardware, software and vendor diversity).

In practice, an NSF serves as a backup for the primary facility to facilitate resumption of operations in the event of a cyber or operational incident that causes data corruption. This involves the FMI using the NSF to run services independently of the FMI's primary facility, thus allowing them to remain uncorrupted. Achieving this independence requires careful consideration of the underlying network infrastructure that connects participants to both facilities.

[28] See CISA, *Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies*, 2016; and NIST "Guidelines on firewalls and firewall policy", *NIST Special Publications*, no 800-41, revision 1, 2009, for more information on network segmentation best practices.

[29] See NIST, "Intrusion detection and prevention systems" for more information on IDS and IPS implementation.

[30] The 2014 cyber report defines an NSF as a facility that "replicates the core functionality of an FMI but using technology different from that used by the primary facility".

Infrastructure-level non-similarity is essential to prevent failures that could compromise both the primary facility and NSF simultaneously. Non-similarity of network resolution infrastructure, such as the domain name system (DNS),[31] which directs how participants' systems locate and connect to an FMI's services, may be especially beneficial. Rather than merely maintaining backup DNS servers, FMIs may increase their resilience by implementing redundancy at multiple layers of the resolution process.[32] This includes ensuring redundant infrastructure exists at both ends of the resolution chain – where queries are initially processed and where destination information is ultimately provided. Additionally, by utilising multiple DNS service providers FMIs can avoid concentrated dependencies on a single vendor or service. Implementing failover redundancy for network switching devices that support DNS resolution capabilities further strengthens this approach. This multi-layered diversity helps to mitigate cascading failures and eliminates single points of failure that could simultaneously affect both the primary facility and NSF.

Vendor and platform diversity across architectural layers further strengthens NSF independence. Additionally, diversity may be incorporated at equivalent architectural levels (ie similar tiers of the technology stack), such as deploying different operating systems or hardware vendors at critical access points and throughout the operational layers. This approach addresses supply chain risks where exploited vulnerabilities within a single piece of software or hardware could have widespread effects across both primary and non-similar facilities.

Using an NSF may require an independent communication channel between the FMI and its ecosystem entities. For example, ecosystem entities may send their data directly and separately to the FMI through the FMI's primary facility and its NSF. Unidirectional network devices (ie data diodes or unidirectional security gateways) can ensure that data transmitted to the NSF remain independent and protected from potential corruption or intrusion originating from the primary facility's network. These devices allow data to travel in only one direction, physically preventing communications access from lower criticality networks to higher criticality NSF networks. This physical traffic flow control maintains protection even if both networks are compromised.[33] In this way, each facility may serve as a basis for fixing-backward. Using an NSF may also provide a way for the FMI to fix-forward; an example is a cold site[34] that starts processing from a defined point onwards.

Despite some obvious benefits, there may be drawbacks to leveraging an NSF. Depending on their design, the use of an NSF can incur increased operational complexity and cost to an FMI, which may in turn undermine the very resilience it is designed to achieve. Infrastructure-level diversity introduces additional complexity in configuration management, quality assurance processes across heterogeneous systems and the testing of interactions between diverse systems within the FMI's environment. An NSF may also introduce its own vulnerabilities and therefore should be employed cautiously, as part of a balanced strategy to help preserve the resilience of an FMI's operations.

[31] The NIST Glossary defines DNS as "The system by which Internet domain names and addresses are tracked and regulated" (https://csrc.nist.gov/glossary/term/domain_name_system_DNS).

[32] Multi-layered DNS redundancy involves ensuring that redundant infrastructure exists at each critical point in the resolution chain: recursive resolvers (where queries are initially processed and cached) and authoritative name servers (where definitive destination responses originate). This is distinct from simply having a secondary DNS site, as it addresses redundancy throughout the resolution process itself. For additional guidance, see CISA's DNS Risk Assessment report on implementing resolution redundancy.

[33] See CISA (2016) for more information on unidirectional network devices.

[34] A cold site is a basic backup facility with limited infrastructure. It is not ready to operate immediately and requires significant setup (eg installing software updates, configuring systems and restoring data) before it can take over operations.

3.3.2 Data resilience

Reconciliation and use of an uncorrupted "golden point"

An FMI's ability to resume its critical operations within two hours after a disruptive cyber or operational incident would likely be conditional on the integrity of data. Extreme but plausible cyber scenarios may involve an integrity breach (ie causing data corruption) or data loss. In these scenarios, comprehensive and possibly time-consuming processes for data reconciliation are required before safe resumption of an FMI's critical operations.

In the event of a data integrity breach, an important step towards recovery is to identify and define when the breach took place and whether the ICT environment, data or applications have been corrupted in any way. This knowledge is critical in determining an uncorrupted "golden point" (also referred to as a "golden copy"), from which affected ICT environment components, data and applications can be restored to the state they were in prior to the attacker's presence.[35]

Effective processes may involve capturing transaction and position data in near real time and storing them in an "air-gapped" environment to facilitate identifying the golden point.[36] Frequent reconciliation against such records may assist in identifying corrupted or fraudulent transactions, either to detect a cyber intrusion or to help establish the golden point. To that end, establishing standing arrangements with ecosystem entities to reconcile transactions can help an FMI to restore data integrity from the golden point more quickly.

Additionally, to facilitate an effective recovery, a golden point may need to include both data and infrastructure components, including identity, network and storage configurations. This means implementing robust backup solutions for virtual machines, container registries and infrastructure as code components.

To restore data integrity from a golden point an FMI will likely need to engage in a reconciliation process (see Box 4). Depending on the nature and scale of the issue, different recovery and subsequent reconciliation strategies may be designed as part of a flexible response and recovery posture. Some possible recovery strategies include:

- Fix-backward: In case of extensive data corruption, a full recovery based on the golden point may be necessary. Fixing-backward recovery restores the operational environment to the last "trusted" state, ie the state known to be uncompromised. Depending on the extent of corruption, such measures may require thorough data reconciliation to solve data loss in relation to both internal and external systems. This may be facilitated through the use of an event-driven architecture (see section 3.3.3).
- Fix-forward: In case of a limited data corruption or data loss that would not require a full recovery process based on a golden point, corrections may be carried out directly on live data using analytic tools and queries to analyse live data and swiftly remediate integrity. Fix-forward recovery "selects a less than fully trusted point from which to continue operations while seeking to restore trust in those IT environment components that remain corrupted".[37] Fix-forward recoveries may be viable only during more limited data integrity breaches or when a fix-

[35] This definition of golden point is from the 2014 cyber report, section 4.3.3, "Rolling back to the uncorrupted 'golden point'".

[36] NIST defines an air gap as "An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control)" (https://csrc.nist.gov/glossary/term/air_gap).

[37] 2014 cyber report, page 11.

backward strategy is impractical.[38] The viability of fixing-forward may be greatly improved through the use of automated IaC and appropriate use of immutable and ephemeral infrastructure.[39]

A "write-once, read-many" (WORM) storage solution can support golden point identification and recovery, by preventing data modification or overwriting or deletion of records. A WORM solution provides immutable storage through controls integrated directly into the storage system itself. This approach goes beyond traditional access control mechanisms (ie identity and access management (IAM)[40]), which can be compromised during an attack. WORM storage solutions may be structured to support both time-based retention (records retained for a fixed period from creation) and event-based retention (records retained until specific business events occur, such as contract maturity). Additionally, separation between immutable record content and mutable operational metadata is key. For example, immutable components include the actual record data, unique identifiers, version numbers, creation timestamps and integrity checksums, while mutable components include access control lists or retention controls that can be extended but not shortened.[41] Typical features of a WORM storage solution include:

- object-level retention locking mechanisms that prevent any user, including system administrators and root users, from shortening retention periods or deleting protected records;[42]
- automated versioning that prevents overwriting by creating new versions rather than modifying existing records;
- retention controls that specify an immutable "retain until" date; and
- data encryption at rest and support for encryption of data in-transit using checksums.

WORM protects a golden point from destructive modification, but it does not by itself guarantee recoverability or data integrity; therefore, using WORM in tandem with other tools increases resilience.

From an ecosystem-wide resilience perspective, data-sharing agreements with trusted third parties can also play a key role in supporting cyber incident recovery efforts. Such arrangements enable organisations to access reliable and uncorrupted data sources in a timely manner, thereby facilitating the restoration of critical operations and reducing resumption time. These agreements may also strengthen collective resilience by promoting coordinated response mechanisms, improving data availability during crises and mitigating the impact of data corruption.

[38] Per the 2014 cyber report, "Where [fixing-forward] does acquire viability is if failing backward [ie fixing-backward] could not be accomplished in a reasonable time frame. Consequently, the applicability of failing-forward [ie fixing-forward] recovery centres on whether an FMI can afford the downtime required to restore the IT environment supporting its critical operations to a trusted state or whether the FMI should continue to provide critical services in a less than trusted IT environment."

[39] Ephemeral means that the container (see section 3.3.3) can be stopped and destroyed, then rebuilt and replaced with an absolute minimum setup and configuration.

[40] NIST defines IAM as broadly referring "to the administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users" (https://csrc.nist.gov/glossary/term/identity_and_access_management).

[41] NIST defines a checksum as "A value computed on data to detect error or manipulation" (https://csrc.nist.gov/glossary/term/checksum).

[42] A retention lock is a feature used to ensure that critical data cannot be modified or deleted for a specified duration. This may be used to meet legal, regulatory or organisational requirements for data preservation. For example, retention locks may help to ensure that records remain intact and tamper-proof during audits or investigations.

Box 4

Reconciliation for FMIs in the context of cyber resilience

The CPMI Glossary defines the term reconciliation as "a procedure to verify that two sets of records issued by two different entities match".[43]

In the context of a loss of data integrity, reconciliation processes may include:

- Matching records: comparing records of transactions, balances or other data between an FMI and its participants to ensure they are consistent and accurate.
- Record recovery: replay of (lost) transactions and/or rebuild of participants' positions.
- Error detection: identifying and resolving discrepancies or mismatches in data or transaction records.
- Operational integrity: ensuring that the FMI and the entities within its ecosystem have a shared and accurate view of critical data.

Purposes and uses of reconciliation for specific FMI types include:

- Payment systems: reconciliation ensures that payment instructions processed by the FMI match the records of participants and counterparties.
- Central counterparties: reconciliation ensures that trade records, margin requirements and collateral positions are accurate and consistent.
- Central securities depositories and securities settlement systems: reconciliation ensures that securities balances and ownership records are accurate.

Implementing an isolated recovery environment

When conducting reconciliation based on secured backup data (ie golden point), the FMI may need to carry out some checks (such as the verification of completeness or cleanliness of backups) before restoring backup data in the production environment. These checks, if performed in an isolated recovery environment (IRE), a dedicated production-grade environment isolated from production systems and the internet (eg via an isolated VLAN[44]), may provide resilience benefits such as preventing the lateral movement of an attacker or access to trustworthy copies of key systems (eg if compromised authentication systems block administrative access in a primary environment).[45]

Under a data integrity breach (eg a ransomware attack), the IRE can help the ICT team to swiftly carry out checks/queries to validate data and, in some cases, enable a phased restoration per environment rather than a holistic one.

To increase its resilience, an IRE may benefit from:

- WORM storage with a retention lock to prevent an inadvertent or malicious data modification or deletion;

[43] The CPMI Glossary can be accessed at www.bis.org/cpmi/publ/d00b.htm.

[44] A VLAN is a network configuration that allows devices on different physical networks to communicate as if they were on the same local network. It segments a larger network into smaller, isolated sections to improve performance, enhance security and simplify network management.

[45] Lateral movement refers to the techniques that a cyber attacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

- role-based access control (RBAC)[46] to ensure restricted network access; and
- out-of-band management (OOBM)[47] to ensure reliable access for administrators to perform critical tasks, including recovery, reconfiguration and troubleshooting, even if the main network and operating system are compromised.

As part of the response, resumption and recovery process, the IRE may allow the FMI to parallelise activities (ie investigate the root cause of a disruption while working to identify the golden point), thereby improving the overall recovery time. For instance, while the incident response team is analysing and containing the threat, the recovery team may begin restoring critical systems or working on isolated recovery processes. Other non-ICT-related activities may also need to be conducted in parallel by the FMI's dedicated personnel (eg from the compliance or risk departments) to assess the situation and its potential impact and help with decision-making and communication with relevant internal and external stakeholders.

3.3.3 Application resilience

Application-specific resilience capabilities are designed to preserve key functionalities and minimise impacts to operations. Such capabilities may include:

- Continuing operations: In the event of a disruption, the application can continue operating, even with reduced performance (eg during system/network failures). This may be achieved by switching to backup resources or using degraded modes of operation established before the disruption.
- Event-driven architecture: This provides detailed event logging and processing, especially of critical events, at the system level, ensuring consistent traceability and facilitating swift data recovery. This may include maintaining transaction replay capabilities and, in mature implementations, may incorporate the use of event streaming among internal and external systems to allow for continuous reconciliation across critical systems and with ecosystem entities.[48]

– AI use in ICT systems can benefit from logging the following event types to provide visibility into systems: input, output, model version, confidence score, action taken and human overrides.

- Containerisation: This increases an application's isolation and segmentation, provides immutability and minimises dependencies – reducing the application's attack surface and the ability of a threat actor to move laterally through systems.[49]

To implement these capabilities, FMIs may consider mapping dependencies and the flow of data. The mapping would need to be specified: (i) at the application level between the different resources

[46] RBAC is a security mechanism that restricts access to ICT resources (eg files) based on a user's role within an organisation. Instead of granting permissions to individuals, access rights are assigned to roles (eg "analyst") and users are assigned to those roles. This simplifies access management and reduces the risk of unauthorised access.

[47] OOBM is a method of accessing and managing ICT systems and devices through a dedicated, separate communication channel that is independent of the primary network. This is useful for troubleshooting, maintenance, monitoring or recovery in cases where the main network is down or compromised. For example, ICT administrators might use OOBM to remotely fix servers or network devices without relying on the primary network connection.

[48] Event streaming is the capture of real-time data from a system for storage and analytics, which allows applications to work independently and process events asynchronously.

[49] NIST defines a container as "A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container" (https://csrc.nist.gov/glossary/term/container).

of the application itself; (ii) at the system level between applications; and (iii) at the ecosystem level with external systems (eg API, external databases, third-party service providers etc).[50]

Mapping may help design a priority-based recovery strategy whereby the synchronisation of specific parts of the system/application is to be performed first (eg parts of an application such as transactional databases may need to be synchronised before others like user interfaces or non-critical systems).

3.3.4 Operational processes and procedures

Operational processes and procedures form an integral part of an FMI's response, resumption and recovery plans. Effective processes and procedures may help an FMI provide assurance to its ecosystem that it will conduct sound root cause identification and swift implementation of response, resumption and recovery measures.

This section underlines some practical considerations for designing or improving processes and procedures to ensure FMIs have a trusted approach to address cyber and operational incidents. These procedures may affect an FMI's ability to resume operations in two hours and to quantify key benchmarks in the resumption of operations. In such cases, FMIs may benefit from the use of metrics to provide benchmarks for the resumption of operations (see section 1.3.2).

Managing third-party dependencies

Contractual clauses and service level agreements (SLAs) can help manage the risk posed by third-party dependencies by: (i) imposing clear cyber security requirements; (ii) requiring appropriate security controls be applied to the interconnections, interfaces and systems that will support operations; and (iii) enforcing technical safeguards, such as encryption of data, to maintain the confidentiality and integrity of shared information and services. The integration of cyber risk identification efforts into acquisition, change management, architecture and procurement processes may further improve resilience by facilitating regular reviews of critical business processes, information assets and individual and system credentials.

Risk monitoring of third-party dependencies, both contracted and otherwise (ie open source software), can be conducted using a centralised vulnerability management system (see section 4.4.4). In this context, software bills of materials (SBOMs) can provide comprehensive and continuously updated inventories of software components, dependencies and libraries used across critical systems and services. By improving visibility of the software supply chain, SBOMs enable FMIs to rapidly identify whether newly disclosed vulnerabilities affect their environment, including vulnerabilities originating from indirect or downstream dependencies that may otherwise remain unnoticed. SBOMs also support more effective risk assessment and remediation prioritisation by allowing security teams to map vulnerable components to critical business services, operational processes and external providers. This enhances an FMI's ability to assess concentration risks, detect potential systemic exposure to widely used third-party components and coordinate remediation actions in a timely manner. In addition, integrating SBOM data into centralised vulnerability management and threat intelligence platforms can strengthen continuous monitoring capabilities, facilitate incident response and improve overall cyber resilience across the FMI ecosystem.

Additionally, a "zero trust" security model can mitigate the cyber risk posed by a compromised participant or third party to an FMI's systems.[51] Under a zero trust model, governance of internal and external users' and devices' access follows clearly defined least-privilege principles, limiting external

[50] API = application programming interface.

[51] For references to specific zero trust frameworks, see NIST, "Zero trust architecture", *NIST Special Publications*, no 800-27, 2020; and CISA, *Zero trust maturity model*, version 2.0, 2023.

entities' permissions strictly to the minimum necessary to perform their authorised functions and continuously reviewing these permissions to prevent excessive or unnecessary access. The use of a layered architecture helps to implement a zero trust model and reduce the risk posed by third parties.

Pre-authorised emergency procedures

Given that time may be a key constraint in response, resumption and recovery, the establishment of pre-authorised emergency procedures may accelerate an FMI's ability to safely resume operations. These procedures typically provide a clearly defined path for bypassing standard operational constraints during a crisis, enabling rapid access to critical systems, data or internal decision-making roles/bodies. They also provide secure channels for contacting authorities when normal channels are compromised, ineffective or too slow. Procedures for coordination with other operational functions that may be affected, such as risk management, finance and compliance, are critical to avoid unintended consequences.

By formally documenting and regularly testing these procedures, FMIs can verify that all stakeholders understand the conditions under which they may be triggered, who has the authority to do so, what actions are permitted, what the risks and potential consequences of these actions are and how those consequences may be mitigated. This clarity reduces delays caused by uncertainty or administrative bottlenecks, allowing technical and business teams to act decisively and recover essential operations more quickly.

Despite the value of pre-authorised procedures, an effective cyber investigation may still rely on ad hoc tools and queries that facilitate rapid root cause identification and impact analysis. These tools may enable the FMI's teams to access live data and correlate information from multiple sources, providing greater clarity in complex situations.[52]

Non-standard settlement procedures

If an FMI is unable to resume operations by the end of the day, having procedures in place to complete settlement in a non-standardised way can help reduce the impact of the incident on markets. Agreeing to and testing such procedures with ecosystem entities can help increase preparedness for extreme but plausible cyber and operational incidents. For example, an FMI may find it necessary to extend its operating hours to accommodate a delay occurring in the processes of a linked FMI, with the aim of preventing a spillover effect, or it may take other contingency measures, particularly if the linked FMI is experiencing a protracted disruption. The use of non-standardised procedures may also facilitate settlement when an ecosystem entity has been disconnected from the FMI.[53]

Table 5 provides examples of non-standard settlement procedures and practical considerations for tailoring an FMI's approach to meet its specific context and needs. The practicability of each procedure may vary by FMI type.

[52] To preserve data protection, such tools and workarounds need to be deactivated at the end of the investigation or crisis period and must not be used in normal circumstances.

[53] For example, when a participant is disconnected from a CCP during a settlement cycle, it is important to have a way to inform them of potential payment obligations, and have a way for payments to be made, in order to avoid a payment default resulting from operational risk (rather than an inability to pay driven by credit risk).

Examples of non-standard settlement procedures Table 5

Example of procedures	Description	Implementation steps
Coordination with linked FMIs	Adjust operating hours or use contingency processes in collaboration with linked FMIs experiencing disruptions.	• Establish formal coordination agreements. • Conduct joint testing and simulations. • Maintain clear communication channels during disruptions and provide timely information updates.
Alternative communication channels	Use pre-agreed backup channels (eg secure email, phone) for settlement instructions if primary communication networks are unavailable.	• Test alternative channels regularly. • Ensure encryption and authentication.
Rerouting settlement through backup systems	Redirect transactions to a backup system or facility if the primary system is disrupted.	• Maintain up-to-date mirrored backup systems. • Test failover procedures regularly. • Coordinate with participants to ensure connectivity to backup systems. • Verify backup system is unaffected by the disruption.
Prioritisation of critical transactions	Focus on settling high-value or time-critical transactions during disruptions.	• Define criteria for critical transactions.[54] • Communicate prioritisation rules in advance. • Monitor non-critical transactions for later processing.
Semi-manual processing	Switch to semi-manual processing of critical transactions during severe system outages.	• Regularly test manual processes. • Train staff and participants. • Implement security controls to prevent errors or fraud.
Temporary relaxation of settlement requirements	Temporarily relax settlement requirements (eg prefunding) to allow participants to operate despite liquidity constraints.	• Formally agree to and test such measures in advance. • Assess risks of relaxing requirements and implement safeguards. • Clearly communicate temporary changes to participants.
Extending the FMI's operating hours	Temporarily extend the operating hours (if and when feasible) to accommodate delays from linked FMIs and avoid spillover effects.[55]	• Predefine conditions for extensions. • Communicate promptly to participants. • Ensure system and staff readiness for extended operations.

3.4 Conditions and criteria for a safe resumption of critical operations

The following are relevant conditions and criteria for a safe resumption of critical operations after a cyber or operational incident:

- Ability to use alternative providers for the delivery of critical services.
- Involvement of interconnected entities and, if possible, also of national cyber security agencies in resumption operations (eg for coordinated actions, transaction resubmission etc). Sector-

[54] For a CCP, mark-to-market settlement payments are of the highest priority. By contrast, settling certain trades rather than others may be problematic.

[55] This procedure should consider the critical cutoff points of ecosystem entities, eg linked FMIs.

wide collaboration and response is important due to the tight business and technical coupling among FMIs and entities within their ecosystems (see Box 5).

- Prioritisation of the most critical systems. This may require ex ante identification of how, if at all, the operation of those more critical systems can be decoupled from those considered less critical. If it is possible to do so, developing and documenting plans to implement that decoupling on short notice can be helpful.
- Ability to use contingency measures/tools (automated or manual where relevant) to guarantee the availability of at least a subset of the most critical operations, accessible to at least some critical counterparties, during the recovery time frame.[56]
- Complete eradication of the root cause of the cyber incident to avoid any replication of the incident after the restart of the systems. For example, ensure that software vulnerabilities are eradicated eg through a vulnerability and patch management process that is consistently and regularly applied to all critical assets (see Box 7 in section 4).
- Clear and timely communication with the market and all the stakeholders to ensure proper coordination takes place even in crisis situations and to avoid the dissemination of inaccurate information.
- Thorough checks that restored systems are operating as expected and evaluation of the integrity of the restored data.
- Confirmation that there was no cyber contagion to connected providers and other ecosystem entities, including verification by a trusted third party.
- Use of an isolated approach to restart the systems and, if possible, to reconnect the stakeholders after the restoration.
- A streamlined and informed decision-making process where staff in charge of response, resumption and recovery phases receive clear, correct and timely information about the evolution of the problem and relevant root cause analysis.
- Development of pre-defined playbooks on possible scenarios to guide and accelerate the decision-making process.

[56] Under extreme circumstances, it is likely that services will be reduced and prioritisation will occur, taking into account the criticality of operations or the nature of counterparties (eg other FMIs or global systemically important banks for instance). If consistent with security and confidentiality requirements, including plans and procedures and related governance arrangements for extreme circumstances in rulebooks and contractual arrangements can provide legal basis for these actions and transparency to relevant stakeholders to help them manage related risks.

Box 5

Response, resumption and recovery considerations for managing risks arising from an FMI's ecosystem

The following are additional considerations related to managing ecosystem-related risk in support of safely resuming operations as planned by an FMI's cyber resilience strategy and framework:

- Response, resumption and recovery: Develop comprehensive plans that include actions for responding to, resuming and recovering from cyber and operational incidents informed by scenarios that incorporate risks arising from the FMI's ecosystem. For example, plans could include a scenario in which an ecosystem entity that fulfils multiple roles as a participant and settlement bank is compromised. [57] Plans may also integrate enhanced coordination procedures with external stakeholders.
- Contingency planning: Develop playbooks for scenarios where resumption within two hours is not achievable, including coordination with ecosystem entities. Develop contingency plans that address how to achieve resumption objectives and priorities, considering the impact and role of ecosystem entities.
- Interconnections: Coordinate response activities with ecosystem entities to prevent contagion and ensure safe resumption of operations. Define criteria and establish processes and procedures to *safely* isolate or block third-party connections if necessary, reroute critical activities and prevent contagion across ecosystem entities. These processes need to be carefully designed to avoid unintended consequences.
- Integrate ecosystem entities in crisis management: Ensure cyber response aligns with business continuity plans, crisis management and communication protocols across the ecosystem.
- Monitoring: To the extent feasible, implement ongoing monitoring mechanisms across an FMI's ecosystem to identify risks before they materialise. Event-driven architecture can provide effective monitoring by capturing, analysing, correlating and acting on interorganisational data flows such as system logs, API interactions and other external connection activities to identify anomalies, unauthorised behaviours or potential indicators of compromise across interconnected environments.

3.5 Disconnection and reconnection of ecosystem entities

An FMI and its ecosystem entities are tightly interconnected. A cyber incident or other major disruption or operational failure (eg an integrity issue) with an ecosystem entity may be transmitted across the ecosystem, potentially compromising financial stability. Disconnecting a compromised ecosystem entity can prevent contagion to other members of the ecosystem. However, disconnecting an ecosystem entity can also have implications for an FMI and the markets it serves. Therefore, having a framework to guide the disconnection and reconnection of a compromised entity can help to both prevent contagion and mitigate negative impacts.[58]

[57] See also Box 2 and Annex 2A.

[58] A useful reference for establishing such a framework is G7 Cyber Expert Group, "Reconnection framework best practice", 2025, https://home.treasury.gov/system/files/216/G7-CEG-Reconnection-Framework-Best-Practice.pdfis. Industry standards, such as the Securities Industry and Financial Markets Association (SIFMA), *Financial Services Sector Reconnection Framework*, 2025, www.sifma.org/wp-content/uploads/2025/12/SIFMA-FSSCC-Reconnection-Framework-December-2025.pdf, are intended to support and inform a technical view of reconnection. See also Annex 3B.

There are several situations in which an FMI (or an ecosystem entity) may choose to execute a disconnection (and then a reconnection) to limit potential or actual impacts on its operations (or its ecosystem) resulting from a cyber incident or integrity issue:

- An FMI may disconnect (then reconnect) an ecosystem entity.
- An FMI may disconnect (then reconnect) multiple ecosystem entities (group disconnection).
- An FMI may disconnect itself from its ecosystem (then reconnect itself).
- An ecosystem entity may initiate its own disconnection from an FMI or FMIs – but the FMI would likely have to approve the ecosystem entity's eventual reconnection.

3.5.1 Disconnection of affected ecosystem entities

Departments beyond ICT operations (eg financial risk management and treasury management) may face financial and operational impacts if an FMI disconnects ecosystem entities. Internal governance processes for a decision to perform a disconnection and ex ante internal coordination within the FMI can help to identify and address the range of practical consequences of a disconnection.

Including clear criteria and processes in their rulebooks (with respect to participants) or service agreements/contracts (with respect to other ecosystem entities) for how and under what circumstances an ecosystem entity may be subject to disconnection (or may initiate its own disconnection) from the FMI's ICT systems can help to facilitate an orderly disconnection. Such criteria/processes for disconnecting an ecosystem entity may include the following:

- Objective disconnection criteria: specific criteria for when an ecosystem entity may be disconnected from the FMI (eg cyber threats, technical failures, financial or compliance issues), including what specific operational, financial or compliance issues trigger disconnection.[59] The use of and compliance with objective criteria for disconnection (and later reconnection) may also be useful in mitigating legal risk.
- Governance and decision-making processes: transparent and documented processes that are disclosed to ecosystem entities. These help to determine when to disconnect an ecosystem entity and provide clarity to stakeholders on how the decision is communicated (both internally and to the affected ecosystem entity) and executed.
- Terms of service: clear rules for ecosystem entities regarding when and why disconnection occurs, and the nature of the relationship between the FMI and the ecosystem entity during a period of disconnection. These may include the establishment of additional processes to enable a disconnected ecosystem entity to perform its obligations to the FMI.
- Group disconnection: criteria and processes under which the FMI will disconnect multiple ecosystem entities or all of its ecosystem entities.
- Entity-initiated disconnection: criteria and processes under which an ecosystem entity may initiate its own disconnection, including advance notification requirements to the FMI and other relevant parties in the ecosystem.

In cases where an FMI itself experiences a disruption to its critical operations or services due to a cyber or operational incident, it may choose to disconnect itself from its ecosystem to protect other ecosystem entities. Not all disruptions will result in a wholesale disconnection of ecosystem entities from the FMI's operations or services. There may be cases where the FMI's critical operations or services become temporarily unavailable while the underlying communication infrastructure remains operational.

[59] Such criteria include broader financial stability concerns alongside technical, financial and/or compliance issues.

3.5.2 Reconnection of ecosystem entities

Clear criteria and processes for reconnection of all or some portion of the disconnected ecosystem entities can help the FMI be confident that the cyber or operational incident with the ecosystem entities is resolved and that reconnection may occur without putting the FMI ecosystem at risk. Such criteria and processes may include:

- Objective criteria for when an ecosystem entity may be reconnected to the FMI.
- Transparent and documented processes for the reconnection of ecosystem entities, ie reconnection steps an ecosystem entity may take to request reconnection (see Table 6).
- Mechanisms for the ecosystem entity to be notified promptly of the steps and conditions under which the ecosystem entity may be allowed to reconnect.
- Receipt of verification from the compromised entity that the incident has been remediated, which could also be supported by further verification by an independent third party.
- Contingency plans (eg non-standardised procedures) to address circumstances during the period when ecosystem entities have been disconnected from the FMI's ecosystem.

Steps for reconnection for an ecosystem entity

An ecosystem entity disconnected due to a cyber or operational incident may need to take a series of steps to be allowed to reconnect to the FMI ecosystem. Each step may have associated gateway outcomes that have to be achieved before moving to the next step.[60] Using principle-based gateway outcomes may help to ensure flexibility to address different situations and circumstances. Table 6 sets out a stylised example of reconnection steps an FMI may follow and associated gateway outcomes.[61, 62]

Stylised example of reconnection steps and associated gateway outcomes — Table 6

Reconnection steps	Examples of associated gateway outcomes
Assessment	● Disconnected ecosystem entity has identified the type and the extent of the cyber or operational incident and implemented incident response measures. ● Disconnected ecosystem entity has sufficient understanding of the root cause and impacts of the cyber or operational incident on its operations, ICT infrastructures, participants, etc.
Remediation	● Disconnected ecosystem entity has taken remediation steps to restore its operations/ICT infrastructures to a known trusted state. ● Disconnected ecosystem entity can provide evidence of/demonstrate the integrity of its operations/ICT infrastructures as necessary.
Assurance	● Disconnected ecosystem entity has provided sufficient assurance (including verification) to the FMI and other stakeholders as appropriate that its ICT infrastructures are ready to be reconnected to the FMI ecosystem and resume operations.
Reconnection	● Disconnected ecosystem entity has reconnected to the FMI's ICT infrastructures and has undertaken necessary testing to confirm that data and ICT infrastructure integrity have been re-established.
Recovery/resumption	● Disconnected ecosystem entity has recovered/resumed its operations as usual.

[60] A gateway outcome is an intermediate result within a series which is a necessary precondition to achieve further progress towards an objective, in this case reconnection to an ecosystem entity.

[61] This table is modelled on the diagram provided in G7 Cyber Expert Group (2025), with necessary modifications/adaptations to be relevant for FMIs.

[62] Although it is not necessarily specific to the FMI's disconnection/reconnection process, an FMI's reconnection framework may include the "recovery" or "resumption" step(s) after the "reconnection" step.

3.5.3 Communications, testing and review of disconnection/reconnection

Communications

Clear communication between FMIs and ecosystem entities is instrumental for optimising the effectiveness of the disconnection/reconnection processes, enhancing ecosystem readiness and maintaining trust. This includes communication both during an event and under normal conditions to ensure that ecosystem entities, in particular FMI participants, are informed and able to manage associated risks. Advance disclosure of the circumstances in which a disconnection/reconnection may occur can further enhance preparedness, while clear communication during the event itself helps to streamline the disconnection/reconnection process and sustain trust across the ecosystem. Once disconnection occurs, ongoing communication with the disconnected ecosystem entity allows the FMI to understand and monitor its status (including the prompt performance of settlement obligations through alternative means) until its eventual (but conditional) reconnection.

Post-incident/testing review

Recording and reviewing disconnection or reconnection decisions and processes, including the rationales behind them, may help improve disconnection and reconnection criteria and processes and aid the development of alternative approaches to address similar cyber and operational incidents in the future.

Practical considerations for the testing and review of disconnection and reconnection criteria and processes include:

- Regularly testing business continuity plans with ecosystem entities, including scenarios involving different types of disruptions and various staged reconnection approaches.
- Documenting all decisions and actions taken during a disruption and disconnection event and reconnection efforts to support post-incident analysis and continuous improvement.
- Incorporating lessons learned from testing and incidents into an updated framework on disconnection and reconnection.

Annex 3A Business continuity metrics

The metrics in Table 3A.1 provide industry standard terminology that may be helpful for FMIs. Using a standard set of business continuity metrics can facilitate measurement of time frames against stated objectives and enable comparison of performance across different incidents. These definitions are reproduced from NIST SP 800-34 and ISO 22300:2025(en).

Business continuity metrics — Table 3A.1

NIST SP 800-34 definitions	ISO 22300:2025(en) definitions
Recovery point objective: represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.	**Recovery point objective**: point to which information used by an activity is restored to enable the activity to operate on resumption. Note: This can also be referred to as "maximum data loss".
Recovery time objective: defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources,[and] supported mission/business processes.	**Recovery time objective**: period of time following an incident within which a product and service or an activity is resumed or resources are recovered. Note: For products, services and activities, the recovery time objective is less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.
Work recovery time: represents the maximum tolerable amount of time that is needed to verify the status of systems and/or data integrity after resumption. The work recovery time is implicitly addressed in standards and is used to describe the post-recovery phase as part of the contingency planning process.	No comparable definition.
Maximum tolerable downtime: represents the total amount of time the system owner/authorising official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Note: The maximum tolerable downtime value cannot be less than the sum of the resumption time objective and the work recovery time. It usually takes into consideration the detection and decision time.	**Maximum tolerable period of disruption**: time it would take for adverse impacts, which can arise as a result of not providing a product/service or performing an activity, to become unacceptable. Note: This is also referred to as "maximum acceptable outage".

Annex 3B References for disconnection/reconnection processes

- Canadian Centre for Cyber Security (2026): "Ransomware: how to prevent and recover", *Awareness Series*, ITSAP.00.099.
- Cross Market Operational Resilience Group (CMORG) (2023): *System Integrity Reconnection Framework*.
- G7 Cyber Expert Group (2025): *G7 fundamental elements of ransomware resilience for the financial sector*.
- ——— (2025): *Reconnection framework best practice*.
- ——— (2026): *Reconnection framework best practice - Technical annex.*
- National Institute for Standards and Technology (NIST) (2021): "Developing cyber-resilient systems: a systems security engineering approach", *NIST Special Publications*, no 800-160, vol 2, revision 1.
- ——— (2021): "Managing the security of information exchanges", *NIST Special Publications*, no 800-47, revision 1.
- Securities Industry and Financial Markets Association (SIFMA) (2025): *Financial Services Sector Reconnection Framework*.

Annex 3C Reference questionnaire for FMIs

The following questionnaire is composed of a series of thematic questions and possible answers which FMIs may use to assess their response, resumption and recovery plans.

Where provided, the answers aim to reflect different situations or options which are neither mutually exclusive nor exhaustive. Other situations and options may be possible depending on factors including: (i) the type of FMI; (ii) the nature of the cyber threats/risks they intend to address; (iii) their specific business models, cyber resilience strategies/frameworks, operational processes and ICT infrastructures; and (iv) applicable laws, regulations, standards and best practices. The order of appearance of the questions is not an indication of priority or preference.

Design of systems and processes

1. Does your FMI use of any of the following measures to ensure data integrity and safely resume operations in the event of a data integrity breach?
    a. Define clear standards and policies for data integrity requirements and data access, and who is allowed to modify the data based on the "need to know" and "least privilege" principles.
    b. Design and implement data validation rules and input rules to ensure data accuracy and integrity (including those for replicated/restored data).
    c. Utilise secure storage.
    d. Design and implement data encryption.
    e. Design and implement privileged access management to sensitive data.
    f. Put backup and restore procedures in place as well as adequate storage and protection measures for these backups.
    g. Regularly test backup and restoration processes.
    h. Ensure data auditability through logs for data changes.
    i. Implement logging and monitoring of unwanted events such as unauthorised changes of data.
    j. Perform regular security and integrity checks of data (ie together with connected parties if necessary and applicable).
2. In your cyber resilience framework, does your FMI consider extreme but plausible cyber risk scenarios, including but not limited to the following, accompanied by suitable responses to resume operations?
    a. Disruption/suspension of FMI operations without a data integrity issue (eg distributed denial-of-service (DDoS) attack).
    b. Disruption/suspension of FMI operations with a data integrity issue (eg data corruption by a ransomware attack, data loss by a wiper attack).
    c. Disruption/suspension of FMI operations due to a cyber incident derived from participants and/or third-party (nth party) service providers.
    d. Disruption/suspension of FMI operations spanning over two or more business days.
    e. Disruption/suspension of FMI operations due to a cyber attack affecting all/some of the backups (eg corruption/loss of the data copied/stored in the backup facility).

Alternative measures

3. Does your FMI have alternative measures and/or systems such as the following to support resumption of critical operations within two hours in cyber scenarios?

    a. Data recovery services.

    b. Redundant systems (servers, storage, networks, etc) that can instantly take over in case of outage.

    c. Failover and fallback procedures that automatically switch to backup systems.

    d. Synchronous and real-time data replication.

    e. Hot sites or warm sites.

    f. Cold sites or remote recovery sites.

    g. Automated failover and orchestration.

    h. Regular testing and drills or response, resumption and recovery capabilities.

Impediments or extreme circumstances that prevent the FMI from resuming critical operations within two hours

4. Does your FMI consider any cyber scenarios in which completion of settlement by the end of the day seems challenging in your cyber resilience framework, including but not limited to the following?

    a. Disruption/suspension of FMI operations with a data integrity issue (eg data corruption by a ransomware attack, data loss by a wiper attack).

    b. Disruption/suspension of FMI operations spanning over two or more business days.

    c. Disruption/suspension of FMI operations due to a cyber attack affecting all/some of the backups (eg corruption/loss of the data copied/stored in the backup facility).

Conditions/scenarios for safe resumption of critical operations within two hours

5. Does your FMI have a documented business continuity plan/disaster recovery plan/playbook(s) to enable/facilitate resumption of critical operations within two hours in the case of an extreme but plausible cyber scenario? If yes, what is the scope of the plan?

    a. It addresses limited or certain extreme but plausible cyber scenarios.

    b. It addresses a range of extreme but plausible cyber scenarios, excluding those with data integrity issues.

    c. It addresses a range of extreme but plausible cyber scenarios, including those with data integrity issues.

6. Does your FMI have any measures to enable/facilitate the resumption of critical operations within two hours in the case of a severe cyber or operational incident with data integrity issues (eg data corruption)? If yes, what is the scope of the measures?

    a. They enable or facilitate resumption of critical operations in the case of limited severity incidents with data integrity issues.

    b. They enable or facilitate resumption of critical operations in the case of severe incidents with data integrity issues.

7. Which of the following measures, with unique risk profiles, does your FMI use (if any) to enable/facilitate resumption of critical operations within two hours in the case of a severe cyber or operational incident with data integrity issues?

    a. Non-similar facility or alternative systems.

    b. Public cloud service or other similar third-party service providers with high availability and data integrity features.

    c. A (non-active) tertiary data centre/data bunker.

    d. Trusted data sources (eg use of snapshot/golden point, maintenance of immutable backups of critical data in secure, offline environments to support rapid and safe restoration).

Disconnection and reconnection of ecosystem entities

Disconnection criteria/processes

8. Does your FMI have clear criteria/processes for disconnecting ecosystem entities, including the following?

    a. Objective criteria for when an ecosystem entity should be disconnected from the FMI (eg cyber threats, technical failures, financial or compliance issues), including what specific operational, financial or compliance issues trigger disconnection.

    b. Transparent and documented process for determining when disconnection is necessary and how the decision to disconnect an ecosystem entity is made, communicated and executed.

    c. Clear terms of service or rules for ecosystem entities regarding when and why disconnection may occur.

    d. Mechanisms to ensure proportionality and appropriateness to the nature of the breach or risk posed by the ecosystem entity to avoid unnecessary or overburdening disconnection.

    e. Mechanisms for the ecosystem entity to be notified promptly if they are at risk of disconnection, including how quickly ecosystem entities will be informed of impending disconnections.

    f. A grace period or opportunity to correct issues for disconnected ecosystem entities.

    g. An escalation or appeal process for ecosystem entities who disagree with a disconnection decision (eg the conditions under which an ecosystem entity can request an appeal, the procedure for review of the disconnection decision).

    h. Communication strategy to ensure that ecosystem entities are kept informed throughout the disconnection process.

    i. Regular testing of the disconnection capabilities/scenarios and communication strategies.

9. Are the criteria/processes for disconnection in line with industry best practices and/or regulatory/supervisory/oversight expectations?

10. Are there regular updates and reviews to ensure that the disconnection criteria/processes remain appropriate and effective? Do regular updates include requests for inventories of ecosystem entities' connected systems to inform the disconnection approach in the event of an incident?

11. Are the disconnection criteria/processes documented in a clear, accessible format that all ecosystem entities can easily refer to? Are these criteria/processes included in contracts, user manuals or operational guidelines?

Reconnection criteria/processes

12. Does your FMI have clear criteria/processes for when and how a disconnected ecosystem entity can be reconnected to the FMI system, including the following?
    a. Objective criteria for when an ecosystem entity could be reconnected to the FMI system.
    b. A transparent and documented process for the reconnection of ecosystem entities (eg steps an ecosystem entity takes to request reconnection).
    c. Mechanisms for the ecosystem entity to be notified promptly of the conditions on which the ecosystem entity could be reconnected.
    d. Communication strategy to ensure that ecosystem entities are kept informed throughout the reconnection process.
    e. A timely escalation or appeal process for ecosystem entities who disagree with a reconnection decision (eg the conditions under which ecosystem entities can request an appeal, the procedure for review of the reconnection decision).
13. Does the FMI require documented verification from an independent third-party confirming the initial threat has been successfully remediated? Are there documented provisions where such a verification can be waived?
14. Are the criteria/processes for reconnection in line with industry best practices (eg formal root cause analysis, independent cyber security report on the incident etc) and/or regulatory/supervisory/oversight expectations?
15. Are there regular updates and reviews to ensure that the reconnection criteria/processes remain appropriate and effective?
16. Are the reconnection criteria/processes documented in a clear, accessible format that all ecosystem entities can easily reference? Are these criteria/processes included in contracts, user manuals or operational guidelines?

Disconnection/reconnection readiness

17. Does the FMI have an ICT system and/or predefined arrangement or playbook (in coordination with its ecosystem entities) to address possible scenarios for disconnections and reconnections of ecosystem entities?
18. Does the FMI conduct regular tests or exercises to verify that it can ensure timely disconnection and reconnection of ecosystem entities under different scenarios in accordance with its ICT system, predefined arrangement and/or playbook?

4 Cyber resilience testing and exercising

4.1 Introduction

This tool describes the various categories of testing and exercising used in CRF testing programmes. It also provides references and practical considerations for the development of a cyber resilience testing programme and for the preparation and execution of the testing and exercising in each of these categories.

4.2 Understanding the categories of cyber resilience testing and exercising

There are several categories of testing and exercising, each serving a distinct purpose in evaluating cyber security, cyber resilience and business continuity arrangements. The appropriate scope, scale and resource allocation of a testing and exercising programme depends on the FMI's risk appetite and the criticality of its ICT system or the change being evaluated, reflecting a risk-based approach and the cyber maturity of the organisation. Examples of categories of cyber resilience testing and exercising that may be part of a testing programme are described below.

Secure development life cycle

- *Static application security testing (SAST)* and *software composition analysis (SCA)* tools are used to embed testing activities into a secure software development life cycle (SDLC). They identify vulnerabilities in the source code and its dependencies,[63] to reduce technical debt[64] and fix security flaws during the development phase. This is faster and cheaper than remediating flaws in production, thereby shifting security left[65] (see section 4.4.3). *Dynamic application security testing (DAST)* tools may also be used in this context.[66]
- *Security-oriented AI tools,* including SAST and DAST solutions with AI capabilities, can support a secure SDLC by conducting vulnerability scanning, supporting test-driven development and assisting in code review for security issues. However, if not implemented with a human-in-the-loop and other security measures, these tools may pose risks, including false negatives that allow vulnerabilities into production, false positives causing alert fatigue, and potential data exposure when proprietary code is processed or stored by external AI systems.

Regular testing and exercises

- *Vulnerability assessments* of live systems, networks and applications use a combination of threat intelligence, automated tools (such as DAST) and human analysis in production or pre-production environments to identify security weaknesses, such as unpatched software or

[63] SAST tools scan application source code to find weaknesses such as injection flaws or insecure data handling before the application is even compiled. SCA tools scan third-party libraries and open source components to identify known vulnerabilities, outdated versions or licensing issues.

[64] "Technical debt" refers to the extra work caused by choosing quick, short-term solutions over robust, long-term approaches in software development. It can lead to higher maintenance costs, slower development and decreased reliability if not addressed.

[65] "Shifting security left" means integrating security early in the SDLC, rather than at the end. This approach helps to detect and fix vulnerabilities during design, coding and testing stages. It reduces risks, lowers costs and improves software quality by addressing issues proactively.

[66] DAST tools actively probe running applications for runtime vulnerabilities.

misconfigurations. FMIs can then prioritise technical flaws across their deployed infrastructure and allocate resources to address critical security gaps before they can be discovered and exploited by attackers.

- *Penetration testing* takes vulnerability assessments a step further by simulating real-world cyber attacks and validating the exploitability of identified weaknesses and the effectiveness of existing security controls.
- *Red team testing*[67] consists of advanced exercises that simulate multi-stage, sophisticated adversary attacks based on real-world threat actors' tactics, techniques and procedures (TTPs) to assess technology, processes and human response. These tests provide assurance about the effectiveness of protective controls and defensive/detection measures (see section 4.5).

Business continuity plan and operational resilience testing and exercising

- *Backup restoration testing* validates that backed-up data can be successfully restored to a functional state within agreed time frames.
- *Failover, disaster recovery and business resumption testing* validates the FMI's ability to resume critical functions and services and may include ecosystem entities.
- *Comprehensive testing of business continuity arrangements* validates the readiness of stakeholders and the end-to-end services' availability under stress scenarios.
- *Crisis communication exercises (*eg table-top exercises and simulations) assess the effectiveness of internal and external communications strategies, ensuring timely coordination and decision-making.

Cross-sectoral and cross-border activities

- *Ecosystem simulations and stress testing* help uncover vulnerabilities and transmission channels within the ecosystem, informing proactive measures for response, resumption and recovery.
- *Cross-sectoral and cross-border exercises* can validate the effectiveness of coordination between critical stakeholders within and across sectors (eg cross-border crisis management and contingency cyber security resilience exercises).
- *Tabletop exercises* are discussion-based exercises where personnel meet to discuss their roles during an emergency and their responses to a particular emergency situation (see the example provided in Annex 4B). Tabletop exercises can also be used to test decision-making and communication tools.
- *Crisis communication exercises* seek to assess the ability to manage communication during incidents.
- *Functional exercises* are simulations that allow personnel and ecosystem participants to validate their operational readiness for emergencies by performing their duties in a simulated operational environment.
- *Gold teaming* combines, in a strategic framework, leadership team crisis simulation tabletop exercises with cross-functional team exercises that include elements of attack (red team), defence (blue team) and collaboration of the two (purple team) to mimic a real-world scenario. It focuses on leadership's strategic decision-making during cyber incidents, stakeholder

[67] Certain jurisdictions may refer to red team testing as threat-led penetration testing (TLPT). Per the FSB cyber lexicon, TLPT and red team testing are synonymous.

communication, incident response testing, risk prioritisation and the embedding of lessons learned from previous incidents and exercises into operational practice.[68]

4.3 Developing a cyber resilience test programme

This section includes practical considerations for the development of a test programme, including the evaluation of response, resumption and recovery plans.

4.3.1 Practical considerations for test programme development

A testing, training and exercise programme may include several components and rely on a wide range of methods to assess: (i) management and staff's operational readiness; and (ii) the completeness and effectiveness of the FMI's cyber resilience framework as well as its response, resumption and recovery capabilities.[69] The steps in Table 7 can help an FMI design a comprehensive testing programme (see Box 6 for additional testing considerations for managing risks posed by an FMI's ecosystem).

Development of a cyber resilience testing programme — Table 7

Steps	Practical considerations
Scoping and planning	• Define clear objectives for each test and ensure alignment with strategic goals. • Incorporate proportionality to the risks an FMI faces and the criticality of the tested systems. • Establish a testing schedule that balances periodic and ad hoc exercises. • Use a controlled environment for testing to avoid disruptions to live operations.
Training and preparation	• Inform personnel of their roles and responsibilities under the cyber resilience framework. • Provide training to prepare personnel for exercises, tests and actual emergency situations related to response and recovery plans. • Invest in the technical capability to test response, resumption and recovery plans. Test tools in an isolated or non-production environment to validate their effectiveness in supporting response, resumption and recovery.
Testing activities	• See section 4.2 for categories of testing and exercising.
Resource allocation	• Allocate sufficient resources, including budget, skilled personnel and tools. • Engage external experts for advanced testing, such as threat-led penetration testing or red team testing.
Change management	• Conduct tests before and after significant system changes to ICT infrastructure to validate security and operational resilience. • Identify significant changes through a structured change management process.
Ecosystem and cross-sectoral engagement	• Coordinate with ecosystem partners, including counterparties, regulators and critical third-party providers. • Participate in cross-sectoral and cross-border exercises to validate coordination and readiness.
Governance and responsibilities	• Ensure the board and senior management understand and are invited to provide guidance and advice on the scope and objectives of the programme and the test strategies. • Establish clear roles and responsibilities for all stakeholders involved in the testing process.

[68] See for example De Nederlandsche Bank, *Gold teaming guide for the financial sector*.

[69] See for example T Grance, T Nolan, K Burke, R Dudley, G White and T Good, "Guide to test, training, and exercise programs for IT plans and capabilities", *NIST Special Publications*, no 800-84, 2006.

Evaluation and post-test activities	• Define measurable success criteria for each test to evaluate its effectiveness; use metrics such as detection time, response time and recovery time to assess performance. • Conduct a detailed review of test outcomes, including a timeline of events, findings and root cause analysis; document lessons learned and share them with relevant stakeholders. • Develop a remediation plan to address identified vulnerabilities and weaknesses; validate the effectiveness of remediation through follow-up tests or automated tools. • Regularly update the test programme to include emerging threats and evolving technologies. • Provide comprehensive reports to senior management, the board and regulators as required; use test results to inform updates to the cyber resilience framework and testing programme. • Validate lessons learned with internal and external stakeholders, including business lines affected; individuals with response, resumption and recovery responsibilities; and senior management. • Translate lessons learned into remedial actions (eg modify controls and procedures to improve future response, resumption and recovery activities) and track these actions to completion.

An example test programme, using a selection of exercise types with objectives and expected benefits, is provided in Annex 4A.

Box 6

Testing considerations for managing risks posed to an FMI by its ecosystem

The following are additional considerations related to managing ecosystem-related risk through an FMI's testing programme:

- Testing programme: Collaborate with stakeholders in the FMI's ecosystem (eg the FMI's participants) when conducting response and recovery testing to help an FMI identify complexities, dependencies and weaknesses in its response, resumption and recovery plans. Consider incorporating multiple ecosystem entity groups to identify complexities, interconnections and contagion risks.
- Coordination: Leverage end-to-end mapping of business functions and processes to conduct scenario-based testing with ecosystem entities. Participate in authority and/or industry-led system-wide cyber resilience exercises that test the resilience of the financial system.
- Information-sharing: Actively participate in information-sharing arrangements within the ecosystem to gather and disseminate threat intelligence.
- Cooperation arrangements: Establish formal channels with other FMIs and their ecosystem entities to validate the effectiveness of coordination and provide a forum for information-sharing on best practices, discussion of cyber and operational incidents and mitigation strategies against existing and potential vulnerabilities.[70] Such frameworks may be used to coordinate crisis management and joint decision-making across authorities and ecosystem entities; share sensitive and time-critical information through secure, pre-established channels; conduct sector-wide exercises, drills and simulations to validate procedures and build awareness; plan and test business continuity measures, enabling participants to assess and improve internal playbooks; define activation criteria and response protocols for major operational or cyber incidents; and conduct regular awareness-raising initiatives for key cyber security topics.

[70] At the international level, the G7 Cyber Expert Group (CEG) is a multi-year working group that coordinates cyber security policy and strategy across the G7 jurisdictions. The CEG conducts workstreams to improve the cyber resilience of the financial sector through preparedness, a consensus of the threat landscape and a shared approach to mitigating risk. At the national level, in several jurisdictions, there are financial sector cooperation structures for enhancing the cyber resilience of member FMIs and their ecosystem entities. See the US Department of the Treasury website at https://home.treasury.gov/policy-issues/international/g-7-and-g-20/g7-cyber-expert-group for more information.

4.4 Testing and exercising before and after significant system changes

A key component of cyber resilience is the rigorous testing of ICT systems both before and after significant system changes to verify their integrity, security and operational availability. Changes in the cyber threat landscape, such as the emergence of AI-driven threats, may also warrant updating the management and testing of system changes. This section provides insights into risks potentially stemming from system changes. It also provides practical considerations for the identification of significant system changes and for cyber resilience testing and exercising before and after such changes.

4.4.1 Risks from system changes

Significant changes may introduce new risks, including but not limited to new attack vectors, unpatched vulnerabilities and data integrity issues. Unmitigated risks may expose an FMI to adverse impacts, including the following:

- System changes may inadvertently create new attack vectors that attackers can exploit. For instance, software updates may introduce coding errors or insecure third-party integrations, while hardware upgrades or network reconfigurations may leave vulnerabilities if security settings are not properly adjusted.
- Not applying patches or updates may leave systems exposed to known vulnerabilities. However, even when patches are applied (see Box 7), they may not fully resolve the security issue or may unintentionally disrupt system functionality if not properly validated.
- Changes to databases, storage systems or backup processes may compromise data integrity or recoverability. For example, a software update that alters data processing workflows may inadvertently corrupt data or weaken encryption standards. Similarly, changes to backup systems may render them ineffective, leaving FMIs unable to restore operations after a cyber or operational incident.

Box 7

Practical considerations for software vulnerability and patch management processes

The following are practical considerations for the effective identification and eradication of software vulnerabilities to reduce cyber risks and maintain the cyber resilience of an FMI's ICT environment:

- Establish a clear policy that defines responsibilities and timelines, and ensure that critical vulnerabilities are prioritised, particularly for information assets involved in the FMI's processing of critical operations, including at all backup sites.
- Stay informed about new vulnerabilities through vendor updates and advisories.
- Automate the patching process and schedule regular updates to improve consistency and reliability.
- Test patches in a controlled environment to minimise disruptions and confirm successful deployment.
- Consider adopting new technology, such as AI vulnerability scanning and development tools, to accelerate the remediation of vulnerabilities and the deployment of software upgrades to critical code bases and dependencies.

4.4.2 Identification of significant changes to systems

A significant change to ICT systems (as well as to operational policies, procedures or controls) is generally any modification that may introduce new vulnerabilities, disrupt operations or affect the security and

reliability of critical systems. Rigorous testing of such changes helps to mitigate risks, ensure continued operational resilience of systems and maintain alignment with cyber resilience goals. This can be accomplished through a change management approach that includes:

- Following a structured and collaborative approach to identifying significant changes to ensure that no critical modifications are overlooked.
- Systematically documenting and categorising all ICT system modifications, prioritising those with the highest potential impact on security or operations and logging them in the FMI's change register.
- Conducting a cyber impact risk assessment for each change to evaluate the likelihood and potential consequences of new cyber vulnerabilities, ensuring that all system changes are tested in a risk-based manner and that testing resources are focused on the most critical areas.
- Engaging relevant stakeholders, including ICT development, cyber security and operational teams, to comprehensively identify and flag all significant changes requiring testing.

The nature and scope of significant changes is likely to determine the level and intensity of testing required. High-impact changes, such as those affecting critical systems or services, may demand more rigorous and comprehensive testing compared with lower-impact modifications. For example, a major upgrade to an ICT system would necessitate extensive testing – including vulnerability assessments, penetration testing and failover tests – to ensure security and operational continuity. Conversely, a minor configuration change to a non-critical ICT system may require only targeted validation. By aligning testing intensity with the significance of the change, FMIs can allocate resources efficiently and ensure testing efforts remain proportionate to the risks involved.

Categories of significant system changes

The following list outlines common types of significant system changes that typically require rigorous testing to manage security, operational and resilience risks:

- Technology upgrades (software and hardware) to catch defects, compatibility issues or unintended interactions.
- Network and configuration changes (eg network topology redesign, firewall reconfiguration, cloud migrations, multifactor authentication (MFA) implementation or virtual private network (VPN) updates) to prevent misconfigurations that may open new attack paths.
- New technologies, infrastructure and third-party integrations (eg AI, distributed ledger technology, external dependencies or cloud services) to conduct pre-implementation and ongoing testing to manage unknowns and supply chain risks.
- Upgrades to critical ICT systems and services (eg those supporting payment, clearing, settlement, fraud detection or participant data management) warrant thorough testing due to potential direct impacts on an FMI's core operations and security.
- Modifications to critical operational processes (eg authentication workflows, data processing procedures or disaster recovery plans) to avoid weakening controls or introducing reliability issues.
- Significant business changes (eg moving operations to a different location, onboarding new products, types of participants or outsourcing arrangements) to address related business and IT architecture risks.

4.4.3 Test automation and secure development life cycle

Performing vulnerability assessments and penetration tests after every significant system change, especially when major ICT infrastructure changes occur, materially improves cyber resilience.

DevSecOps[71] and test automation can enhance an FMI's cyber resilience testing programme by increasing the coverage, frequency and consistency of their testing programmes. These benefits can be further realised by embedding continuous integration/continuous delivery (CI/CD) pipelines[72] into the SDLC.

The following practices can improve the effectiveness of cyber resilience testing practices and the SDLC:

- Integrate test automation and DevSecOps into development and change management, enabling repeatable validation after patches, reconfigurations or upgrades by using automated vulnerability scanning and IaC security checks before deployment, and triggering targeted post-change tests in CI/CD pipelines. This enables repeatable, timely validation of security controls after patches, reconfigurations or upgrades, reducing the window of exposure to newly introduced vulnerabilities.
- Embed DevSecOps to make security continuous across the SDLC ("shift left") – apply SAST and SCA early during continuous delivery, use DAST and automated tests in continuous integration, leverage the latest AI security tools and rely on production monitoring and alerting for ongoing assurance.

Adopting these practices may help to reduce remediation costs and technical debt and promote shared responsibility.

4.4.4 Tracking remediation and validation

Effective tracking, prioritisation and remediation of vulnerabilities identified before or after significant system changes is particularly important for maintaining robust cyber resilience and helping FMIs systematically manage and close security gaps. This structured process normally begins with logging all findings in a centralised vulnerability management system to ensure accountability and traceability, with each vulnerability assigned a risk-based priority focused on threats to critical operations.

A centralised vulnerability management system helps to provide a single source for logging, assigning and monitoring all identified security weaknesses. Integrating this system with automated tools improves efficiency and enables oversight through dashboards that track key metrics like time to remediate. For example, a vulnerability permitting unauthorised access to any of the FMI's critical services would be immediately assigned to the security team with a high-priority status and a defined resolution deadline.

Established frameworks like the Common Vulnerability Scoring System (CVSS) provide a process to objectively assess the severity and potential impact of each weakness.[73] This ensures

[71] DevSecOps is a practice that integrates security (Sec) as a shared responsibility throughout the entire SDLC, merging it with development (Dev) and operations (Ops). It emphasises automation, collaboration and continuous security validation from initial code development through to deployment and operation, ensuring that security is not a bottleneck but an embedded and enabling component of agile delivery.

[72] A CI/CD pipeline automates integrating, testing and deploying code. CI frequently merges and tests code, while CD automates releases and deploys changes automatically. A CI/CD pipeline provides faster delivery, better quality and fewer errors.

[73] See https://nvd/nist.gov/vuln-metrics/cvss.

resources address the most significant threats first, such as a vulnerability enabling unauthorised fund transfers in a clearing system, while lower-risk issues are scheduled appropriately. Risk assessments may be periodically revisited as a vulnerability's severity can evolve with new threat intelligence. Moreover, FMIs may combine the technical assessment of a vulnerability, known as a base score, with a risk assessment considering ICT architecture and defence in depth features, known as an environmental score.[74] For example, a CVSS base score of seven in a particular FMI context may be adjusted after a risk assessment to a score of four, the latter value being the basis for risk assessments, prioritisation for remediation and validation of fixes. Environmental scores should recognise that cyber threats may combine multiple vulnerabilities together to circumvent defence in depth features, for example by using a combination of lower-risk issues to gain access to otherwise isolated systems.

Remediation efforts can be validated through rigorous retesting to confirm vulnerabilities are fully resolved and that no new risks are introduced (or residual risks are left unaddressed). This involves re-running targeted scans or penetration tests against patched systems, a process that can be streamlined with automated validation tools. For instance, after a flaw is addressed, focused tests are conducted to ensure the fix withstands attack simulations and maintains system stability.

Implementing such a structured approach may help FMIs to reduce operational risks and maintain trust among ecosystem entities. By ensuring every identified vulnerability is tracked, prioritised and promptly remediated, and by continuously monitoring the evolving threat landscape, FMIs may strengthen their defensive posture and protect the integrity of financial markets.

4.4.5 Stakeholder roles and responsibilities

Clearly defined roles and responsibilities related to testing for all stakeholders involved in strategies, planning, execution and validation help to ensure accountability and comprehensive coverage. Key stakeholders include risk management functions, executive management, ICT and cyber security teams, operational staff and third-party vendors – each with distinct contributions to the testing life cycle.

An FMI's board and senior management provide strategic planning, oversight and resource allocation for testing activities. ICT and cyber security teams lead technical execution, while operational staff ensure tests are conducted without disrupting critical functions. Ideally, third-party service providers and vendors would cooperate fully during the testing of their services and promptly address identified vulnerabilities.

An independent validation function may be useful to verify testing methodologies and to provide effective challenge. Identifying a designated remediation owner can help to maintain accountability for addressing findings, tracking progress and providing updates to relevant stakeholders. This approach helps to ensure testing outcomes are effectively integrated into the FMI's risk management framework.

4.5 Red team testing

This section provides practical considerations for red team testing, detailing a range of approaches to evaluate cyber resilience by simulating sophisticated, real-world attack scenarios that mirror the TTPs of actual adversaries. Unlike conventional penetration testing, which often focuses on technical

[74] Defence in depth is a layered security strategy that applies multiple, complementary controls across people, processes and technology to reduce reliance on any single safeguard. It combines preventive measures (eg firewalls, MFA, patching), detective capabilities (logging, monitoring, endpoint detection and response) and responsive actions (isolation, incident response) to slow, detect and contain attacks. Built on principles like segmentation, least privilege, strong authentication and redundancy, it spans endpoints, networks, applications, data, identities and third parties. The result is improved resilience, reduced blast radius and greater assurance that critical services remain secure even if one control fails.

vulnerabilities, red team testing adopts a holistic approach, assessing people, processes and technology across the organisation, including critical third-party dependencies.

Given that red team testing attempts to simulate realistic attack scenarios based on real-world threats, it can go beyond classical testing to identify:

- unknown vulnerabilities
- privilege escalation paths
- data exfiltration paths
- configuration management gaps
- well-hidden misconfigurations
- weaknesses arising from the interplay of different factors (eg human, procedural and technical)
- delays in patching
- weaknesses in detection, triaging and escalation.

The main participants in red team testing belong to the following teams, depending on their roles and responsibilities:[75]

- blue team – the people in the entity that is the subject of the test, whose prevention, detection and response capabilities are being tested without their foreknowledge
- threat intelligence provider – the team that looks at the range of possible threats and carries out reconnaissance on the entity
- red team testers – the team that carries out the simulated attack by attempting to compromise the critical functions of the entity, mimicking a cyber attacker
- control team: a small team within the target entity whose members are the only ones who know a test is happening and who lead and manage the test.

Integrating red team testing into an FMI's cyber resilience framework offers significant benefits, including the ability to validate the effectiveness of defensive measures under realistic conditions and identify gaps that may not be apparent through traditional testing. The results can feed directly into vulnerability management; response, resumption and recovery plans; and continuous improvement cycles.

The following subsections provide some practical considerations to assist FMIs in adopting, designing and executing red team testing exercises to achieve a quality baseline for their conduct.[76]

4.5.1 Considerations for designing red team testing

The following aspects may be helpful in designing a red team testing programme:

- Scope and objectives: Agreeing to the scope and objectives in advance, including which critical functions, critical systems and third parties are involved, helps to align red team testing with

[75] These definitions are from ECB, *TIBER-EU framework: how to implement the European framework for threat intelligence-based ethical red teaming*, 2025, www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html.

[76] The US NIST and Sandia Laboratories provide a useful reference guide, the Information Design Assurance Red Team (IDART) quick reference sheet, which can be found at www.sandia.gov/app/uploads/sites/87/2021/08/2017-09-13_IDART_QRS_SAND2017-9579-TR.pdf.

overall cyber resilience objectives.[77] Focused red team testing, followed by a tracked remediation plan and retest, strengthens the overall cyber resilience strategy if conducted regularly, including after significant system changes.

- Staff and resources: Red team testing requires significant planning and resources. See section 4.5.3 for detailed considerations on governance, resourcing and timeline planning.
- Baseline cyber maturity: Since red team tests involve attacks on live production systems, these tests tend to be more useful when firms have succeeded in establishing a robust cyber security baseline. If significant flaws and weaknesses are known, there is a high risk of wasting dedicated resources, since the target systems may be easily compromised by the testers.
- FMI size and risk profile: An FMI's size and risk profile determines the level at which red team testing is implemented within the firm's cyber testing framework. While larger firms may regularly conduct full-scale red team testing, lighter testing approaches may be used in the case of resource constraints. Testing can be further tailored to an FMI to realistically assess the impact of real world attacks on live production systems, such as simulating a multi-stage end-to-end attack as well as testing detection and response capabilities, potentially also including compromised third-party service providers.

4.5.2 Risks involved in red team testing

Red team testing involves inherent risks due to the critical nature of the targeted systems, personnel and processes. As red team testing activities are carried out against live production systems, an FMI may be exposed to heightened operational risk should incidents arise during testing. Careful risk assessments, safeguards and specific supervisory engagement from relevant stakeholders and managers across the FMI's organisation help to mitigate these risks. Designing red team tests to avoid adverse impact on participants is critical. Securing informed, exercise-specific written consent from potentially affected participants and implementing effective safeguards can also mitigate risk.

To ensure the realism of attack scenarios, the TTPs used by red teams should continually evolve to be consistent with the TTPs of real threat actors. AI tools may help red teams to identify attack paths faster, ultimately resulting in the remediation of vulnerabilities. However, red teams' use of certain AI tools, such as AI agents, if not subject to sufficient guardrails, could pose new risks to FMIs given their autonomous nature and decision-making capabilities.

More specifically, risk management throughout the complete test process is critical to prevent denial-of-service incidents, system crashes, damage to critical or important live production systems, or loss, modification or disclosure of data. Such risk management may be informed by the considerations listed in Table 8.

Risk management throughout the red team testing process — Table 8

Activities	Practical considerations
Risk assessment and management	● Conduct a thorough risk assessment during the preparation phase of a test. ● Track risk and manage measures for test conduct (eg regularly update the risk register, define red team actions requiring permission from the entity, etc).
Backup and restoration	● Ensure backup and restoration capabilities are in place and functioning.
Escalation chain	● Inform personnel at relevant positions within the escalation chain to contain unwanted escalations (eg isolating servers, involving law enforcement, etc).

[77] Frameworks like TIBER-EU, CBEST and ART provide structured methodologies for the implementation of comprehensive red team testing: TIBER-EU Framework, CBEST Threat Intelligence-Led Assessments | Bank of England, Advanced Red Teaming (ART) | De Nederlandsche Bank.

Secure communication	• Use secure communication channels, such as encrypted mail and secure data rooms, as well as out-of-band channels. • Use code names to avoid the defenders becoming aware of the testing.
Red team testing provider contracts	• Require providers to meet stringent security standards, including data handling, storage and deletion, as well as breach notification provisions and confidentiality. • Define out-of-scope systems. • Specify actions not allowed to be performed, eg unauthorised destruction of equipment, uncontrolled modification of data, blackmailing, violence, threats to or bribing of employees, inclusion of indemnity insurance and coverage.
Availability and qualifications of red team members	• Ensure trustworthiness of personnel, eg by performing background checks and checking for potential conflicts of interest. • Ensure availability of sufficient personnel (including adequate replacement for red team members on leave or holidays). • Ensure a large variety of technical and other skills, eg sector-specific knowledge, operating systems, network security, web application security, programming and scripting, malware, cloud security, virtualisation, mobile security, exploit development, social engineering, vulnerability analysis, etc. • Ensure required language, project management, communication and presentation skills, particularly for the red team lead. • Collect evidence of the provider's experience of the sector and of the qualifications of the individual red team members by requiring curricula vitae, accreditations, professional certificates, references and proof of adequate experience in testing.

4.5.3 Practical considerations for conducting red team testing

When conducting red team testing, the following practical considerations help to maximise learning.

Governance

Given their responsibility for cyber resilience, boards generally take direct ownership of red team testing, including authorising a test as well as taking responsibility for providing adequate resources for the respective remediations. This may include one board or senior management member being regularly informed about or involved in the test. Governance best practices include documented risk assessments, clear out-of-scope boundaries, safety controls and post-exercise reporting.

Resources

During red team testing exercises, an effective control team may include a certain cross-section of the FMI, such as cyber testing/project management personnel, business leaders, technical experts and risk and control staff. Control team members are clearly separated from the defenders in their daily work and are bound to secrecy (eg via a non-disclosure agreement), to not reveal the conduct of the test to the defenders (which would affect the realistic testing conditions).

The resources required for a test might vary based on the test's size and scope. Below are some practical considerations related to resourcing:

- Adequate time: Active red team testing may last for only several weeks or months, but the complete test, including preparation, threat intelligence collection and closure (including replay and learning), can easily require more than a year. More complex red team testing, including

testing different scenarios that mimic different threat actors and attack paths, may require further time commitments.[78]

  - A control team lead and a deputy are assigned to each red team and typically dedicate up to half of their time during the active testing and other "hot" periods. Additional experts are also granted sufficient time resources based on their level of involvement.
  - Following the conclusion of the active testing phase, the defenders need sufficient time for evidence collection, processing, report writing, workshops, exchanges with the red team members and remediation planning.
- Adequate monetary resources: Red team testing costs can vary largely based on the size and scope of the test as well as the range of additional services procured.
- Implementation of remediation measures and retesting are not part of red team testing itself but may require additional resources.

Leveraging leg-ups and grey boxing

"Leg-up" and "grey boxing" techniques allow the red team to simulate more skilled and better attackers. Using these techniques, the control team helps the red team: (i) simulate more skilled and better resourced attackers in a shorter time period; and (ii) test all stages of the cyber kill chain up to the final target systems.

Leg-ups are a form of planned informational or technical support to the red team members by the control team, in which they help the red team members bypass a barrier they would otherwise not be able to penetrate. [79] They are usually granted after the red team members have tried for an agreed period of time to complete a certain attack step.

Leg-ups can range from providing information about systems or security measures to provisioning of dedicated user or even privileged accounts. They are therefore vital to allow for test continuation and to ensure testing of all phases (ie in, through, out) of the cyber kill chain, according to an "assume breach" mentality. Leg-ups are generally clearly outlined in the test plan, including information on when they will be granted and the specific actions to be performed. In general, leg-ups are minimal; they are used only to bypass one barrier in the test. They are not meant for use across different scenarios, to avoid triggering detections in multiple test phases.

Grey boxing is another form of support where the control team may provide additional information about certain test situations to red team members, mainly with the aim of helping the red team save time. Grey boxing is similar to informational leg-ups, but more ad hoc and case-specific and therefore not pre-planned. Examples of grey boxing include but are not limited to:

- informing the red team members that they are on the wrong path (ie have a clearly wrong assumption or are walking into a dead end);
- providing additional, situational information to help the red team members advance more quickly (eg providing information on why something is blocked, certain defence mechanisms, the functionality of certain systems, etc); and
- providing internal insights into processes, policies or certain known vulnerabilities.

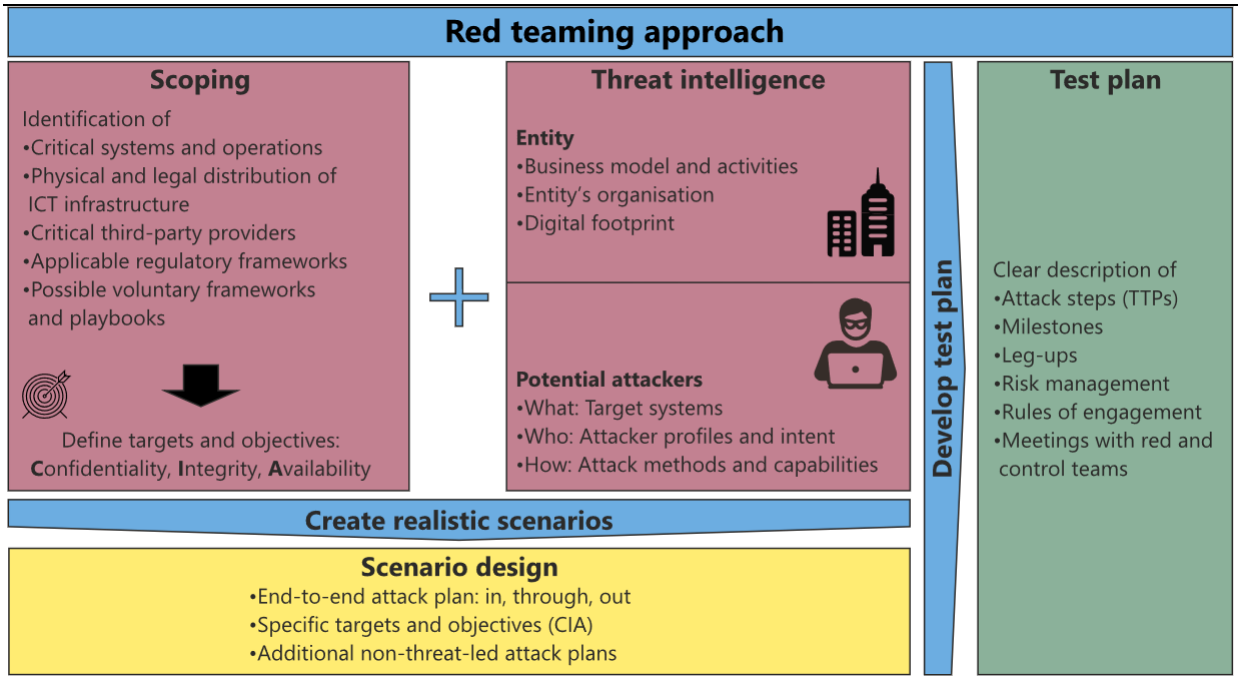
[78] For example, certain frameworks foresee that the time commitment does not fall significantly below 30 staff days per scenario to allow for adequate testing intensity.

[79] Examples of informational leg-ups include phishing delivery details, target paths (eg network segments or IP addresses) and system defences. Technical leg-ups include user accounts for failed phishing attacks and privileged accounts for failed escalation attempts.

4.5.4 Tailored approach for red team testing

Using a tailored approach for scoping and planning red team testing can align testing with an FMI's context and needs. This subsection provides practical considerations an FMI may use when adopting such a tailored approach (summarised in Figure 3).

Tailored approach for red team testing Figure 3



Source: CPMI.

Scoping

It is important to tailor a red team test's scope to consider an FMI's critical operations and systems. Often, critical operations and systems are already known from other assessments, eg information security management systems, asset inventories, business impact analyses, business continuity planning, business resolution planning or business strategies.[80]

It is also critical to address an FMI's ecosystem in scoping red team testing. This includes contemplating the distribution of critical ICT infrastructure across multiple jurisdictions, considering dependencies on critical third parties and conducting red team testing jointly with different legal entities and jurisdictions. In this context, FMIs may consider the following:

- Which type of service providers are critical services outsourced to and whether these services are already covered by certain red team testing regimes applicable to these providers.
- If outsourced services are covered within red team testing, or the interests of participants are affected, the respective third-party provider or participant needs to be informed or included in the control team. This is because attacks could affect the systems or other interests of a provider

[80] See section 3 on cyber response, resumption and recovery plans.

or participant and therefore require respective risk management and risk decisions, supported by informed consent, by the provider or participant.

Overall, it is useful to scope the target objectives (also referred to as "flags to be captured") in red team testing by defining them and providing a description of the respective action and evidence of their achievement or "capture", eg reading the content of a classified document or being able to place a dummy file on the hard disk of a certain critical system.

Threat intelligence

Threat intelligence collected by an external provider is used to make red team testing more realistic and relevant.[81] During threat intelligence collection, all relevant information about the internet footprint of the tested entity as well as potential attackers with an interest and the required skillset to attack such entity is collected in a threat intelligence report. Such information can be formally combined using threat scores (eg capability multiplied by intent) to rank attacks by likelihood and link certain attackers to the critical assets of the FMI. This allows for the identification of the most realistic scenarios.

Threat intelligence collection may include the elements listed in Table 9.

Threat intelligence elements (examples) Table 9

[81] An FMI may use internal teams to collect threat intelligence elements from various sources.

Tested entity	• **Digital footprint** - General information on domains and IP address ranges - Front ends and interfaces exposed to the internet - Hardware and software tools used - Employee credentials found on the internet - Look-alike domains which might be mistaken for the FMI's official domains - Vulnerable/exploitable software, systems or technologies - Relevant social media presence of employees - Sensitive information leaked on the darknet - Physical target information, eg on buildings and potential ways to physically access them • **Business model** • **Entity structure** • **Potential layoffs** • **Planned business changes** - Mergers and acquisitions
Potential attackers	• **Threat actor groups** - Any specific groups relevant to the FMI's context • **Type of threat actor** - eg nation state, criminal group, insider hacktivist • **Capability and intent to attack the tested FMI** • **Past activities** • **Critical functions and systems these threat actors are most likely to target** • **Other geopolitical implications or current trends**

Scenario design

By incorporating the collected threat intelligence, red team testing scenarios may be selected and further tailored to a specific test, including:

- Providing a detailed description of the end-to-end attack steps for each scenario, eg following the in, through and out phases of the cyber kill chain to simulate attacks as realistic to the entity as possible.
- Using TTPs, milestones, leg-ups and target objectives.
- Designing scenarios with alternative, non-threat-led attack paths to anticipate and test novel or otherwise interesting attack vectors (eg physical perimeter penetration which is often not threat-led, but of interest to many FMIs).

Test planning

To execute a successful attack, it is important to develop a comprehensive test plan, which may include but is not limited to the following aspects:

- A thorough description of the planned attack steps for each scenario, such as:

– attack steps (TTPs)

– target systems and flags to be captured

– milestones to be reached within certain deadlines

– leg-ups to be provided in case a milestone cannot be reached on time.

- Risk management measures taken by the red team members and regular risk tracking (eg continuously maintaining a register of current risks during the testing phase, regularly updated by the red team).
- Rules of engagement (eg actions which require prior authorisation by the entity, such as executing implants on critical servers, using exploits, etc).
- Meeting frequency and formats for regular exchanges during active testing (eg daily meetings between control team and red team members, weekly status updates, etc).
- Risks related to strategic and business objectives.

4.5.5 Effective attack execution on live production systems

For red team testing, attack scenarios are executed on live production systems, not in test or pre-production environments (unless explicitly used as an entry vector to gain access to production systems). Typically, the control function has mitigation measures in place, including protocols to manage detection of simulated attacks. For an effective attack execution, red team members may be given certain flexibility to also stray from planned TTPs if new opportunistic attack paths become apparent. Control team mitigations would need to be equally adaptable to accommodate this range of TTPs.

The control team does not reveal the test to the defenders for as long as possible, to maintain realistic testing conditions. If the red team testing activities are detected by the defenders (who are not aware of the ongoing test), the control team can utilise pre-planned plausible cover stories to prevent unwanted escalations, such as external reporting or system disconnects, while allowing the defenders to implement their response and mitigation measures to test remediation (ie triaging and reporting). Such situations require close monitoring to avoid impacts to critical systems.

When a test cannot proceed in a safe manner, it might be paused, for example if:

- A real attack is going on in parallel (in this case it might even be necessary to reveal the test to the defenders).
- The defenders detect the red team testing activities. Even if the escalation is contained by the control team, it can be helpful to pause the test for a few days or weeks to allow for a cooldown period for defender activity before the test resumes.
- There is a risk that a critical system would be damaged by an attack step. In this case the control team and the red team may have to reassess mitigation measures. For example, if the attack is deemed too risky, the control team could issue a leg-up and plan to perform a proof of concept of the attack step in the closure phase together with the defenders (see section 4.6.1 for information on the closure phase).

If the test cannot be resumed in an adequate manner without informing the defenders of the test, the control team may have clear concepts at hand for continuing the test in a purple teaming mode (ie involving both the red and blue teams).[82]

[82] ECB, *TIBER-EU purple teaming guidance*, 2025, offers additional insights on conducting purple teaming when a test cannot proceed otherwise (https://www.ecb.europa.eu/pub/pdf/annex/ecb.tiber_eu_purple_best_practices_2025.en.pdf?759d46ff75caf6e644af0fd757415aee).

4.6 Learning and evolving from testing and exercising

4.6.1 Learning from red team testing

After the completion of the active testing phase of a red team test, the control team can inform the defenders of the test about why it was conducted. This is referred to as the "closure phase". The following processes provide an effective means for implementing the red team's findings during the closure phase:[83]

- Provision of a red team members' test report, including a detailed timeline, findings with criticality, root cause analysis and recommendations.
- Provision of a defenders' test report, including logs, detections, own actions taken as well as a discussion of the findings and potential remediation measures.
- Joint review by the red team and defenders of performed actions for each scenario, anticipated attack steps not executed during the testing phase and potential measures for improvement.
- A remediation plan, including (per finding) the finding description, planned remediation measures, responsible unit and timeline.
- A test summary report which includes the involved parties, the project plan, the validated scope, executed attacks and paths, techniques and procedures used, deviation from the red team members' test plan and defenders' detection.
- A feedback event including all involved stakeholders to collect and preserve procedural lessons learned about the test to inform future tests.

After implementation of the remediation measures, the entity may retest based on the findings, eg during regular penetration testing and vulnerability scanning activities, to ensure they are properly implemented.

It is common practice to perform a risk assessment to determine current risk levels after a red team test. This would inform the prioritisation of remediation measures or the acceptance of any issues with minimal residual risk.

4.6.2 Learning and evolving from simulated exercises and real incidents

Testing and exercising programmes and broader cyber resilience frameworks can be enhanced through analysis of an FMI's own exercise results alongside external resources documenting international practices and actual cyber incidents. The following resources and approaches support this ongoing learning:

- International experiences on developing strategies for sector-wide operational resilience, including for FMIs, have been documented by international organisations as part of efforts to learn good practices in cyber risk regulation and supervision.[84] As part of the IMF Financial Sector Assessment Program during 2020 to 2025, cyber risk was covered in 16 jurisdictions with systemically important financial sectors. The testing and exercising findings from these reports may inform the continued development of testing and exercising programmes.[85]

[83] Having a board member or senior management present when delivering this message can help underscore leadership support and commitment to the test.

[84] T Gaidosch, E Islam, T Khiaonarong, R Ravikumar and C Wilson, "Good practices in cyber risk regulation and supervision", *IMF Departmental Paper*, 2026, www.imf.org/-/media/files/publications/dp/2026/english/gpcrrsea.pdf.

[85] The lessons learned from the analysis of cyber risk are contained and published in the financial stability assessment reports and technical notes, where applicable, for the respective jurisdictions and are publicly available. See www.imf.org/en/publications/fssa.

- Analysis of past incidents where cyber risks materialised from an FMI's ecosystem may be advantageous to FMIs given their interconnectedness with ecosystem entities. Learning from incidents where ecosystem-related risk materialised includes:
  - distilling concrete lessons on data integrity risk and contagion across an FMI's ecosystem;
  - identifying control failures and specifying target controls with key performance indicators/key risk indicators; and
  - practising cross-authority and cross-FMI coordination during cyber-driven operational crises.
- CISA's concise real-world case studies provide actionable insights to support the evolution of testing and exercising programmes.[86]

[86] www.cisa.gov/real-world-case-studies.

Annex 4A Example of a cyber resilience test programme

Table 4A.1 provides an example of a cyber resilience test programme combining several types of tests and exercises.

Sample cyber resilience test programme Table 4A.1

Exercise type	Description	Expected benefits
Phishing exercise	Test employee's awareness	Improve staff vigilance
Tabletop exercise	Discuss response, resumption and recovery plans and playbooks for incident responders	Build and practise cross-team coordination to improve participants' and service providers' muscle memory
Live simulation (eg penetration tests, red team tests)	Test technical response	Enhance practical skills of cyber security and ICT personnel
Computer-based simulation	Test systems under stress	Provide insights into the main vulnerabilities of the financial sector and key transmission channels that necessitate pre-emptive action and recovery and response measures
Executive-level exercise	Test decision-making under pressure	Improve crisis management
Ecosystem exercise	Coordinate across organisations, between the FMI and its participants	Strengthen industry resilience and communication lines

The FSB's report on effective practices for cyber incident response and recovery may be a useful resource to further develop an FMI's cyber resilience programme.[87]

[87] FSB, *Effective practices for cyber incident response and recovery: final report*, 2020.

Annex 4B Example of a tabletop exercise's test plan and playbook structure

This annex provides an example of a tabletop exercise and associated playbook as a reference. The tabletop exercise aims at testing an FMI's response, resumption and recovery plans to address a third-party vendor's software package corruption (as an example of testing supply chain resilience).

Sample tabletop exercise test plan structure Table 4B.1

Element of plan	Description
Objective	Validate a two-hour window for resuming FMI's core services relying on a vendor's software packages
Scope	List the dependent systems of the FMI's core services relying on the vendor's software packages
Scoring criteria	Define impact tolerances such as blackout time, data loss, issue count (could be in terms of complaints received from participants)
Debrief	Mandatory debrief immediately after the test to capture lessons learned

Sample tabletop exercise playbook structure Table 4B.2

Playbook aspect	Description
Internal teams and external partners	• Internal teams include the incident response team and operational platform team. • External partners include impacted and alternative vendors for the business continuity plan.
Signals identification, trigger for incident and incident type	• Signals are successive failures across different systems. • Trigger is external via public outage notification. • Incident type is for the vendor to determine, eg what type of breach it is, whether it is a compromised source code package or a ransomware incident. • Consider necessary internal escalation and incident reporting to relevant authorities.
Mitigation	• If there was a compromised source code package, mitigation could include freezing the FMI's CI/CD pipelines to prevent further spread, rotating associated API keys and signing certificates.
Investigation and analysis	• Determine the root cause, scope and impact (confidentiality, integrity, availability). Collect CI/CD logs for evidence, build artefacts/SBOMs, repo history, registry metadata, IAM/audit and network telemetry. Eg a malicious update to a third-party source package was ingested into the CI/CD pipeline, resulting in corrupted builds that propagated to the FMI's core services. The incident was detected after successive deployment failures and increased participant error reports. • Triage/scoping: freeze affected pipelines, map dependencies, pinpoint first bad build and package/version changes. • Forensics: verify signatures/hashes, reproduce in isolation, analyse credential usage and anomalous network activity. • Findings/decisions: confirm compromise, roll back to known good versions, preserve evidence, notify stakeholders and document lessons.
Eradication and recovery	• Remove corrupted source package from the vendor's software and provide the vendor's corrected package for integration into the FMI's CI/CD pipelines. • Recover the FMI's core services after verification and integrate the vendor's uncorrupted software package.
After action review (AAR)	• Assess the response to a compromised vendor's source code package affecting the FMI's core services, identify lessons learned and define corrective actions to strengthen resilience. • Hold a blameless AAR within 24–72 hours; include cross-functional/internal and relevant external stakeholders: what was expected, what happened, what went well, what needs improvement, decisions/constraints. Produce a corrective action plan with owners, deadlines and tracking in the risk register; define verification (eg follow up drills). Update runbooks, playbooks, communication templates and training. Share anonymised lessons with sector partners as appropriate.