EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

CYBER RESILIENCE OVERSIGHT EXPECTATIONS (CROE) FOR FINANCIAL MARKET INFRASTRUCTURES

Table of contents

1. INTRODUCTION

1.1. Background

The safe and efficient operation of financial market infrastructures (FMIs) is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In this context, the level of cyber resilience, which contributes to an FMI's operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy.

In June 2016, CPMI-IOSCO published the ***CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (Guidance)***[1]***,*** which requires FMIs to immediately take the necessary steps to implement it, in concert with relevant stakeholders, to ensure that they enhance their levels of cyber resilience. While cyber risks should be managed as part of an FMI's overall operational risk management framework, some unique characteristics of cyber risk, as noted in the Guidance***,*** present challenges to FMIs' traditional operational risk management frameworks:

First, a distinguishing characteristic of sophisticated cyber attacks is the persistent nature of a campaign conducted by a motivated attacker. The presence of an active, persistent and sometimes sophisticated adversary in cyber attacks means that, unlike most other sources of risk, malicious cyber attacks are often difficult to identify or fully eradicate and the breadth of impact difficult to determine.

Second, there is a broad range of entry points through which an FMI could be compromised. As a result of their interconnectedness, cyber attacks could arise through FMIs' participants, linked FMIs, service providers, vendors and vendor products. FMIs could themselves become a channel to further propagate cyber attacks – for example, via the distribution of malware to interconnected entities. Unlike physical operational disruptions, cyber risk posed by an interconnected entity

[1] https://www.bis.org/cpmi/publ/d146.pdf

is not necessarily related to the degree of that entity's relevance to the FMI's business. From a cyber perspective, the small-value/volume participant or a vendor providing non-critical services may be as risky as a major participant or a critical service provider. Internally, the risk of an insider threat from rogue or careless employees opens up yet another avenue for possible compromises.

Third, certain cyber attacks can render some risk management and business continuity arrangements ineffective. For example, automated system and data replication arrangements that are designed to help preserve sensitive data and software in the event of a physical disruptive event might, in some instances, fuel the propagation of malware and corrupted data to backup systems. Overall, a cyber attack's potential to cause significant service disruption of the broader financial system dictates the urgency of having an effective approach in place to manage it, and to minimise the probability that service resumption will introduce additional risks to an FMI or the wider financial sector.

Fourth, cyber attacks can be stealthy and propagate rapidly within a network of systems. For example, they can exploit unknown vulnerabilities and weak links in systems and protocols to cause disruption and/or infiltrate an FMI's internal network. Malware designed to take advantage of such latent vulnerabilities may circumvent controls. To minimise the impact of such attacks, FMIs would require capabilities to swiftly detect, respond to, contain and recover from such attacks.

Therefore, FMIs should continuously work to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to both the FMI itself and its overall ecosystem.

1.2. Purpose

FMIs are required to comply with the Guidance immediately, and overseers must simultaneously develop an oversight approach to assess their FMIs against the Guidance.

In this context, the Cyber Resilience Oversight Expectations (CROE) serves three key purposes: (i) it provides overseers with clear expectations to assess the FMIs under their responsibility and determine their cyber resilience maturity levels; (ii) it

provides FMIs with detailed steps on how to operationalise the Guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time; and (iii) it provides the basis for a meaningful discussion between the FMIs and their respective overseers.

The CROE are predicated on the Guidance and leverage off the existing "*CPSS-IOSCO Principles for financial market infrastructures"* (PFMIs) to ensure a full and coherent set of expectations. Additionally, whilst developing the CROE, the Eurosystem oversight function also considered existing international guidance documents and frameworks. In particular, the NIST Cybersecurity Framework, ISO/IEC 27002, COBIT 5, Information Security Forum's Standard of Good Practice for Information Security and Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool were used as a basis. Although FMIs may use maturity models from other international standards and frameworks for their internal purposes, the maturity models set out in the CROE provide the benchmark for overseers to determine the cyber resilience maturity levels of their FMIs against the Guidance.

1.3. Addressees

On 3 June 2013 the Governing Council adopted the "*Principles for financial market infrastructures*", introduced in April 2012 by the Committee on Payment and Settlement Systems (CPSS) of the Bank for International Settlements and the Technical Committee of the International Organization of Securities Commissions (IOSCO), for the conduct of Eurosystem oversight in relation to all types of FMIs. As the Guidance has been developed to provide supplemental guidance to the PFMIs in relation to several Principles, the CROE [*have also been adopted by the Governing Council of the ECB*] and will be applied by the Eurosystem for the oversight of all FMIs and also T2S.

Although the oversight of payment systems and of T2S is a Eurosystem competence, the oversight of clearing and settlement systems (SSSs/CSDs and CCPs) in most countries of the euro area is conducted by NCBs under national law competencies, often in cooperation with other national authorities. Therefore, these other authorities may also opt to use the CROE for these FMIs, in line with the applicable laws and regulations, to achieve the intended results.

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

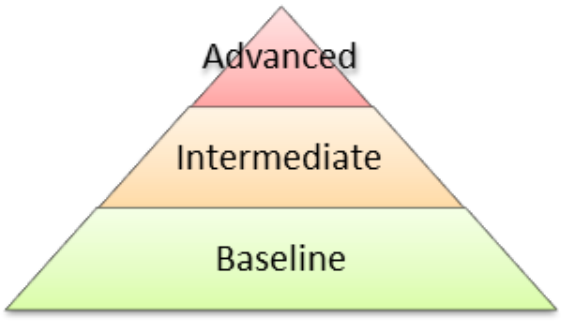
1.4. Requirements by type of FMI

1.4.1. Levels of maturity

The cyber threat landscape is constantly evolving and reaching higher levels of sophistication. In light of this, FMIs should make ongoing efforts to adapt, evolve and improve their cyber resilience maturity. To address the idea of continuous adaptation, evolution and improvement, the CROE uses a maturity model which provides the overseers and the FMIs with a benchmark against which they can evaluate the FMIs' current level of cyber resilience, measure progression and establish priority areas for improvement. The CROE establishes three levels of maturity: **Baseline, Intermediate** and **Advanced.**

The three levels of maturity (**Baseline, Intermediate** and **Advanced)** are defined as follows:

Baseline maturity level: Essential *capabilities* are established and sustained across the FMI to identify, manage and mitigate cyber risks, in alignment with the Board-approved cyber resilience strategy and framework, and performance of practices is monitored and managed.



Intermediate maturity level: In addition to meeting the Baseline maturity level, practices incorporate more advanced implementations (e.g. advanced technology and risk management tools) that have been improved over time, to proactively manage cyber risks to the enterprise.

Advanced maturity level: In addition to meeting the Baseline and Intermediate maturity levels, capabilities across the FMI are enhanced as needed, in the midst of the rapidly evolving cyber threat landscape, in order to strengthen the cyber resilience of the FMI and its ecosystem by proactively collaborating with its external stakeholders.

The CROE extensively refers to the term ***"capabilities"***, which is the FMI's ***"people, processes and technologies used to identify, mitigate and manage its cyber risks to support its objectives".***

1.4.2. Requirements

Although the CROE have been developed to provide FMIs with detailed and specific expectations on how to operationalise the Guidance, they also allow a degree of flexibility needed when dealing with a heterogeneous set of FMIs that differ from one to another in terms of size, volume and value of transactions and their role within the financial system. The role of the respective overseers or supervisors in applying this flexibility and judgement is very important.

For all **PIRPS and ORPS**, the Eurosystem Oversight function expects them to reach and maintain, at a minimum, a **Baseline** level of maturity, with active steps to be taken over time by the operator to attain an Intermediate level, where deemed appropriate.

In the case of **SIPS and T2S**, the minimum level of cyber maturity expected is **Intermediate**, with active steps to be taken over time by the operator to attain an Advanced level, where deemed appropriate.

The CROE should, however, not be considered as a checklist of measures FMIs need to strictly comply with, but instead as a set of practices that can contribute to FMIs' compliance with the Guidance. It will be the overseers' or supervisors' judgement to see whether the FMI, commensurate with its criticality, is complying with the baseline, intermediate or advanced level.

It is expected that FMIs will reach the aforementioned maturity levels across all eight categories of the Guidance; once FMIs reach and maintain their expected levels of maturity, they should continue to evolve and improve by taking relevant steps to

reach the higher levels of maturity, where it is appropriate and in line with their business specificities. This process of evolution and improvement should occur through discussions between the FMI and the respective overseer and supervisor over a sustained period of time and commensurate with the criticality of the specific FMI.

The three levels of maturity are intended to allow the FMI to build and evolve its maturity and capabilities in a multi-layered fashion over a longer period of time, with each level of maturity building additional mutually reinforcing good practices on top of each other. Therefore, the FMI should review the CROE in detail and consider how to implement the measures contained therein, giving due consideration on how best to build, improve and use its people, processes and technologies.

For other relevant regulatory, supervisory and oversight authorities that intend to use the CROE for other types of FMIs (e.g. CSDs, CCPs and TRs) under their responsibility, it is at the discretion and judgement of the authorities to determine what level of maturity they expect from the FMIs.

1.5. Structure of the document

In line with the Guidance, the CROE is presented in chapters that outline five primary risk management categories and three overarching components that should be addressed across an FMI's cyber resilience framework. The risk management categories are: (i) governance; (ii) identification; (iii) protection; (iv) detection; and (v) response and recovery. The overarching components are: testing; situational awareness; and learning and evolving.

The expectations in each chapter of the CROE are preceded by a preamble, taken from the Guidance, setting out the overarching objectives of each category and component. Depending on their complexity, chapters are then structured into one or more sections, which contain a specific set of expectations for each of the three levels of maturity.

In order to achieve the cyber resilience objectives, investments across the eight categories and components included in this document can be mutually reinforcing and should be considered jointly.

The CROE uses terms and abbreviations which are defined in Annexes 1 and 2. In addition, Annex 3 provides a description of the roles and responsibilities of the Senior Executive/CISO function.

2. CYBER RESILIENCE OVERSIGHT EXPECTATIONS

2.1. GOVERNANCE

2.1.1 Governance - Preamble

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

Strong cyber governance is essential to an FMI's implementation of a systematic and proactive approach to managing the prevailing and emerging cyber threats that it faces. It also supports efforts to appropriately consider and manage cyber risks at all levels within the organisation and to provide appropriate resources and expertise to deal with these risks. This chapter provides guidance on what basic elements an FMI's cyber resilience framework should include and how an FMI's governance arrangements should support that framework.

2.1.2. Governance - Expectations

2.1.2.1. Cyber resilience strategy and framework

BASELINE

Cyber resilience strategy:

1. The FMI should establish an internal, cross-disciplinary steering committee comprised of senior management and appropriate personnel from multiple business units (e.g. business, finance, risk management, internal audit, operations, information security, information technology, communications,

legal, HR and organisation) to collectively develop a cyber resilience strategy and framework. The steering committee should provide multiple views and perspectives to ensure that the cyber resilience strategy and framework is holistic and focuses on all elements related to people, processes and technology. Amongst other things, the steering committee should:

a. Evaluate the needs and expectations of internal and external stakeholders, prioritising these and deciding on the overall requirements from cyber resilience;
b. Provide direction to senior management about what cyber resilience should achieve;
c. Define who makes cyber resilience decisions and how those decisions should be made;
d. Consider the FMI's risk landscape and risk tolerance when defining how cyber risks should be addressed;
e. Evaluate how the different business units are impacted, and can work together in an integrated manner to achieve enterprise-wide outcomes; and
f. Consider how to monitor the performance and outcomes of cyber resilience and intervene if necessary to ensure that the specified direction is followed.

2. Based on the above reflections, the FMI should document its cyber resilience strategy. The FMI should ensure that the following aspects are considered and included in the strategy:
    a. The importance of cyber resilience to the FMI and its key stakeholders;
    b. The high-level requirements of internal and external stakeholders, so that these can be taken into account when defining governance of cyber resilience and goals for cyber resilience management. Some common categories of stakeholders that may be considered include: owners and investors, customers and clients, suppliers, employees, legal and regulatory authorities and competitors and industry bodies;
    c. The vision and mission of the FMI in relation to cyber resilience;
    d. The cyber resilience objectives that the FMI will work towards, which should include ensuring the ongoing efficiency, effectiveness and economic viability of its services to its users and maintaining and promoting the FMI's ability to anticipate, withstand, contain and recover from cyber attacks;

e. The FMI's cyber risk appetite to ensure that it remains consistent with the FMI's risk tolerance, as well as with the FMI's overall business objectives and Corporate Strategy;
f. Clear and credible target states of cyber maturity and a roadmap/implementation plan, with change delivery and planning of capabilities across people, processes and technology at pace with threats and proportionate to the size and criticality of the FMI. The strategy should clearly set out how this roadmap/implementation plan will be delivered and how delivery should be tracked and monitored by Board;
g. Which assets will be used to manage cyber resilience and how performance of these assets can be optimised;
h. The governance that is needed to enable cyber resilience to be designed, transitioned, operated and improved;
i. How cyber resilience initiatives will be delivered, managed and funded, including the budgeting process and organisational capabilities; and
j. How cyber resilience will be integrated into all aspects of the FMI, which includes people, processes, technology and new business initiatives.

3. The FMI should ensure that the cyber resilience strategy is aligned to its Corporate Strategy.
4. If an FMI has an IT Strategy, it should ensure that it is aligned to the cyber resilience strategy, as set out above.
5. The FMI's Board should approve the cyber resilience strategy, and should ensure that it is regularly reviewed and updated according to the FMI's threat landscape.
6. The Board should be regularly apprised of the FMI's cyber risk appetite to ensure that it remains consistent with the FMI's risk tolerance, as well as the FMI's overall business objectives and Corporate Strategy.

Cyber resilience framework:

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

8. The FMI's cyber resilience framework should systematically incorporate the requirements (i.e. policies, procedures and controls) related to governance, identification, protection, detection, response and recovery, testing, situational awareness and learning and evolving.
9. The FMI should use leading international, national and industry-level standards, guidelines or recommendations, reflecting current industry best practices in managing cyber threats, as a benchmark in designing its cyber resilience framework and incorporating the most effective cyber resilience solutions.
10. At the broader level, the FMI's cyber resilience framework should be consistent with its enterprise risk management framework.
11. The FMI's Board should endorse this cyber resilience framework, ensuring it is aligned with the FMI's formulated cyber resilience strategy, and review and update it, at least annually, to ensure that it remains relevant.
12. The FMI's cyber resilience framework should clearly define the roles and responsibilities including accountability for decision-making within the organisation for identifying, mitigating and managing cyber risk.

Cyber resilience strategy and framework:

INTERMEDIATE

13. The FMI should use relevant metrics and maturity models to assess and measure the adequacy and effectiveness of and adherence to its cyber resilience framework through independent compliance programmes and audits carried out by qualified individuals, on a regular basis.
14. The FMI should ensure that, as part of its formal process to review and update its cyber resilience strategy and framework (including all policies, procedures and controls), a number of factors are considered, such as:
    a. The current and evolving cyber threats (e.g. those associated with the supply chain, use of cloud services, social networking, mobile applications and the Internet of Things (IoT));
    b. Threat intelligence on threat actors and new tactics, techniques and procedures which may specifically impact the FMI;
    c. The results of the risk assessments of the FMI's critical functions, key roles, processes, information assets, third-party service providers and interconnections;

d. Actual cyber incidents which directly impacted the FMI or external cyber incidents from the ecosystem;
e. Lessons learned from audits and tests on the cyber resilience framework;
f. Performance of the FMI against the relevant metrics and maturity models; and
g. New business developments and future strategic objectives.

Cyber resilience strategy and framework:

ADVANCED

15. The cyber resilience strategy should outline the FMI's future state of cyber resilience, in terms of maturity, with short-term and long-term perspectives, and senior management should continuously improve and adapt the existing cyber resilience strategy and framework as the desired maturity level changes.
16. The FMI's cyber resilience strategy and framework should consider how the FMI would continuously review and proactively identify, mitigate and manage the cyber risks that it bears from and poses to its participants, other FMIs, vendors, vendor products and its service providers, which are collectively referred to as an FMI's ecosystem.
17. The FMI should establish the appropriate structures, processes and relationships with the key stakeholders in the ecosystem to continuously and proactively enhance the cyber resilience of the ecosystem and promote financial stability objectives as a whole.

2.1.2.2. Role of the board and senior management

BASELINE

Board and management responsibilities:

18. The FMI's Board should be responsible for approving the cyber resilience strategy and framework, setting the FMI's risk tolerance for cyber risks and closely overseeing the FMI's implementation of its cyber resilience framework, and the policies, procedures and controls that support it.

19. In order to discharge the aforementioned responsibilities, the FMI's Board should ensure that it collectively possesses the appropriate balance of skills, knowledge, and experience to understand and assess cyber risks facing the FMI, and is sufficiently informed and capable of posing credible challenge to the recommendations and decisions of designated senior management.
20. The Board and senior management should ensure that a senior executive (e.g. Chief Information Security Officer) is responsible and accountable for the implementation of the cyber resilience strategy and framework at the enterprise level. The senior executive should be independent, possess the appropriate balance of skills, knowledge and experience, have sufficient resources and report directly to the Board. For further clarification on the possible roles and responsibilities of such a Senior Executive, please refer to Annex 3.
21. The Board and senior management should ensure that personnel (including senior management), responsible for cyber activities, have suitable skills, knowledge, and experience, and are sufficiently informed and empowered to make timely decisions.
22. The Board and senior management should ensure that cyber risk, implementation of the cyber resilience framework, and any associated issues are regularly on the Board agenda. Boards should have adequate access to cybersecurity expertise, and discussions about cyber risk management should be given adequate time on the Board meeting agenda.
23. Senior management should regularly provide a written report on the overall status of its cyber resilience programme and keys risks and issues to the Board.
24. As part of the Board updates, senior management should provide their budgeting and forecasting activities plan for ongoing and future resource needs to ensure continual achievement of cyber resilience objectives.

Culture:

25. The Board and senior management should cultivate a strong level of awareness of and commitment to cyber resilience. To that end, an FMI's Board and senior management should promote a culture that recognises that staff at all levels have important responsibilities in ensuring the FMI's cyber resilience, and lead by example.

26. The Board and senior management should ensure that behavioural and cultural change is nurtured and conveyed through leadership and vision, with clear and effective messages such as: “Cyber resilience is everyone’s duty”. This could be executed throughout the FMI, possibly built into charters, vision statements and mandates from senior management, or through Cyber Awareness Campaigns.
27. Senior management should ensure that situational awareness materials are made available to employees when prompted by highly visible cyber incidents or by regulatory alerts. For example, the FMI could send internal emails about cyber events or post articles on its intranet site.

Skills and accountability:

28. Senior management should ensure that it has a programme for continuing cyber resilience training and skills development for all staff. This training programme should include the Board members and senior management and should be conducted at least annually. The annual cyber resilience training should include incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security) and emerging issues.
29. Senior management should ensure that employees and contractors, with privileged account permissions and/or which have access to sensitive assets and information, receive additional cyber resilience training commensurate with their levels of responsibility, and business units are provided cyber resilience training relevant to their particular business risks.
30. In order to implement the cyber resilience strategy and framework, senior management should ensure that it identifies the competencies, skills and resources required. Senior management should adopt well known skills frameworks, such as the European e-Competence Framework (e-CF) or the Skills Framework for the Information Age (SFIA) to determine its organisational needs.
31. Senior management should continuously review the skills, competencies and training requirements to ensure that it has the right set of skills as technologies and risks evolve.

INTERMEDIATE

Board and management responsibilities:

32. The FMI should ensure that the Board members' and senior managements' understanding of their roles and responsibilities with regard to cyber resilience is regularly assessed, including their knowledge of cyber risks.
33. The Board should ensure that senior management regularly conducts a cyber resilience self-assessment[2], which evaluates the FMI's cyber maturity. The Board should review the self-assessment and take appropriate decisions to improve the effectiveness of cyber activities and integration with the Corporate Strategy across the FMI.
34. The Board should review and approve senior management's prioritisation and resource allocation decisions based on the results of the cyber (self-) assessments, performance against Key Performance Indicators (KPIs) and their evolution against their target state of maturity, and the FMI's overall business objectives.

Culture:

35. Senior management should establish and sustain incentives (e.g. Staff Recognition Awards) to ensure behaviours are consistent with the intended cyber risk culture.
36. Senior management should produce a formal Cyber Code of Conduct and ensure that all employees comply with it.
37. Senior management should validate the effectiveness of its cyber resilience training programme (e.g., social engineering or phishing tests) and assess whether training and awareness programmes positively influence behaviour. Based on the lessons learned from its training programme, the FMI should improve the employee awareness programmes.
38. Senior management should develop key performance metrics (e.g. KPIs) and key risk metrics (e.g. Key Risk Indicators (KRIs)) and markers (both quantitative and qualitative) and ensure supporting data is routinely collected

[2] The FMIs may use the Cyber Resilience Oversight Expectations (CROE) as the basis for their self-assessments.

at the senior management level to monitor, measure, and report on the implementation, effectiveness, consistency and persistence of cyber activities.

Skills and accountability

39. Senior management should embed a programme for talent recruitment, retention, and succession planning for the cyber resilience staff, and ensure such staff are aligned to cyber activities and deployed effectively across the FMI.
40. Senior management should ensure there are well-defined plans for succession of high risk staff, and recruitment for key cyber roles require suitable cyber skills, knowledge and experience in alignment with defined succession plans.
41. Senior management should ensure that staff performance plans are tied to compliance with cyber resilience policies and standards in order to hold employees accountable.

ADVANCED

Board and management responsibilities:

42. The FMI should institute a dedicated cyber expert within the Board.
43. The standard Board meeting package should include reports and metrics that go beyond events and incidents to address threat intelligence trends for the ecosystem and facilitate discussions on how the FMI should respond accordingly.
44. The Board and senior management should pro-actively make enhancements to its strategic goals, objectives, and tactical plans, as needed, to support cyber activities and improvements across the ecosystem, leveraging any available sector-defined requirements and coordinated initiatives, and clearly communicate this to the relevant stakeholders.

Culture:

45. Senior management should proactively cooperate with other stakeholders to promote a cyber resilience culture across the ecosystem.
46. Senior management should ensure that cyber resilience awareness information is provided to its participants (including banks and ancillary systems) regularly.

Skills and accountability:

47. Senior management should regularly benchmark its cyber resilience capabilities against the market to identify its gaps, in terms of governance, skills, resources and tools; treat these as cyber risks; and address them accordingly.
48. Senior management should actively foster partnerships with industry associations and cybersecurity practitioners to develop solutions for future cyber resilience needs, which will be useful to the FMI and the ecosystem as a whole.

2.2. IDENTIFICATION

2.2.1 Identification - Preamble

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

2.2.2. Identification - Expectations

BASELINE

1. The FMI should identify and document all its critical functions, key roles, processes and information assets that support those functions, and keep this updated on a regular basis.
2. The FMI should identify and document all business processes that are dependent on third-party service providers and identify its interconnections, and keep this updated on a regular basis.
3. The FMI should maintain an updated inventory of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections. The FMI should integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its inventory.
4. The FMI should have a risk management framework to identify risks and to conduct risk assessments, on a regular basis, of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections to determine, classify and document their level of criticality.
5. The FMI should create and maintain a simplified network map of network resources, with associated IP addressing plan, that locate routing and security devices, servers supporting the FMI's critical functions, and that identify links with the outside world.
6. The FMI should conduct risk assessments before the deployment of new and/or updated technologies, products, services, and connections to identify

potential threats and vulnerabilities. It should also update its risk assessment in case new information affecting information security risks is identified (e.g. a new threat, vulnerability, adverse test result, hardware change, software change, or configuration change). The results of the risk assessments should feed into the cyber resilience strategy and framework.

7. The FMI should have and maintain an exhaustive inventory of all individual and system accounts (especially including privileged ones and remote access accounts) to know the access rights to information assets and their supporting systems. The FMI should review and keep this inventory updated on a regular basis.

INTERMEDIATE

8. The FMI should use automated, centralised Asset Inventory Management (AIM) tools that enable it to support the identification and classification of the critical functions, processes, information assets and interconnections. The FMI should ensure that the inventory is updated accurately and in a timely manner. The tools should be able to automatically send alerts in case of changes in the FMI's inventory.
9. The FMI should use automated, centralised Identity and Access Management (IAM) tools that enable it to support the identification and classification process of roles, user profiles, individual and system credentials, and ensure that these are updated accurately and in a timely manner. The tools should be able to automatically send alerts in case of changes.
10. In the use of the AIM and IAM, the FMI should define and establish criteria and rules to identify unexpected changes that need further investigation.
11. The FMI should also maintain current and complete maps of network resources, interconnections and dependencies, and data flows with other systems or assets, including the connections to business partners, the internet-facing services, cloud services and any other third-party systems. The FMI should use these maps to undertake risk assessments of key dependencies and apply appropriate risk controls, when necessary.
12. FMIs should continuously monitor connections among assets and cyber risk levels throughout the life cycle of the assets, and store and analyse these data. The information gathered this way should enable the FMI to support

timely responses to cyber threats (including insider threats) or vulnerabilities and investigation of anomalous activities.

13. The FMI should update its asset inventory, including the critical assets, to address new, relocated, repurposed and sunset assets, on a regular basis or when these changes occur.

ADVANCED

14. The FMI should identify emerging risks in real time, and use automated feeds from above (i.e. AIM and IAM), in order to continuously update its risk assessments and take the necessary mitigating actions, in a timely manner and in line with the FMI's risk tolerance.
15. The FMI should identify the cyber risks that it bears from entities/poses to entities in its ecosystem and coordinate with relevant entities, as appropriate. This should entail identifying common vulnerabilities and threats, and taking appropriate measures collectively to address such risks, with the objective of improving the overall resilience of the ecosystem.

2.3. PROTECTION

2.3.1. Protection - Preamble

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

2.3.2. Protection - Expectations

2.3.2.1. Protection of processes and assets

2.3.2.1.1. Control implementation and design:

BASELINE

1. The FMI should implement a comprehensive and appropriate set of security controls that will allow it to achieve the security objectives needed to meet its business requirements. The FMI should implement these controls based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections, as per the risk assessment in *Identification*. These security objectives may include:
    a. Ensuring the continuity and the availability of its information systems and data.
    b. Ensuring the integrity of the information stored in its information systems and while in transit.
    c. Ensuring sensitive data protection and confidentiality while at rest and while in transit.
    d. Ensuring the conformity to applicable laws, regulation and standards.

2. The FMI should develop its security controls in order to address cyber security and related physical security and people security. The controls should be designed according to the threat landscape, prioritised in accordance with the risks facing the FMI (risk-based security controls), and aligned to its business objectives.

3. The FMI should regularly assess the effectiveness of its security controls in order to adapt them to its moving threat landscape. They should be monitored and audited regularly to ensure that they remain effective and that they have been applied to all assets where they might be needed.
4. When designing and developing its systems and processes, the FMI should capture security requirements alongside system and process requirements in order to identify at the earliest stage security controls necessary for protecting its systems, processes and data.
5. The FMI should apply a defence-in-depth strategy, i.e. it should implement multiple independent security controls to provide redundancy, so that if one control fails or a vulnerability is exploited, alternative controls will be able to protect targeted assets and/or processes.

INTERMEDIATE

6. The FMI should develop and implement a bespoke information security management system (ISMS) based on well-recognised international standards (e.g. ISO 27001, ISO 20000-1, etc.), in order to establish, implement, operate, continuously monitor, review, maintain and improve a comprehensive information security control framework.
7. The FMI should consider cyber resilience at the earliest stage of system design, development and acquisition, as well as throughout the system development lifecycle, so that vulnerabilities in software and hardware are minimised and security controls incorporated into systems and processes from their inception. It should adopt a bespoke system development life cycle (SDLC) methodology that embeds the resilience by design approach when designing, building, acquiring or modifying its systems, processes and products. At each step of the SDLC, the FMI should manage its cyber risk and integrate resilience based on the risk analysis results.

ADVANCED

8. The FMI should seek certification of its ISMS, which is based on well-recognised international standards.
9. The FMI should develop processes and procedures to constantly and automatically adjust and refine its security countermeasures (controls) to ensure protection against known and emerging threats. Its security controls'

design and implementation should be data driven to move from reactive to predictive responses to cyber attack, using real time information on threats, vulnerabilities and operational changes.

10. The FMI should actively cooperate with other FMIs across the ecosystem, share their knowledge and best practices to analyse and design necessary protective controls dedicated to the financial ecosystem as a whole. The FMI should use threat intelligence to help identify forthcoming or real attacks and strengthen its protective controls accordingly.

2.3.2.1.2. Network & Infrastructure Management:

BASELINE

11. The FMI should establish a secure boundary that protects its network infrastructure, using network perimeter defence tools such as router, firewall, IPS/IDS, proxies, VPN, DMZ, etc. The boundary should identify trusted and untrusted zones according to the risk profile and criticality of assets contained within each zone, and appropriate access requirements should be implemented within and between each security zone according to the principle of least privilege.
12. The FMI should seek to use a separated and dedicated network for information system administration. At a minimum, the FMI should prohibit, whenever possible, direct internet access from devices or servers used for information system administration.
13. The FMI should establish baseline system and security configurations for information systems and system components, including devices used for accessing the FMI network remotely, to facilitate the consistent application of configuration to and security hardening of those systems and components. These baselines should be documented, formally reviewed and regularly updated to adapt them to the FMI's moving threat landscape.
14. The FMI should harden its network infrastructure and information systems using recognised industry security standards. Changes to system configurations should be strictly controlled and monitored, and programmes that can alter or override system configuration should be restricted. This should also be applicable to devices and environments used for accessing the FMI network remotely.

15. The FMI should seek to use secure network protocols (e.g. SSH, protocols relying on TLS or equivalent) when they exist in order to guarantee the confidentiality and integrity of information exchanged within its network and beyond, including remote connections.
16. The FMI should define and implement procedures that limit, lock and terminate system and remote sessions after a pre-defined period of inactivity and predefined conditions are met.
17. The FMI should activate and configure local firewalls on workstations and endpoint systems, including devices used for accessing the FMI network remotely to block by default administration ports except from explicitly identified devices (e.g. administration).
18. The FMI should implement intrusion detection/prevention systems (e.g. IDS/IPS) and endpoint security solutions (e.g. antivirus, firewall, and HIDS/HIPS), in particular on devices and environments used for accessing the FMI network remotely, to detect and block actual and attempted attacks or intrusions.
19. The FMI should implement controls that prevent non-controlled devices to connect to its internal network (e.g. personal devices, rogue access point, etc.) and endpoints (e.g. removable media), from inside the premises or outside (e.g. remote connections). The FMI's infrastructure should be regularly scanned to detect rogue devices and access points.
20. The FMI should regularly scan its legacy technologies to identify potential vulnerabilities and seek upgrade opportunities. Controls and additional defence layers should be implemented and tested in order to protect unsupported systems.
21. The FMI should use applications that have been developed following secure development practices and that meet a prudent level of security. It should develop security control requirements for all applications, whether they were acquired or developed internally.
22. The FMI should have policies and controls that prevent users from installing unauthorised applications. Procedures should be in place to manage the installation of application.

INTERMEDIATE

23. The FMI should implement a defence-in-depth security architecture, based on the network and data flow diagrams that identify hardware, software and network components, internal and external connections, and type of

information exchanged between systems. As required in Identification, the FMI should maintain current and complete network and data flow diagrams.

24. The FMI should segment its network infrastructure with security policies appropriate to its use and commensurate to its risk score, which define proper access policy to systems and applications. Sensitive traffic between systems and zones should be segregated using network management.
25. The FMI's IT environments and functions should be adequately separated, with different security levels and controls implemented.
26. The FMI should implement technical measures to prevent the execution of unauthorised code on institution-owned or managed devices, network infrastructure and system components. The FMI should consider implementing technical measures such as Network Access Control (NAC) solutions in order to prevent the successful connection of unauthorised devices.
27. The FMI should employ automated mechanisms to help maintain an up-to-date, complete, accurate and readily available baseline of system and security configurations for the information system and system components. These mechanisms might include hardware and software inventory tools, configuration management tools and network management tools.

ADVANCED

28. The FMI's infrastructure should be engineered to block or at least limit the effects of a cyber attack on production environments. It should implement automated controls based on the risk scores of its infrastructure assets, and it should be able to automatically disconnect or isolate affected assets in the case of an adverse event.
29. In the context of a defence-in-depth strategy, the FMI should seek to implement cyber deception capabilities and techniques that enable it to lure the attacker and trap it to a controlled environment where all activities can be contained and analysed, allowing the FMI to gain vital threat intelligence that will help to improve its protection controls.

2.3.2.1.3. Logical & Physical security management

BASELINE

30. The FMI should identify and restrict physical and logical access to its system resources to the minimum required for legitimate and approved work activities, according to the principle of least privilege.
31. The FMI should establish policies, procedures and controls that address access privileges and how that access should be administered. The information system access should be regularly evaluated to identify unneeded access or privileges. Physical, logical and or remote access to high-risk or confidential systems should be restricted, logged and unauthorised access should be blocked. Administration rights on systems should be strictly limited to operational needs. Procedures should be in place for a periodic review of all access rights.
32. The FMI should establish and administer user accounts in accordance with a role-based access control (RBAC) scheme that organises allowed information system access rights and privileges into roles. Role assignments should be regularly reviewed by appropriate personnel (e.g. management, system owners, etc.) in order to take appropriate action when privileged role assignments are no longer appropriate.
33. The FMI should establish processes to manage the creation, modification or deletion of user access rights. Such actions should be submitted to and approved by appropriate personnel, and should be recorded for review if necessary.
34. The FMI should implement specific procedures to allocate privileged access on a need-to-use or an event-by-event basis. Administrators should have two types of accounts: one for general purpose and one to carry out their administrative tasks. The use of privileged accounts should be tightly monitored and controlled. The use of generic accounts for administration purpose should be strictly limited and traced. Whenever possible, user and administrator accounts should be nominative and clearly identifiable (e.g. using dedicated taxonomy for usernames).
35. The FMI should have a dedicated password policy that specify password characteristics such as complexity, renewal period, and limits to password attempts and reuse. Default authentication settings (e.g. passwords and unnecessary default accounts) should be deactivated, changed or removed before systems, software and/or services go live.

36. The FMI should develop appropriate controls (e.g. end-to-end encryption, authentication and access control) to protect data at rest, in use and in transit. The controls should be commensurate to the criticality and the sensitivity of the data held, used or being transmitted, as per the risk assessment conducted in *Identification*.
37. The FMI should have dedicated controls to prevent unauthorised access to cryptographic keys. Dedicated policy and procedures should be defined for the management of and access to cryptographic materials.

INTERMEDIATE

38. The FMI should implement technical controls that trigger automated notification to appropriate personnel whenever user access permissions change. Controls should be in place to prevent unauthorised escalation of user privileges.
39. The FMI should adopt encryption of data as a result of its data classification and risk assessment processes.
40. The FMI should implement automated mechanisms to support the management of information system access accounts. These might include the implementation of security controls embedded in the information system allowing it to automatically disable and/or remove inactive, temporary and emergency accounts after a predefined period of time.

ADVANCED

41. The FMI should establish strong governance on identity and access management enforced by the use of dedicated tools such as Identity and Access Management (IAM) or Governance, Risk and Compliance (GRC) tools, in an integrated way, ensuring all systems update each other consistently.
42. The FMI should use an Attribute-Based Access Control (ABAC) paradigm that allow it to, contextually and dynamically, manage the access to its IT environment.
43. The FMI should employ automated mechanisms that allow a continuous audit and monitoring of account creation, modification, enabling, disabling and removal actions, in order to notify appropriate personnel when potential

malicious behaviour or damage is detected. The FMI should implement adaptive access controls to prevent potential malicious behaviour or damage.

2.3.2.1.4. Change & patch management:

BASELINE

44. The FMI should have in place policies, procedures and controls for change management, which should include criteria for prioritising and classifying the changes (e.g. normal vs emergency change). Prior to any change, the FMI should ensure that the change request is:
    a. reviewed to ensure that it meets FMI business needs;
    b. categorised and assessed for identifying potential risks and to ensure that it will not negatively impact confidentiality, integrity and availability, and the FMI's systems and data; and
    c. approved before implementation by the appropriate level of management.

45. The FMI should ensure that the Information Security team is involved throughout the lifecycle (beginning to end) of the change management process.
46. The FMI should put in place necessary procedures (e.g. code review, unit testing, etc.) guaranteeing that changes are implemented correctly and efficiently. The FMI should employ best practices when implementing changes.
47. The FMI should test, validate and document changes to the information system before implementing them into production (e.g. this might include integration tests, non-regression tests, user acceptance tests, etc.). The changes to information systems include, but are not limited to, modification of hardware, software or firmware components, system and security configuration settings. The FMI should ensure that processes are in place to schedule change implementation and communicate to those impacted prior to implementation, including consulting them when necessary.
48. The FMI should have processes to identify, assess and approve genuine emergency changes. Post implementation reviews should be conducted to validate that emergency procedures were appropriately followed and to determine the impact of the emergency change.

49. The FMI should have a comprehensive patch management policy and processes that include: the maintenance of current knowledge of available patches, the identification of appropriate patch for particular systems and the analysis of impacts if installed, the assurance that patches are installed properly (e.g. by applying the four eyes principle), and tested prior and after installation, the documentation of all associated procedures, such as specific configurations required. The policies, procedures and controls must leverage on the asset inventory management process described in the *"Identification"* phase that provides information on the installed programs and binaries.
50. The FMI should consider using standardised configuration of IT resources to facilitate its patch management process.
51. The FMI should ensure that the installations of new patches have prior approval from the appropriate level of management.
52. The FMI should have in place necessary procedures for recovering quickly when changes or patches fail. Any changes to the production environment must have an associated fall-back plan, when applicable.
53. The FMI should have policies and procedures to prohibit changes and patch installation to the information system, that have not been pre-approved.

INTERMEDIATE

54. The FMI should establish its change management process based on well-established and industry recognised standards and best practices (e.g. Information Technology Infrastructure Library).
55. The FMI should consider automatising, when possible, its patch management process for guaranteeing that all its systems remain consistently up to date.
56. The FMI should consider building segregated or separated environment that mirror the production environment, allowing rapid testing and implementation of changes and patches, and providing for rapid fallback when needed.

ADVANCED

57. The FMI should implement automated mechanisms to prohibit changes and patches installation to the information system that have not been pre-approved.

2.3.2.2. People management

2.3.2.2.1. Human resources security:

BASELINE

58. The FMI should embed information security at each stage of the employment life cycle, specifying security related actions required during the induction of each employee, their ongoing management and termination of their employment:
    a. Prior to employment, the FMI should carry out background security checks on all candidates (employee or contractors), commensurate to their future role and depending on the criticality of the assets and information they might have access to, in order to fulfil their duty. Responsibilities for information security should be clearly stated in the contractual agreement.
    b. During employment, the FMI should ensure that employees and contractors comply with established policies, procedures and controls. When an employee is changing responsibilities, the FMI should ensure that all the access related to its previous position and not necessary for its new responsibilities are revoked in due time. Employees that change responsibilities to roles requiring privileged access to critical systems or become high risk staff should be pre-screened. And on a more general level, the FMI should ensure that there is a process for carrying out recurrent background checks for all employees on a periodic basis, in line with local laws and regulations.
    c. The FMI should establish processes to revoke immediately the access of leavers. Upon termination of employment, internal and external individuals should be required to return all the assets that belong to the FMI including important documentation (e.g. related to business processes, technical procedures and contact details), equipment, software, authentication hardware, etc.
59. The FMI should establish policies, procedures and controls for granting/revoking employee physical and logical access to its systems based on job responsibilities, principles of least privilege and segregation of duties. Procedures for regularly reviewing such access should be in place.
60. The FMI should establish capabilities, including people, processes and technologies to monitor privileged user's activity and access to critical

systems in order to identify and deter anomalous behaviour and notify appropriate personnel.

INTERMEDIATE

61. The FMI should implement mechanisms that trigger, upon change to employment status, automated notification to appropriate personnel in charge of granting/revoking access to information system.
62. The FMI should implement mechanisms to automatically grant or revoke employee access to its information system upon change to employment status.

ADVANCED

63. The FMI should implement systems to monitor and analyse employee behaviour (e.g. network use patterns, work hours, known devices, etc.) to alert anomalous activities and evaluate the implementation of innovative solutions (e.g. data analytics, machine learning, AI, etc.) to support detection and response in real time to insider threats' activity.

2.3.2.2.2. Security awareness and training:

BASELINE

64. The FMI should ensure that its employees have a good understanding of the cyber risk they might face when conducting their job and that they understand their roles and responsibilities in protecting the FMI's assets.
65. On a regular basis, at least once a year, the FMI should provide training to its entire staff (employees and contractors) to support information security policy compliance and the incident reporting process. This training should include elements to maintain appropriate awareness of cyber-related risks and good practices for dealing with potential cyber incidents including how to report unusual activity. Information security awareness training should be part of the on-boarding programme for newcomers.
66. The FMI should ensure that high-risk staff (e.g. management, system administrator, software developer, etc.) receive dedicated security awareness training as relevant for their responsibilities.
67. Prior to going into service operations, staff operating new systems, should receive appropriate user training and be familiar with the operating procedures.

INTERMEDIATE

68. The FMI should validate the effectiveness of its training (e.g. social engineering or phishing tests) and assess whether the training and awareness positively influence behaviour and ensure that staff comply with information security policy and the incident reporting process.

ADVANCED

69. FMI's senior management should ensure a continuous improvement of cyber risk cultural awareness across the organisation and its ecosystem. Training programmes should be regularly updated to take into account the evolving threat landscape of the ecosystem.

2.3.2.3. Supplier and third-party security management

BASELINE

70. The FMI should maintain and regularly update an inventory of its participants and third-party service providers, and ensure that its cyber resilience framework addresses its interconnections with the aforementioned entities from a cyber risk perspective.
71. The FMI's third-party risk assessment should be carried out regularly, taking into account the evolution of its threat landscape. The FMI should ensure that the provision of outsourced services are accorded the same level of cyber resilience as if they were provided by the FMI itself.
72. The FMI should assess the third-party service provider's security capabilities at least through third-party self-assessment (e.g. self-assessment against Annex F[3]). Provision of settlement services to ancillary systems by overseen entities is not considered to be third-party service provision.

INTERMEDIATE

73. The FMI should automate its inventory of participants, third-party service providers and interconnections, for example, through the use of its

[3] https://www.bis.org/cpmi/publ/d101a.pdf (Pages 170-171).

Governance, Risk and Compliance (GRC) tools, and ensure that it receives trigger alerts to any changes.

74. The FMI should design security controls, which detect and prevent intrusions from third-party connections.
75. The FMI should ensure that there are appropriate procedures in place to isolate or block its third-party connections (in a timely manner), if there is a cyber attack and/or a risk of contagion.
76. The independent audit function should validate the FMI's third-party relationship management and outsourcing.
77. The FMI should obtain assurance of the third-party service provider's cyber resilience capabilities, and may use tools such as certification, external audits (e.g. ISAE3402), summary of test reports, SLAs, KPIs, etc.

ADVANCED

78. The FMI should work closely with its third-party service providers and other FMIs in the ecosystem to maintain and improve the security of interconnections and end-point security. For example, the FMI could conduct response and recovery tests with its third-party service providers and other FMIs.

2.4. DETECTION

2.4.1. Detection - Preamble

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

2.4.2. Detection - Expectations

BASELINE

1. Based on the risk assessment performed in *Identification*, the FMI should define, consider and document the baseline profile of system activities to help detect deviation from the baseline (e.g. anomalous activities and events).
2. The FMI should develop the appropriate capabilities, including the people, processes and technology, to monitor and detect anomalous activities and events, by setting appropriate criteria, parameters and triggers to enable alerts.
3. The FMI should have capabilities in place to monitor user activity, exceptions, faults and information security events.
4. The FMI should have capabilities in place to monitor connections, external service providers, devices and software.
5. The FMI should analyse the information collected and use it to further enhance its detection and monitoring capabilities, and incident response process.
6. The FMI should ensure that its detection capabilities, baseline profile of system activities and the criteria, parameters and triggers are periodically reviewed, tested and updated appropriately.

7. The FMI should ensure that its staff are trained to be able to identify and report anomalous activity and events.
8. The FMI should build multi-layered detection controls covering people, processes and technology which support quick attack detection and isolation of infected points.
9. The FMI should ensure that its detection capabilities are informed by threat or vulnerability information, which can be collected from different sources and providers, as set out in the chapter on *Situational Awareness*.
10. The FMI should define alert thresholds for its monitoring and detection systems in order to trigger and facilitate the incident response process.
11. The FMI's monitoring and detection capabilities should support information collection for the forensic investigation. To facilitate forensic investigation, the FMI should ensure that its logs are backed up at a secure location with controls in place to mitigate the risk of alteration.

INTERMEDIATE

12. The FMI should develop and implement a Security Information and Event Management system (SIEM), which provides automated mechanisms to correlate, across its business units, all the network and system alerts and any other anomalous activity in order to detect and prevent multifaceted attacks (e.g. simultaneous account takeover and DDOS attack).
13. The FMI should have a process to collect, centralise and correlate event information from multiple internal sources and log analysis to continuously monitor the IT environment and detect anomalous activities and events. This should include information on anomalous activity and other network and system alerts across business units. This capability could be achieved through a Security Operation Centre (SOC) or equivalent.
14. The FMI should have processes in place to monitor activities which are not in line with its security policy and might lead to data theft or destruction.
15. The FMI's monitoring and detection capabilities should allow the automatic alert of the appropriate staff who can respond.
16. The FMI should have the capabilities, in collaboration with other stakeholders, to detect cyber events and swiftly adapt its security controls. Such events may include attempted infiltration, movement of an attacker

across systems, exploitation of vulnerabilities, unlawful access to systems and exfiltration of information or data.

17. The FMI should continuously monitor and inspect the network traffic, including remote connections, and endpoint's configuration and activity for timely identification of potential vulnerabilities or anomalous events. The network traffic, including remote connections, and the endpoint configuration should be continuously compared with the expected traffic and configuration baseline profile and data flows.

ADVANCED

18. The FMI should use multiple external sources of intelligence, correlated log analysis, alerts, traffic flows, and geopolitical events to predict potential future attacks and attack trends, and proactively take the appropriate measures to improve its cyber resilience capabilities.
19. The FMI should develop intrusion detection capabilities to automatically detect and block the attacks in real time, including zero-day exploits. The intrusion detection capabilities should assist the FMI to proactively identify vulnerabilities and deficiencies in its protective measures.
20. The FMI should seek to implement deception mechanisms which trigger alerts and enable detection. For example, the FMI could create and place fictitious confidential data with alerting tags attached to it, which would trigger alerts and inform the FMI of potential malicious activity when accessed.

2.5. RESPONSE AND RECOVERY

2.5.1. Response and recovery - Preamble

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

2.5.2. Response and recovery - Expectations

2.5.2.1. Cyber resilience incident management

BASELINE

1. The FMI should, based on the Identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections, plan for how to operate in a diminished capacity or safely restore services over time based on services' relative priorities, and with accurate data. In order to make the best decisions about its recovery objectives following a cyber incident, the FMI must first define its Recovery Point Objectives (RPO) and its Recovery Time Objectives (RTO), commensurate to its business needs and systemic role in the ecosystem.
2. Based on expectation (1), the FMI should consider a range of different cyber scenarios, including extreme but plausible ones, to which they may be exposed, and conduct business impact analyses to assess the potential impact such scenarios might have on the FMI. The FMI should review its range of scenarios and conduct the business impact analysis, in line with the evolving threat landscape, on a regular basis.
3. The FMI should, based on the different cyber scenarios, develop a contingency plan that achieves recovery objectives, restoration priorities and determines the required capacities for continuous availability of the system. The plan should define roles and responsibilities, and set out options to re-route or substitute critical functions and/or services that may be affected for a significant period by a successful cyber attack.

4. The FMI should develop comprehensive cyber response, resumption and recovery plans, to manage cyber security events or incidents in a way that limits damage, prioritises resumption and recovery actions in order to facilitate the processing of critical transactions, increases the confidence of external stakeholders, and reduces recovery time and costs. Such plans should define policies and procedures, as well as roles and responsibilities for escalating, responding to, and recovering from cyber security incidents. The FMI should ensure all relevant business units (including Communications) are integrated into the plans.
5. The FMI should ensure that its incident response team has the requisite skills and training to address cyber incidents.
6. The FMI should define alert parameters and thresholds for detecting information security incidents, which trigger the incident management processes and procedures, including alerting and escalating to the appropriate personnel.
7. The FMI should regularly test its cyber contingency, response, resumption and recovery plans, against a range of different plausible scenarios, and ensure that the plans are approved by the Board.
8. The FMI should have processes and procedures in place for collating and reviewing information from its cyber security incidents and testing results in order to continuously improve its contingency, response, resumption and recovery plans.

INTERMEDIATE

9. The FMI's cyber incident response, resumption and recovery processes should be closely integrated with crisis management, business continuity and disaster recovery planning and recovery operations.
10. The FMI should implement an effective incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication and recovery. Such capability should allow the FMI to perform, at the early stage, analysis of cyber security incidents upon their detection, with minimal service disruption. This capability might include direct cooperative or contractual agreements with incident response organisations or providers to assist rapidly with mitigation effort.

11. The FMI should define and develop functional and security dependency maps of identified information system assets supporting critical functions to understand and prioritise their restoration order.
12. The FMI should be able to use lessons learned from real-life cyber attacks on the institution and its ecosystem to improve its contingency, response, resumption and recovery plans.
13. The FMI should consult with relevant external stakeholders (e.g. main participants, service providers and other FMIs) within the ecosystem to further enhance its contingency, response, resumption and recovery plans.
14. The FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a cyber disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Notwithstanding this capability to resume critical operations within two hours, FMIs should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, while taking into account the fact that completion of settlement by the end of day is crucial.
15. The FMI should continuously monitor, evaluate and consider technological developments and solutions in the market, which may enhance its contingency, response, resumption and recovery capabilities.

ADVANCED

16. The FMI should implement processes to improve continuously its cyber response, resumption and recovery plans, taking into account cyber threat intelligence feeds, information sharing with its ecosystem and lessons learned from previous events. The FMI should set KPIs to measure its performance in achieving its recovery time objectives and driving improvement in its response, resumption and recovery plans.
17. The FMI should consult, collaborate and coordinate with relevant external stakeholders (e.g. main participants, service providers and other FMIs) within the ecosystem to develop common contingency, response, resumption and recovery plans for cyber scenarios which may impact the ecosystem as a whole. The FMI should conduct regular scenario tests (e.g. industry-wide and FMI-specific simulation exercises), with the relevant external stakeholders.
18. The FMI should implement a Computer Security Incident Response Team (CSIRT) that is responsible for responding to security incidents and intrusions,

and coordinating activities amongst the relevant internal and external stakeholders. Such team should have the authority to direct the FMI to make the changes necessary to recover from the incident.

19. The FMI should establish and implement processes to manage cyber security incidents, and enable automated responses, triggered by pre-defined criteria, parameters and thresholds. For example, the FMI could develop configurable capability to isolate or disable automatically affected information systems if cyber attacks or security violations are detected.

2.5.2.2. Data integrity:

BASELINE

20. The FMI should develop a formal backup policy specifying the minimum frequency and scope of data, based on data criticality and the frequency that new information is introduced.
21. The FMI should develop backup and recovery methods and strategies to be able to restore system operations with a minimum downtime and limited disruption.
22. The FMI should backup regularly all data necessary to replay participants' transactions.
23. Backups should be protected at rest and in transit to ensure the confidentiality, integrity and availability of data. Backups should be tested regularly to verify their availability and their integrity.

INTERMEDIATE

24. The FMI should store backup copies in an alternate storage site which is not co-located with the operational system, with transfer rate consistent with actual recovery point objectives. The alternate storage site and backups should be safeguarded by stringent protective and detective controls.
25. The FMI's information systems should implement transaction recovery mechanisms for transaction-based systems, which might include transaction rollback and logging. The FMI should maintain transaction replay capability and conduct frequent periodic independent reconciliation of participants' positions.

26. The FMI should develop capabilities to restore information system components within the actual recovery time objectives using predefined, standardised configuration of IT resources, whose integrity is protected.

ADVANCED

27. The FMI's backup and recovery methods and strategies should be integrated into the FMI's system infrastructure at the development and/or acquisition phase.
28. The FMI should accomplish information system backup by maintaining a redundant secondary system that is not co-located with the primary system and that can be activated without loss of information or disruption to operations.
29. The FMI should consider having a data-sharing agreement with third parties and/or other stakeholders in order to obtain uncorrupted data from them for recovering its business operations in a timely manner and with accurate data.

2.5.2.3. Communication and collaboration

2.5.2.3.1. Contagion:

BASELINE

30. The FMI should identify, document and regularly review systems and processes supporting its critical functions and/or operations, which are dependent on external connectivity.
31. The FMI should have in place monitoring controls covering all external connections.
32. The FMI should develop policies and procedures that define how it should work together with relevant interconnected entities to enable the resumption of operations (the first priority being its critical functions and services) as soon as it is safe and practicable to do so.

INTERMEDIATE

33. The FMI should closely cooperate with its interconnected entities within the ecosystem establishing roll-back processes in order to restore all its services

in an accurate, safe manner. Moreover, the FMI should test the effectiveness of these procedures regularly.

ADVANCED

34. The FMI should implement real-time monitoring of external connections, coupled with interactive diagram(s) that shows real-time changes to the network connection infrastructure, volume fluctuation and alerts when risks arise.
35. The FMI should design its network connection infrastructure in a way that allows connections to be segmented or severed instantaneously to prevent contagion arising from cyber attacks.

2.5.2.3.2. Crisis communication and responsible disclosure:

BASELINE

36. The FMI should identify and determine employees that are essential for mitigating the risk of a cyber incident, and make them aware of their roles and responsibilities in incident escalation.
37. The FMI's incident response plan should identify the internal and external stakeholders that must be notified, as well as the information that has to be shared and reported, and when this should take place.
38. The FMI should establish criteria and procedures for escalating cyber incidents or vulnerabilities to the Board and senior management based on the potential impact and criticality of the risk.
39. The FMI should have a communication plan and procedures in place to notify, as required or necessary, all relevant internal and external stakeholders (including oversight, regulatory authorities, media and customers) in a timely manner, when the institution becomes aware of a cyber incident. The FMI should notify the appropriate internal and external stakeholders when a cyber incident occurs.
40. The FMI should have a policy and procedures to enable the responsible disclosure of potential vulnerabilities. In particular, the FMI should prioritise disclosures that could facilitate early response and risk mitigation by stakeholders for the benefit of the ecosystem and broader financial stability.
41. The FMI should establish and regularly review the information sharing rules, agreements and modalities in order to control the publication and distribution

of such information, and to prevent dissemination of sensitive information that may have adverse consequences if disclosed improperly.

INTERMEDIATE

42. The FMI should develop a range of cyber incident scenarios, based on the incident criteria established in *Baseline*. The FMI should thereafter develop dedicated incident response and communication plans for each of these scenarios. These incident response and communication plans should take into consideration the legal and regulatory reporting requirements at a jurisdictional level.

ADVANCED

43. The FMI should develop mechanisms to provide instantaneous notification of cyber incidents to its senior management, relevant employees and relevant stakeholders (including oversight and regulatory authorities) through multiple communication channels with tracking and verification of receipt. Such mechanisms should be based on predefined criteria and informed by scenario-based planning and analysis, as well as prior experience.

2.5.2.4. Forensic readiness

BASELINE

44. The FMI should identify the threat scenarios that might have a potential impact on its business and determine the cases which will require the collection of digital evidence, which includes the types of logs, for further forensic investigation.
45. The FMI should identify and document the digital evidence available on its systems, its location and understand how the evidence should be handled throughout its lifecycle.
46. The FMI should map the type and location of digital evidence to the different identified threat scenarios, which will be required to conduct a forensic investigation.
47. Based on 1), 2) and 3), the FMI should develop and implement a Forensic Readiness Policy approved by the Board and capability to support forensic

investigation, which also outlines the relevant system logging policies that include the types of logs to be maintained and their retention periods.

48. The FMI should develop procedures for securely collecting digital evidence in a forensically acceptable manner and in accordance with the requirements defined in the Forensic Readiness Policy.
49. The FMI should establish policies for securely handling and storing the collected digital evidence, ensuring their authenticity and integrity. The FMI should develop procedures to demonstrate that the integrity of the evidence is preserved whenever it is accessed, used or moved (i.e. chain of custody).

INTERMEDIATE

50. The FMI should closely integrate Forensic Readiness plans with incident management plans and other related business planning activities.
51. The FMI should establish procedures to assemble and collate the digital evidence for the purposes of supporting a forensic investigation or legal case, taking into account the requirements of the local jurisdiction. These procedures should describe how investigative staff should produce step-by-step documentation of all activities performed on digital evidence and their impact.
52. The FMI should train its staff, so that all those involved in an incident understand their role and are capable of adequately handling the digital evidence, ensuring its authenticity and integrity is not compromised and remains valid as per the requirements of the local jurisdiction. The FMI should ensure that staff involved in handling evidences have the appropriate degree of competence.

ADVANCED

53. The FMI should have a management review process that improves Forensic Readiness plans in accordance with experience and new knowledge.
54. The FMI should take an open and collaborative approach with the ecosystem to improve lawful forensic investigation and incident handling methodologies and tools.

2.6. TESTING

2.6.1. Testing - Preamble

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

Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the FMI's cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cyber resilience posture and reduce or eliminate identified gaps. This chapter provides guidance on areas that should be included in an FMI's testing and how results from testing can be used to improve the FMI's cyber resilience posture on an ongoing basis. The scope of testing for the purpose of this guidance includes vulnerability assessments, scenario-based testing, penetration tests and tests using red teams.

2.6.2. Testing - Expectations

BASELINE

1. The FMI should establish and maintain a comprehensive testing programme as an integral part of its cyber resilience framework. The testing programme should consist of a broad spectrum of methodologies, practices and tools for monitoring, assessing and evaluating the effectiveness of each component of the cyber resilience framework.
2. The FMI should adopt a risk-based approach in developing the comprehensive testing programme. This should be reviewed and updated on a regular basis taking into due account the evolving landscape of threats and the criticality of the information assets.
3. The FMI should develop appropriate capabilities and involve, if deemed necessary, all relevant internal stakeholders (including business lines and operational units) when implementing its testing programme.

4. The FMI should ensure that the tests are undertaken by independent parties, whether internal or external.
5. For continuous improvement of its cyber resilience posture, the FMI should establish policies and procedures to prioritise and remedy issues identified from the various tests and perform subsequent validation to assess whether gaps have been fully addressed.
6. The FMI's Board and Senior Management should incorporate lessons learned from the test results.
7. The FMI should test critical systems, applications and data recovery plans at least annually.
8. The FMI should test response, resumption and recovery plans including governance and the coordination and crisis communication arrangements and practices at least annually.
9. The FMI should test the information backups periodically to verify they are accessible and readable.

Vulnerability assessments:

10. The FMI should develop a documented and regularly updated vulnerability management process in order to classify, prioritise and remedy potential weaknesses identified in vulnerability assessments and perform subsequent validation to assess whether gaps have been fully addressed.
11. The FMI's vulnerability management process should support the identification of any type of exploitable weakness (technical, processual, organisational and emergent) in the critical functions, their supporting processes and the physical and logical assets where they reside.
12. The FMI should conduct vulnerability scanning for their external-facing services and the internal systems and networks on a regular basis.
13. The FMI should perform vulnerability assessments before any deployment/redeployment of new/existing services supporting critical functions, applications and infrastructure components for fixing bugs and weaknesses consistently with change and release management processes in place.
14. The FMI should periodically conduct vulnerability assessments on running services, applications and infrastructure components for compliance checks against regulations, policy and configurations as well as for monitoring and evaluating the effectiveness of security controls to address the identified vulnerabilities.

Scenario-based testing:

15. The FMI should perform different scenario-based tests, including extreme but plausible scenarios, to evaluate and improve its incident detection capability as well as response, resumption and recovery plans. Scenario-based tests can take the form of desktop exercises or cyber simulation.
16. The FMI's Board and Senior Management should be engaged in the scenario-based test, when appropriate.
17. To improve the FMI's staff awareness and enhance the risk culture within the organisation, the scenario-based tests should include social engineering and phishing simulation.
18. The FMI should test the adequacy of internal skills, processes and procedures to respond to unconventional scenarios, with a view to achieving stronger operational resilience.

Penetration tests:

19. The FMI should conduct penetration tests on their external-facing services and the internal systems and networks to identify vulnerabilities in the adopted technology, organisation and operations regularly, or at least on an annual basis. Penetration tests should be conducted whenever systems are updated or deployed.
20. The FMI should perform penetration tests, engaging all critical internal and external stakeholders in the penetration testing exercises: system owners, business continuity, incident and crisis response teams.

INTERMEDIATE

General:

21. The FMI should include testing practices as an integrated part of its enterprise risk management process with the aim of identifying, analysing and fixing cybersecurity vulnerabilities stemming from new products, services, or interconnections.
22. The FMI should develop capabilities to seek, analyse and use cyber threat intelligence to help inform and update its testing programme to ensure it is in line with the latest threat landscape, modus operandi of attackers and vulnerabilities.

23. The FMI should adopt best practices and automated tools to support processes and procedures in place to fix technical and organisational weaknesses identified during the testing exercises and to check for compliance with approved policy and configurations.
24. The FMI should perform security tests at all phases of the System Development Life Cycle (SDLC) and any level (Business, Application and Technology) for the entire application portfolio including mobile applications.

Vulnerability assessments:

25. The FMI should perform vulnerability scanning on an ongoing basis, rotating amongst environments in order to scan all environments throughout the year.

Scenario-based testing:

26. The FMI should test its response, resumption and recovery plans against cyber attack scenarios which include data destruction, data integrity corruption, data loss and system and data availability.
27. The FMI should use cybersecurity incident scenarios involving significant financial loss, as part of its stress testing process, to better understand potential spillovers and risk to its business model. The FMI should use such stress tests to further improve its risk management framework.

Penetration tests:

28. The FMI should design and perform penetration tests to simulate realistic attack techniques on systems, networks, applications and procedures.

Red-teaming tests:

29. The FMI should conduct red-teaming exercises to test *critical functions* for possible vulnerabilities and the effectiveness of an FMI's mitigating controls, including its people, processes and technology.
30. The FMI should perform red-teaming exercises using reliable and valuable cyber threat intelligence, based on specific and plausible threat scenarios.

31. The FMI should use the TIBER-EU framework[4], to conduct their red-teaming exercises.
32. The FMI should outsource the conduct of red-teaming exercises to external, third-party providers. Simultaneously, the FMI should build its internal processes and capabilities to undertake the externally outsourced exercise (e.g. establishing an internal White Team, developing incident escalation procedures, following appropriate methodologies and establishing robust risk management controls), as set out in the TIBER-EU framework.

ADVANCED

General:

33. The FMI should develop, monitor and analyse metrics to assess the performance and effectiveness of its testing programme. The FMI should use the analysis conducted to further improve its testing programme.
34. The FMI should regularly conduct tests in collaboration with its peers, participants and third parties.
35. The FMI should proactively engage in industry-wide tests in order to test cooperation and coordination protocols and communication plans. These exercises should foster the FMI's awareness on cross-sector cooperation and third-party risks.
36. The FMI should promote and participate in cross-sector cyber testing exercises to assess the soundness and security of its value chain as a whole.
37. The FMI should test, at least annually, the cooperation arrangements in place with relevant external entities (e.g. third-party security service providers, law enforcement agencies, CERTs/ISACs, etc.) in order to validate their effectiveness.
38. The FMI should share the test results with relevant stakeholders to boost the cyber resilience of its ecosystem and the financial sector as a whole, as far as possible and under specific information sharing arrangements.

[4] Link of TIBER-EU Guide to be inserted.

Vulnerability assessments:

39. The FMI should consider developing a Bug Bounty programme as part of its vulnerability management process, and have appropriate safeguards in place to manage the programme.

Scenario-based testing:

40. The FMI should conduct scenario-based tests that cover breaches affecting multiple portions of the FMI's ecosystem in order to identify and analyse potential complexities and interdependencies both at business and operational level which should be taken into account in the FMI's cyber resilience framework.
41. The FMI should collaborate with the ecosystem to develop cybersecurity incident scenarios involving significant financial loss and use them for stress tests to better understand potential spillovers and contagion risk to the ecosystem. The FMI should use such stress tests to further improve its cyber resilience posture, which contributes to the improvement of the resilience of the ecosystem as a whole.

Red-teaming tests:

42. In addition to periodic independent, external red-team exercises, the FMI should develop an internal red-team capability, with the appropriate methodologies, sophisticated tools and appropriately skilled personnel. The internal red-team test should regularly conduct red-team exercises and engage with the internal blue team, to transmit its findings and make improvements to the FMI's cyber resilience posture.

2.7. SITUATIONAL AWARENESS

2.7.1. Situational awareness - Preamble

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

2.7.2. Situational awareness - Expectations

2.7.2.1. Cyber threat intelligence

BASELINE

1. The FMI should identify cyber threats that could materially affect its ability to perform or to provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem.
2. The FMI should have capabilities in place to gather cyber threat information from internal and external sources (e.g. application, system and network logs; security products such as firewalls and intrusion detection systems; trusted threat intelligence providers; and publicly available information).
3. The FMI should belong or subscribe to a *threat and vulnerability information sharing source* and/or *information sharing analysis centre* that provides information on cyber threats and vulnerabilities. Cyber threat information gathered by the FMI should include analysis of tactics, techniques and procedures (TTPs) of real-life attackers, their modus operandi and information

on geopolitical developments that may trigger cyber attacks on any entity within the FMI's ecosystem.

4. The FMI should have the capabilities to analyse the cyber threat information gathered from different sources, while taking into account the business and technical characteristics of the FMI, in order to:
    a. Determine the motivation and capabilities of threat actors (including their TTPs) and the extent to which the FMI is at risk of a targeted attack from them;
    b. Assess the risk of technical vulnerabilities in operating systems, applications and other software, which could be exploited to perform attacks on the FMI;
    c. Analyse information security incidents experienced by other organisations, including types of incident and origin of attacks, target of attacks, preceding threat events and frequency of occurrence and determine the potential risk these pose to the FMI.
5. The FMI should analyse the information gathered above to produce relevant cyber threat intelligence, and continuously use it to assess and manage security threats and vulnerabilities for purpose of implementing appropriate cyber security controls in its systems and, on a more general level, enhancing its cyber resilience framework and capabilities on an ongoing basis.
6. The FMI should ensure that the gathering and analysis of the cyber threat information, and production of cyber threat intelligence, is regularly reviewed and updated.
7. The FMI should ensure that cyber threat intelligence is made available to appropriate staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels within the FMI.
8. The FMI should incorporate lessons learned from its analysis of the cyber threat information into the employee training and awareness programmes.

INTERMEDIATE

9. The FMI should continuously use its cyber threat intelligence to anticipate a cyber attacker's capabilities, intentions and modus operandi, and subsequently possible future attacks.

10. The FMI should develop a *Cyber Threat Risk Dashboard and Reports*, which uses the cyber threat information and intelligence, to outline, amongst other things:
    a. The most likely threat actors for the FMI;
    b. The TTPs that may be used by such threat actors;
    c. The likely vulnerabilities that may be exploited by such threat actors;
    d. The likelihood of attack from such threat actors and the impact on the confidentiality, integrity and availability of the FMI's business processes and to its reputation that could arise from such attacks;
    e. The impact of attacks already conducted by such threat actors on the ecosystem; and
    f. The risk mitigation measures that are in place to manage a potential attack.
11. The Cyber Threat Risk Dashboard and Reports should be continuously reviewed and updated in light of new threats and vulnerabilities, and discussed by the Board and senior management.
12. The FMI should include in its threat analysis those threats which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. The FMI should regularly review and update this analysis.

ADVANCED

13. The FMI should ensure that the scope of cyber threat intelligence gathering should include the capability to gather and interpret information about relevant cyber threats arising from the FMI's participants, service and utility providers and other FMIs, and to interpret this information in ways that allow the FMI to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems.
14. The FMI should seek to automate its cyber threat intelligence process.
15. The FMI should integrate and align its cyber threat intelligence process with its Security Operating Centre. The FMI should use information gathered from its Security Operating Centre to further enhance its cyber threat intelligence; and conversely, use its cyber threat intelligence to inform its Security Operating Centre.

2.7.2.2. Information sharing

BASELINE

16. The FMI should define the goals and objectives of information sharing, in line with its business objectives and cyber resilience framework. At the very least, the objectives should include collecting and exchanging timely information that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber attack.
17. The FMI should define the scope of information-sharing activities by identifying the types of information available to share (e.g. modus operandi of attackers, indicators of compromise, threats and vulnerabilities, etc.), the circumstances under which sharing this information is permitted (e.g. in the case of a cyber incident), those with whom the information can and should be shared (e.g. the direct stakeholders of the FMI such as critical service providers, participants, other interconnected FMIs, etc.), and how information provided to the FMI and other sector participants will be acted upon.
18. The FMI should establish and regularly review the information-sharing rules and agreements and implement procedures that allow prompt sharing of information, in line with the objectives and scope established above, while ensuring at the same time its obligations for protecting potentially sensitive data that may have adverse consequences if disclosed improperly.
19. The FMI should establish trusted and safe channels of communication with its direct stakeholders in exchange of information.
20. The FMI should have in place a process to timely access and share information with external stakeholders, such as regulators, law enforcement or other organisations within the FMI's ecosystem.

INTERMEDIATE

21. The FMI should participate actively in existing information-sharing groups and facilities, including cross-industry, cross-government, and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats.
22. The FMI should establish and implement protocols for the sharing of threat, vulnerability and cyber incident information with employees, based on their specific roles and responsibilities.

23. The FMI should share information with relevant stakeholders in the ecosystem to achieve broader cyber resilience situational awareness, including promoting an understanding of each other's approach to achieve cyber resilience.

ADVANCED

24. The FMI should develop an in-house threat intelligence capability (including personnel, infrastructure and training) which sources and stores internal and external threat and vulnerability information, analyses this information, and disseminates it to the relevant stakeholders in the ecosystem in a prompt manner, so as to facilitate early response and risk mitigation by the stakeholders. The FMI should, as far as possible, automate this process.

25. The FMI should participate in efforts to identify the gaps in current information-sharing mechanisms and seek to address them, in order to facilitate a sector-wide response to large-scale incidents.

2.8. LEARNING AND EVOLVING

2.8.1. Learning and evolving - Preamble

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

2.8.2. Learning and evolving - Expectations

BASELINE

1. The FMI should have capabilities in place to gather information on common vulnerabilities, cyber threats and events (cyber incidents and near misses), occurring both within and outside the FMI.
2. The FMI should have the capabilities to analyse the information gathered, and assess the potential impact on its cyber resilience framework.
3. The FMI should distil and classify the lessons learned (e.g. strategic, tactical and operational), identify the key stakeholders to whom these apply, then incorporate them to improve the FMI's cyber resilience framework and capabilities, and convey them to each relevant stakeholder, on an ongoing basis.
4. Senior management should ensure that it has a programme for continuing cyber resilience training and skills development for all staff. This training programme should include the Board members and senior management and should be conducted at least annually. The annual cyber resilience training should include incident response, current cyber threats (e.g. phishing, spear phishing, social engineering and mobile security) and emerging issues. The FMI should ensure that the training programme equips staff to deal with cyber incidents, including how to report unusual activity.
5. The FMI should ensure that cyber security awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts.
6. The FMI should incorporate lessons learned into the employee training, awareness programmes and materials, on an ongoing and dynamic basis. The

FMI should leverage off industry and authority initiatives around awareness and training, where possible.

7. The FMI should set a range of indicators and develop management information to measure and monitor the effective implementation of the cyber resilience strategy and framework on a regular basis and its evolution over time. For example, relevant information and indicators could be: percentage of the FMI's personnel that have received cybersecurity training; percentage of incidents reported within required timeframe per applicable incident category; percentage of vulnerabilities mitigated within a defined time period after discovery, yearly reports monitoring progress of indicators, etc.

INTERMEDIATE

8. The FMI should validate the effectiveness of incorporating lessons learned into the employee training and awareness programmes on a regular basis.
9. An FMI should actively monitor technological developments and keep abreast of new cyber risk management processes that can effectively counter existing and newly developed forms of cyber attack. An FMI should consider acquiring such technology and know-how to maintain its cyber resilience.
10. The FMI should analyse and correlate findings from audits, management information, incidents, near misses, tests (e.g. vulnerability assessment, penetration testing, red-team testing, etc.), exercises and external and internal intelligence in order to drive and enhance improvement in its cyber resilience capabilities. An internal cross-disciplinary steering committee could drive this activity.
11. The FMI should incorporate lessons learned from real-life cyber events and/or from testing results on the FMI and/or other organisations, to improve the FMI's risk mitigation capabilities as well as its cyber contingency, response, resumption and recovery plans.
12. The FMI should continuously track its progress in developing its cyber resilience capabilities from a current state to a defined future state. A maturity model can assist the FMI in documenting this progress.

ADVANCED

13. The FMI should use multiple sources of intelligence, correlated log analysis, alerts, traffic flows, cyber events across other sectors and geopolitical events to predict potential future cyber events and trends, and proactively take the appropriate measures to improve its cyber resilience capabilities.

ANNEX 1 - GLOSSARY

[To be drafted during and after the Public Consultation – during the Public Consultation, the Eurosystem will ask the market to indicate which terms would benefit from a precise definition. In the interim, some terms have been included, which the Eurosystem will include in the final version.]

Term	Definition	Source
Adaptive Access Controls		Source
Attribute-based Access Control		Source
Background checks		Source
Bug Bounty Program		Source
Capabilities		Source
Critical functions		Source
Defence-in-depth		Source
Digital Evidence		Source
Higher risk staff		Source
Information Security Control Framework		Source
Information Security Management System		Source
Information Sharing and Analysis Centre		Source
Information System		Source
Interconnections		Source
Internal cross-functional steering committee		Source
Key roles		Source
Least privilege		Source

Maturity model	Source
Network Infrastructure	Source
Penetration testing	Source
Performance Plan	Source
Recovery Point Objectives	Source
Recovery Time Objectives	Source
Red-Team Testing	Source
Responsible disclosure programme	Source
Rogue Device	Source
Scenario based testing	Source
Security Controls	Source
Security Operating Centre	Source
System Development Life Cycle	Source
Third-party service provider	Source
Threat and Vulnerability Information Sharing Source	Source
Unconventional scenarios	Source
Vulnerability assessments	Source
Etc	Source

ANNEX 2 - ABBREVIATIONS

[To be drafted during the Public Consultation]

Abbreviation	Definition
ISAC	Information Sharing and Analysis Centre
ISMS	Information Management Security System
SDLC	System Development Life Cycle
Etc.	

ANNEX 3 – GUIDANCE ON THE SENIOR EXECUTIVE

1. The FMI should appoint a Senior Executive, normally a Chief Information Security Officer (CISO), who is responsible for all cyber resilience issues within the FMI and with regard to third parties. The Senior Executive ensures that the cyber resilience objectives and measures defined in the FMI's cyber strategy, cyber resilience policies and guidelines are properly communicated both internally and, when relevant, to third parties, and that compliance with them is reviewed, monitored and ensured.

2. The Senior Executive or CISO function has in particular the following tasks:
    a. Supporting senior management and the Board when defining and updating the cyber resilience policies, and advising on all cyber resilience issues; this includes helping to resolve conflicting goals (e.g. cost-efficiency versus cyber resilience);
    b. Participating in the cyber risk management, as the second line of defence;
    c. Producing cyber resilience guidelines and, where appropriate, any other relevant rules and as well as checking compliance;
    d. Influencing the FMI's cyber resilience processes as well as monitoring the involvement of IT service providers and assisting in any related tasks;
    e. Participating in the production and updating of the contingency plan with regard to cyber issues;
    f. Initiating and monitoring the implementation of cyber resilience measures;
    g. Participating in projects relevant to cyber resilience (e.g. monitoring security testing for new components before entering production);
    h. Acting as a point of contact for any questions relating to cyber resilience coming from within the FMI or from third parties;
    i. Investigating cyber incidents and reporting these to the senior management and the Board;
    j. Continuous surveillance of threats applicable to IT-assets;
    k. Initiating and coordinating measures to raise awareness on cyber resilience as well as training sessions; and

l. Reporting to senior management and the Board regularly, at least quarterly, and on an ad hoc basis on the status of cyber resilience issues. This status report includes, for example, an evaluation of the cyber resilience situation compared with the last report, information about cyber resilience projects, cyber incidents and the results of penetration and red-team tests.

3. In terms of organisation and processes, the Senior Executive or CISO must be independent to avoid any potential conflicts of interest. Therefore, the following measures, in particular, are expected to be applied:
    a. Organisational set-up to ensure the Senior Executive or CISO can act independently from the IT/operations department and be able to report to senior management and the Board directly and at any time[5]; also ensuring that the Senior Executive or CISO is not involved in internal audit activities;
    b. Determination of the necessary resources required by the Senior Executive or CISO;
    c. Designation of a budget for cyber resilience training sessions within the FMI and for further training of the Senior Executive or CISO personnel/team; and
    d. Requirement to all employees in the FMI as well as to IT service providers to report any incidents relevant to the cyber resilience of the FMI, according to the escalation procedure.

4. The FMI must maintain its own Senior Executive or CISO in house, depending on the specific structure and organisational setup of the FMI.

[5] We do observe organisational set-ups where the CISO has a functional reporting line to the CIO, but with guarantees for the CISO to have direct access to senior management and the Board directly and with sufficient resources for the CISO to conduct its independent role.