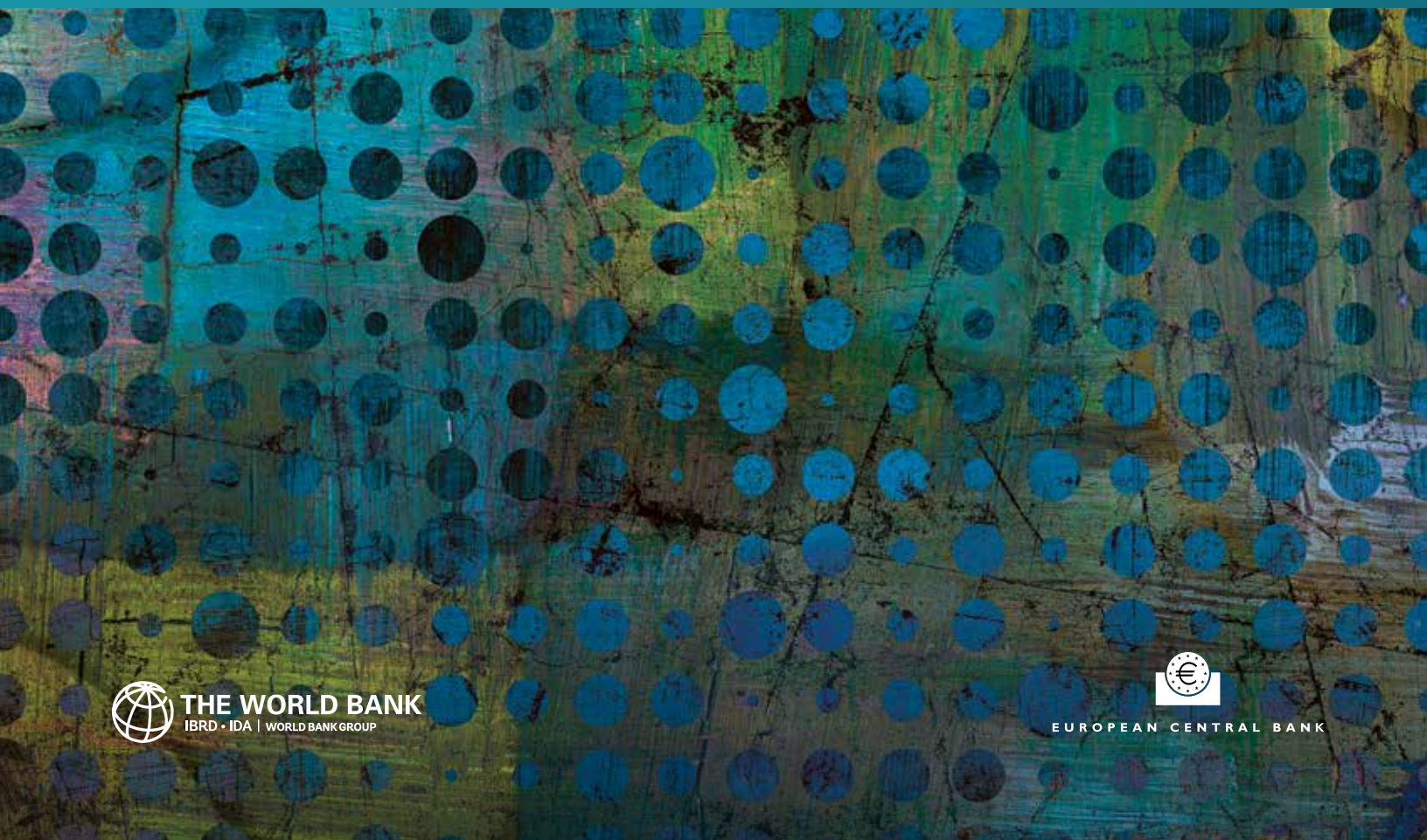
FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

Cyber Resilience for Financial Market Infrastructures

NOVEMBER 2019



THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

EUROPEAN CENTRAL BANK

CONTENTS

Cyber Resilience for Financial Market Infrastructures

NOVEMBER 2019[1]

ABSTRACT

The Financial Inclusion Global Initiative (FIGI) was launched by the World Bank Group, the International Telecommunication Union (ITU) and the Committee on Payments and Market Infrastructures (CPMI), with support from the Bill & Melinda Gates Foundation, to advance financial inclusion in developing countries. The FIGI initiative comprises 3 working groups (WG), the Digital Identity WG, Electronic Payments Acceptance WG, and Security, Infrastructure and Trust WG. Under the Security, Infrastructure and Trust Working Group, a dedicated workstream focus on cyber security for Financial Market Infrastructures (FMIs), to contribute to improve the cyber resilience of systems critical to financial stability and financial inclusion, especially in developing countries.

This document presents a methodology developed by the European Central Bank to operationalize the CPMI-IOSCO Guidance on Cyber Resilience for FMIs (Guidance), which could be used by FMIs to comply with the Guidance and by authorities (supervisors and overseers) to assess their FMIs against the Guidance, hence enhancing the overall cyber resilience of financial market infrastructures critical for financial stability and financial inclusion.

1. The document was first presented during the FIGI Symposium in Cairo in January 2019

Abbreviations

ABAC	Attribute-based access control
AI	Artificial intelligence
AIM	Asset inventory management
CCP	Central counterparty clearing house
CISO	Chief information security officer
COBIT	Control objectives for information and related technology
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CROE	Cyber resilience oversight expectations
CSD	Central securities depository
CSIRT	Computer security incident response team
DDoS	Distributed denial of service
DMZ	Demilitarised zone
e-CF	European e-Competence Framework
FFIEC	Federal Financial Institutions Examination Council
FMI	Financial market infrastructure
GRC	Governance, risk management and compliance
HIDS	Host intrusion detection system
HIPS	Host intrusion prevention system
HR	Human resources
IAM	Identity and access management
ICT	Information and communication technology
IDS	Intrusion detection system
IOSCO	International Organization of Securities Commissions
IoT	Internet of things
IPS	Intrusion prevention system
ISAE	International Standard on Assurance Engagements
ISAE 3402	Assurance reports on controls at a service organisation
ISMS	Information security management system
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information technology
KPI	Key performance indicators
KRI	Key risk indicators
NAC	Network access control
NCB	National central bank
NIST	National Institute of Standards and Technology
ORPS	Other retail payment systems
PFMIs	Principles for financial market infrastructures
PIRPS	Prominently important retail payment systems
RBAC	Role-based access control
RPO	Recovery point objectives
RTO	Recovery time objectives
SDLC	Software/system development life cycle
SFIA	Skills Framework for the Information Age
SIEM	Security information and event management
SIPS	Systemically important payment systems
SLA	Service level agreement
SOC	Security operations centre
SSH	Secure Shell
SSS	Securities settlement system
T2S	Target2-Securities
TLS	Transport layer security
TR	Trade repositories
VPN	Virtual private network
TIBER	Threat intelligence-based ethical red teaming
CERT	Computer emergency response team
ISAC	Information sharing and analysis centre
TTP	Tactics, techniques and procedures

I. Introduction and Background

Financial inclusion, and payment services as a critical financial need and gateway to other financial services, requires safe and efficient financial market infrastructures. Core payments infrastructures provide the foundation for the operation of electronic payment instruments and services, and constitute a critical enabler for financial inclusion, as demonstrated in the CPMI-WBG report on Payment Aspects of Financial Inclusion (PAFI, 2016).

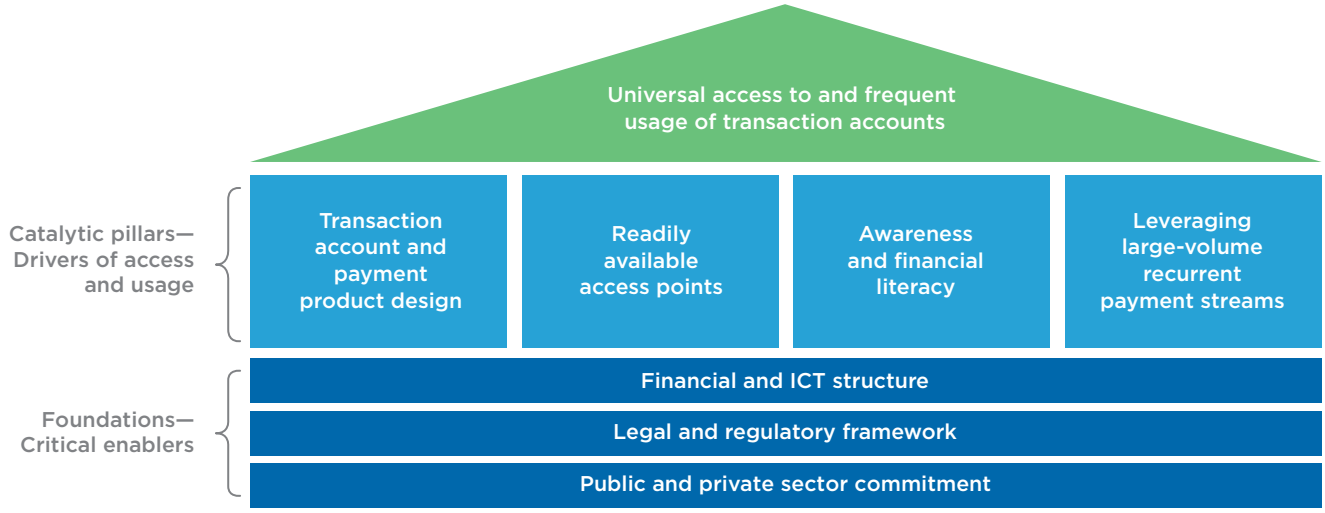
Cyber threat[2] has emerged as a systemic risk concern for the financial sector, and especially for financial market infrastructures, because of their unique role and characteristics. As demonstrated by the CPMI, cyber risk presents unique challenges for FMIs' traditional operational risk management frameworks. Firstly, the persistence and sophistication of cyber risk, make cyber-attacks difficult to identify or fully eradicate and equally difficult to determine the breadth of damage caused by cyber-attacks. Secondly, there is a broad range of entry points through which an FMI could be compromised. As a result of their interconnectedness, cyber-attacks could come through an FMI's participant, linked FMIs, service providers, vendors and vendor products. FMIs can themselves become a channel to further propagate cyber-attacks. Unlike physical operational disruptions, cyber risk posed by an interconnected entity is not necessarily related to the degree of that entity's relevance to the FMI's business. Thirdly, some cyber-attacks can render some risk management and business continuity arrangements of FMIs ineffective. Automated systems 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.

In 2016, the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published the "Guidance on cyber resilience for financial market infrastructures" (the Guidance), to support and standardize industry's efforts to enhance the cyber resilience of payment and securities settlement systems, and to support the consistent and effective oversight and supervision of their cyber resilience. The Guidance covers the ability of FMIs to preempt cyber-attacks, respond rapidly and effectively to them, and achieve faster and safer target recovery objectives if the attacks succeed.

The Guidance outlines 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: governance; identification; protection; detection; and response and recov-

2. A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security. (FSB Cyber Lexicon, November 2018)

FIGURE 1. PAFI Framework



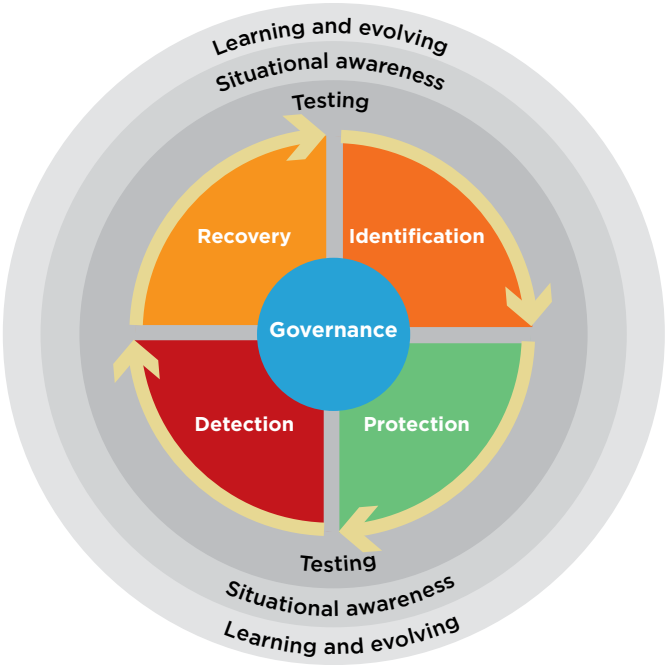
Source: Payment Aspects of Financial Inclusion, The World Bank 2016

ery. The overarching components are: testing; situational awareness; and learning and evolving.

FMIs are required to comply with the Guidance, and overseers must develop an oversight approach to assess their FMIs against the Guidance, but there is currently no detailed methodology to do it (comparable to the PFMIs methodology to assess the compliance with the CPMI-IOSCO Principles for Financial Market Infrastructures). In order to operationalize the CMPI Guidance, a more detailed methodology is therefore required. The European Central Bank (ECB) has developed such a methodology, through the Cyber Resilience Oversight Expectations (CROE). They set out clear criteria against which the overseers can assess the FMIs for which they are responsible, provide FMIs with concrete steps to implement the Guidance and enhance their cyber resilience, as well as a detailed basis for discussion between the FMIs and their authorities.

Although the CROE is designed in the context of the European Union, it could be used by authorities and FMIs in many countries, enhancing cyber resilience of FMIs at a global level and allowing for international references and benchmarking. It is therefore proposed that the FIGI cyber security for FMIs workstream considers using the methodology in its mandate to contribute to the dissemination of best practices related to cyber resilience of FMIs.

FIGURE 2. CPMI-IOSCO framework for cyber resilience of FMIs



Source: CPMI-IOSCO Guidance, 2016

II. Description of the CROE

In March 2017 the Governing Council of the ECB approved the "Eurosystem cyber resilience strategy for FMIs"[3] . The objective of this strategy is to improve the cyber resilience of the euro area financial sector as a whole by enhancing the "cyber readiness" of individual FMIs that are overseen by the Eurosystem central banks, and to foster collaboration among FMIs, their critical service suppliers and the authorities. Specifically, the strategy aims to put the Guidance into practice and comprises three pillars. The evolving nature of cyberattacks makes it necessary to ensure that FMIs strengthen their individual level of cyber maturity. In this regard, Pillar 1 (FMI Readiness) aims to ensure that the Guidance is put into practice in a consistent manner, by implementing a harmonised approach to assessing FMIs in the euro area against the Guidance. To facilitate this process, the ECB has—among other things[4]—developed the CROE.

The CROE serves three key purposes: (i) 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; (ii) it provides overseers with clear expectations to assess FMIs under their responsibility; 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 supplement the existing 'CPSS-IOSCO Principles for financial market infrastructures' (PFMIs), to ensure a full and coherent set of expectations. Additionally, whilst developing the draft CROE, the ECB also considered existing international guidance documents and frameworks. In particular, the National Institute of Standards and Technology (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.

In line with the Guidance, the CROE is presented in eight 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. Each chapter sets out three levels of expectations, which provide clarity and further details to both the FMI and its respective competent authority on how to concretely operationalize the Guidance. It is expected to review and

3. https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html
4. See for example the TIBER-EU Framework (www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html)

update the CROE in light of future market developments, as and when deemed necessary.

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.

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.

A. LEVELS OF EXPECTATION

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 capabilities. To address the idea of continuous adaptation, evolution and improvement, the CROE sets out levels of expectations 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 expectations: Evolving, Advancing and Innovating.

The essence of these three levels of expectations is continuous improving and maturing on the part of the FMI; the levels of expectations are not designed to establish static requirements and an end state of maturity, which risks creating a culture of compliance. Rather, FMIs are expected to be constantly evolving, advancing and innovating in light of the continuously evolving cyber threat landscape.

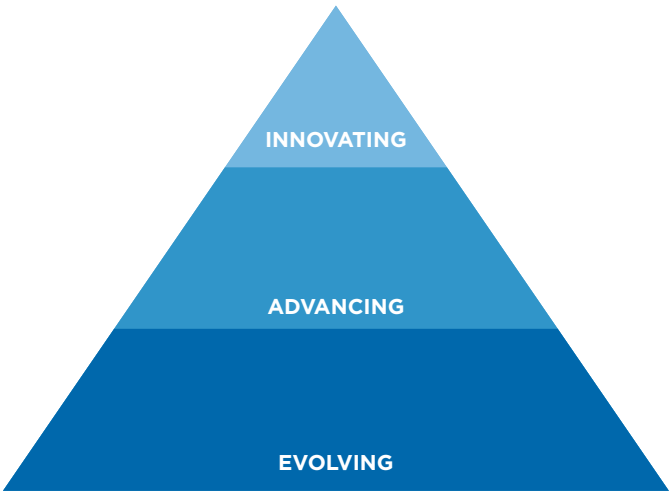
The three levels of expectations (Evolving, Advancing and Innovating) are defined as follows:

Evolving level: Essential capabilities are established and evolve, and are 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.

Advancing level: In addition to meeting the Evolving level, practices incorporate more advanced implementations (e.g. advanced technology and risk management tools) that are integrated across the FMI's business lines and have been improved over time, to proactively manage cyber risks to the FMI.

Innovating level: In addition to meeting the Evolving and Advancing 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 Innovating level entails driving innovation in people, processes, and technology for the FMI and the wider ecosystem to manage cyber risks and enhance cyber resilience. This may entail developing new controls, new tools, or creating new information-sharing groups.

FIGURE 3. CROE Levels of Expectation



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".

B. APPLICATION OF LEVELS OF EXPECTATIONS

Although the CROE have been developed to provide FMIs with detailed and specific expectations on how to operationalize 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.

The CROE should 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. The overseers or supervisors will determine the level of expectation their FMIs should meet and thereafter it will be the overseers' or supervisors' judgement to see whether the FMI, commensurate with its criticality, is meeting the Evolving, Advancing or Innovating levels. The professional judgement of the overseer or supervisor is an essential factor in determining whether the FMI is meeting the levels of expectations.

This judgement should be driven by a number of considerations, such as: the local laws and regulations governing the FMI; the overseer's or supervisor's broader historic knowledge of the FMI; the size, criticality and business model of the FMI, which should ensure a proportionate approach is taken; and the ongoing discussions between the overseer/supervisor and the FMI.

It is expected that FMIs will reach the levels of expectations, as determined by the relevant authority, across all eight categories of the Guidance; once FMIs reach and maintain their prescribed levels of expectations, they should continue to evolve and improve by taking relevant steps to reach the higher levels of expectations, 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 expectations are intended to allow the FMI to build and improve its capabilities in a multi-layered fashion over a longer period of time, with each level of expectation 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 expectations contained therein, giving due consideration on how best to build, improve and use its people, processes and technologies.

As FMIs implement the expectations, it is acknowledged that at times they will do so in different ways. In cases where the FMI does not meet the prescribed expectation, it should provide an explanation on how it meets the objective of the underlying expectation. The 'meet or explain' principle provides the FMI with a degree of flexibility in its approach of enhancing its cyber resilience capabilities, given that FMIs are heterogeneous and will differ by size, organizational and operating structure, business model and infrastructure set-up. Consequently, it is feasible that FMIs may fulfil the underlying objectives of the expectations by using different processes, technologies and methodologies.

III. ECB Cyber Resilience Oversight Expectations

1 GOVERNANCE

1.1 Preamble

Cyber governance refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks. Effective cyber governance should start with a clear and comprehensive cyber resilience framework that prioritizes 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 recognizes that staff at all levels have important responsibilities in ensuring the FMI's cyber resilience.

Strong cyber governance is essential to an FMI's implementation of a systematic and proactive approach to managing the prevailing and emerging cyber threats that it faces. It also supports efforts to appropriately consider and manage cyber risks at all levels within the organization and to provide appropriate resources and expertise to deal with these risks. This 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.

1.2 Expectations

1.2.1 Cyber resilience strategy and framework

EVOLVING

Cyber resilience strategy:

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

(a) evaluate and prioritise internal and external stakeholders' needs and expectations, deciding on the overall requirements from cyber resilience;

(b) provide direction to senior management on 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;

(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) Internal and external stakeholders' high-level requirements, so that these can be taken into account when defining cyber resilience governance 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 FMI's vision and mission 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 cyber maturity targets and a roadmap or implementation plan with change delivery and planning of capabilities relating to people, processes and technology at pace with threats and proportionate to the FMI's size and criticality. The strategy should clearly set out how this roadmap or implementation plan will be delivered and how the Board should track and monitor delivery.

(g) The high-level scope of technology and assets which will be used to manage cyber resilience.

(h) The interactions with other participants, FMIs and third parties, on areas such as information sharing.

(i) The governance necessary to enable cyber resilience to be designed, transitioned, operated and improved.

(j) How cyber resilience initiatives will be delivered, managed and funded, including the budgeting process and organisational capabilities.

(k) 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 and other relevant strategies (e.g. enterprise risk management, operational risk and IT).

4. 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.

5. The Board should be kept regularly informed of the FMI's cyber risk and ensure consistency with the FMI's risk tolerance and appetite, so that it can achieve the FMI's overall business objectives and corporate strategy.

Cyber resilience framework:

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

7. 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.

8. The FMI should use leading international, national and industry-level standards, guidelines or recommendations (e.g. NIST, COBIT 5 and ISO/IEC 27000, etc.), reflecting current industry best practices in managing cyber threats, as a benchmark for designing its cyber resilience framework and incorporating the most effective cyber resilience solutions.

9. At the broader level, the FMI's cyber resilience framework should be consistent with its enterprise risk management framework.

10. The FMI's Board should endorse this cyber resilience framework, ensuring it is aligned with the FMI's formulated cyber resilience strategy, review it at least annually and update it when needed to ensure that it remains relevant.

11. 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.

ADVANCING

Cyber resilience strategy and framework:

12. The FMI should use maturity models and define relevant metrics 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 staff on a regular basis.

13. 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, etc.);
    (b) threat intelligence on threat actors and new tactics, techniques and procedures which may specifically impact the FMI;
    (c) the results of risk assessments of the FMI's critical functions, key roles, processes, information assets, third-party service providers and interconnections;
    (d) actual cyber incidents that have impacted the FMI directly or external cyber incidents from the ecosystem;
    (e) lessons learned from audits and tests on the cyber resilience framework;
    (f) the FMI's performance against the relevant metrics and maturity models;
    (g) new business developments and future strategic objectives.

14. 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.

INNOVATING

Cyber resilience strategy and framework:

15. The cyber resilience strategy should outline the FMI's future state of cyber resilience, in terms of maturity and/or risk, with short and long-term perspectives, and senior management should continuously improve and adapt the existing cyber resilience strategy and framework as the desired maturity level and/or risk landscape changes.

16. The FMI should establish the appropriate structures, processes and relationships with the key stakeholders in the ecosystem to continuously and proactively enhance the ecosystem's cyber resilience and promote financial stability objectives as a whole.

1.2.2 Role of the Board and senior management

EVOLVING

Board and management responsibilities:

17. 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.

18. In order to carry out 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 the cyber risks facing the FMI. It should also be sufficiently informed and capable of credibly challenging the recommendations and decisions of designated senior management. Although the Board should collectively increase its skills and knowledge on cybersecurity, it can also access specific expertise through a Board member with adequate experience, or through experienced staff and/or external independent organisation(s) reporting to and advising the Board.

19. The Board and senior management should ensure that a senior executive (e.g. the CISO) is responsible and accountable for implementing 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, and have sufficient resources and direct access to the Board. For further clarification on the possible roles and responsibilities of such a senior executive, see Annex 3.

20. The Board and senior management should ensure that staff (including senior management) who are responsible for cyber activities have suitable skills, knowl-

edge and experience, and are sufficiently informed and empowered to make timely decisions.

21. The Board and senior management should ensure that cyber risk, implementation of the cyber resilience framework and any associated issues appear regularly on the Board's meeting agenda. Boards should have adequate access to cybersecurity expertise (whether internal or external), and discussions about cyber risk management should be given adequate time on the Board's meeting agenda.

22. Senior management should regularly provide a written report to the Board on the overall status of its cyber resilience programme and keys risks and issues.

23. As part of the Board's updates, senior management should provide their budgeting and forecasting activities plan for ongoing and future resource needs to ensure cyber resilience objectives are continually achieved.

Culture:

24. 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 for ensuring the FMI's cyber resilience, and lead by example.

25. 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.

26. Senior management should ensure that situational awareness materials are made available to relevant employees when prompted by highly visible cyber incidents, changes to the threat landscape and the impacts of these threats to the FMI, 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:

27. 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. threats, threat actors and vulnerabilities), tactics and techniques (e.g. phishing, spear phishing, social engineering and mobile security) and emerging issues, according to staff members' levels of responsibility and the risks associated with their respective roles.

28. Senior management should ensure that employees and contractors with privileged account permissions and/or access to sensitive assets and information, receive additional cyber resilience training commensurate with their levels of responsibility, and that business units are provided with cyber resilience training relevant to their criticality to the business.

29. 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 could 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.

30. 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.

ADVANCING

Board and management responsibilities:

31. 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.

32. The Board should ensure that senior management regularly conducts a cyber resilience self-assessment , 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.

33. 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:

34. Senior management should establish and sustain incentives (e.g. staff recognition awards) to ensure behaviours are consistent with the intended cyber risk culture.

35. Senior management should produce a formal cyber Code of Conduct, which can be incorporated into the FMI's enterprise Code of Conduct, and ensure that all employees comply with it.

36. 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.

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

Skills and accountability:

38. Senior management should embed a programme for talent recruitment, retention and succession planning for the staff, and ensure such staff are aligned to cyber activities and deployed effectively across the FMI.

39. Senior management should ensure that there are well-defined plans for the succession of high-risk staff (e.g. senior management, system administrators, software developers and critical system operators, etc.), and the recruitment requirements for key cyber roles include suitable cyber skills, knowledge and experience in alignment with defined succession plans.

40. Senior management should ensure that staff performance plans are tied to compliance with cyber resilience policies and standards in order to hold employees accountable.

INNOVATING

Board and management responsibilities:

41. The FMI should appoint a dedicated cyber expert to the Board.

42. The standard Board meeting package should include reports and metrics that cover areas such as suspicious cybersecurity events (e.g. increased network behaviour and unusual user activity), cyber incidents and threat intelligence trends for the ecosystem to facilitate discussions on how the FMI should respond accordingly.

43. The Board and senior management should proactively enhance its strategic goals, objectives and tactical plans, as needed, to support cyber activities and improvements across the ecosystem, making use of any available sector-defined requirements and coordinated initiatives, and clearly communicate this to the relevant stakeholders.

Culture:

44. Senior management should cooperate proactively with other stakeholders to promote a cyber resilience culture across the ecosystem.

Skills and accountability:

45. Senior management should regularly benchmark its cyber resilience capabilities against the market to identify its gaps in terms of governance, skills, resources and tools, treating these gaps as cyber risks and addressing them accordingly.

46. 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 IDENTIFICATION

2.1 Preamble

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

2.2 Expectations

EVOLVING

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

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

3. The FMI should maintain an up-to-date inventory of all the critical functions, key roles, processes, infor-

mation assets, third-party service providers and interconnections. It 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 an enterprise risk management framework to identify risks and conduct risk assessments on a regular basis and 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 an associated plan addressing IPs which locate routing and security devices and servers supporting the FMI's critical functions, and which identify links with the outside world.

6. The FMI should conduct risk assessments before deploying 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 cybersecurity 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 a fully comprehensive inventory of all individual and system accounts (especially including privileged and remote access accounts) so that they can be aware of the access rights to information assets and their supporting systems. The FMI should review and update this inventory on a regular basis.

ADVANCING

8. The FMI should use automated tools (e.g. a centralised asset inventory management (AIM) tool) 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 that these changes are shared with the relevant staff in in a timely manner.

9. The FMI should use automated tools (e.g. a centralised identity and access management (IAM) tool) that enable it to support the identification and classification process of roles, user profiles and individual and system credentials, and ensure that these are updated accurately and that relevant staff are informed of the changes in a timely manner.

10. The FMI should also maintain up-to-date and complete maps of network resources, interconnections and dependencies, and data flows with other information assets, including the connections to business partners, internet-facing services, cloud services and any other third-party systems. It should use these maps to undertake risk assessments of key dependencies and apply appropriate risk controls, when necessary.

11. The FMI should update its inventory to address new, relocated, repurposed and sunset information assets, on a regular basis or when these changes occur.

INNOVATING

12. The FMI should use automated feeds from above (e.g. from AIM and IAM tools), in order to identify emerging risks, update its risk assessments in a timely manner and take the necessary mitigating actions in line with the FMI's risk tolerance.

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

3 PROTECTION

3.1 Preamble

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

3.2 Expectations

3.2.1 Protection of processes and assets

Control implementation and design

EVOLVING

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 the identification phase. The security objectives may include ensuring:

(a) the continuity and availability of its information systems;

(b) the integrity of the information stored in its information systems, while both in use and transit;

(c) the protection, integrity, confidentiality and availability of data while at rest, in use and in transit;

(d) conformity to applicable laws, regulation and standards.

2. The FMI should develop its security controls in order to address cybersecurity 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 assess the effectiveness of its security controls regularly in order to adapt them to its evolving threat landscape. They should be monitored and audited regularly to ensure that they remain effective and have been applied to all assets where they might be needed.

4. When designing, developing and acquiring its systems and processes, the FMI should capture security requirements alongside system and process requirements in order to identify the security controls necessary for protecting its systems, processes and data, at the earliest possible stage.

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

ADVANCING

6. The FMI should develop and implement a bespoke information security management system (ISMS), which could be based on a combination of well-recognised international standards (e.g. ISO 27001, ISO 20000-1 and ISO 27103, etc.), in order to establish, implement, operate, continuously monitor, review, maintain and improve a comprehensive cybersecurity 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 life cycle, so that vulnerabilities in software and hardware are minimised and security controls are 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 stage of the SDLC, the FMI should manage its cyber risk and integrate resilience based on risk analysis results.

INNOVATING

8. The FMI should frequently review its ISMS, using certification, audis or other relevant forms of assurance.

9. The FMI should develop processes and procedures and explore potential technologies to constantly adjust and refine its security countermeasures (controls). This will help it to ensure it is protected against known and emerging threats, based on knowledge and best practices obtained from other FMIs across the ecosystem and through the use of threat intelligence.

Network and infrastructure management

EVOLVING

10. The FMI should establish a secure boundary that protects its network infrastructure (using tools such as a router, firewall, intrusion prevention system (IPS) or intrusion detection system (IDS), virtual private network (VPN), demilitarised zone (DMZ) or proxies etc.). The boundary should identify trusted and untrusted zones according to the risk profile and criticality of information 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.

11. The FMI should seek to use a separate and dedicated network for information system administration. At a minimum, the FMI should prohibit direct internet access from devices or servers used for information system administration whenever possible.

12. The FMI should establish a baseline system and security configurations for information systems and system components, including devices used for accessing the FMI network remotely, to help the configuration to and security reinforcement of those systems and components to be applied consistently. These baselines should be documented, formally reviewed and regularly updated to adapt them to the FMI's evolving threat landscape.

13. The FMI should reinforce 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.

14. The FMI should seek to use secure network protocols (e.g. Secure Shell and protocols relying on transport layer security (TLS) or equivalent), when appropriate, in order to guarantee the confidentiality and integrity of information exchanged within its network and beyond, including remote connections.

15. The FMI should define and implement procedures that limit, lock and terminate system and remote sessions after a predefined period of inactivity and predefined conditions are met.

16. The FMI should deploy a broad range of technologies and tools to detect and block actual and attempted attacks or intrusions. The FMI may use intrusion detection or prevention systems, end point security solutions (e.g. antivirus, a firewall, or a host intrusion detection system (HIDS) or host intrusion prevention system (HIPS)) or any other relevant solutions (e.g. an access gateway or a jump box), in particular on devices and in environments used for accessing the FMI network remotely.

17. The FMI should implement controls that manage or prevent non-controlled devices to connect to its internal network from inside or outside the premises to ensure that activities in these zones are logged and monitored for inappropriate use or attempts to access business systems. The FMI's infrastructure should be scanned regularly to detect rogue devices and access points.

18. The FMI should scan its legacy technologies regularly to identify potential vulnerabilities and seek upgrade opportunities. Controls and additional defence layers should be implemented and tested in order to protect unsupported or vulnerable systems.

19. The FMI should have policies and controls that prevent users from installing unauthorised applications. Procedures should be in place to manage the installation of applications.

ADVANCING

20. 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 the identification phase, the FMI should maintain current and complete network and data flow diagrams.

21. 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.

22. The FMI's IT environments and functions should be adequately separated with different security levels and controls implemented.

23. The FMI should implement technical measures to prevent the execution of unauthorised code on institution-owned or managed devices, network infrastructure and system components.

24. The FMI should consider implementing technical measures (e.g. network access control (NAC) solutions) in order to prevent unauthorised devices from being connecting successfully.

25. 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.

INNOVATING

26. The FMI should implement automated mechanisms that can isolate affected information assets in the case of an adverse event.

27. 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 in 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.

Logical and physical security management

EVOLVING

28. 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.

29. 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 evaluated regularly to identify unneeded access or privileges. Physical, logical and/or remote access to critical systems should be restricted and 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.

30. 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 assign-

ments should be reviewed regularly by appropriate staff (e.g. management and system owners, etc.) in order to take appropriate action when privileged role assignments are no longer appropriate.

31. 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 staff, and should be recorded for review if necessary.

32. 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, which ensures that the positions and roles are not apparent).

33. The FMI should have a dedicated policy that covers all the characteristics of its authentication mechanisms (e.g. password, smart cards and biometrics, etc.) and is in line with relevant standards (e.g. NIST-800-63). Default authentication settings (e.g. passwords and unnecessary default accounts) should be deactivated, changed or removed before systems, software and/or services go live.

34. The FMI should develop appropriate controls (e.g. 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 the identification phase.

35. 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.

ADVANCING

36. The FMI should implement controls to prevent unauthorised privileged escalation (e.g. technical controls that trigger automated notification to appropriate staff in the case of changes to user access profiles).

37. The FMI should encrypt data as a result of its data classification and risk assessment processes. The FMI should also use encryption and general cryptographic controls in line with recognised standards and processes, which cover aspects such as algorithm, key length and key generation, etc.

38. The FMI should implement automated mechanisms to support the management of information system access accounts. This might include implementing 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.

INNOVATING

39. 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), in an integrated way, ensuring all systems update each other consistently.

40. The FMI should seek to use an attribute-based access control (ABAC) paradigm that allows it to manage access to its IT environment contextually and dynamically.

41. The FMI should employ automated mechanisms that allow account creation, modification, enabling, disabling and removal actions to be monitored and audited continuously, in order to notify appropriate staff when potential malicious behaviour or damage is detected. The FMI should implement adaptive access controls to prevent potential malicious behaviour or damage.

Change and patch management

EVOLVING

42. The FMI should have policies, procedures and controls in place 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, as well as the FMI's systems and data;
    (c) approved before it is implemented by the appropriate level of management.

43. The FMI should ensure that the cybersecurity team is involved throughout the life cycle of the change management process, as appropriate.

44. The FMI should put necessary procedures in place (e.g. code review and unit testing, etc.), guaranteeing that changes are implemented correctly and efficiently. The FMI should employ best practices when implementing changes.

45. The FMI should test, validate and document changes to the information system before implementing them into production (this might include integration tests, non-regression tests and user acceptance tests, etc.). The changes to information systems include, but are not limited to, modifying hardware, software or firmware components and 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.

46. 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.

47. The FMI should have a comprehensive patch management policy and processes that include: maintaining current knowledge of available patches; identifying appropriate patches for particular systems and analysing impacts if installed; assuring that patches are installed properly (e.g. by applying the four-eyes principle) and tested prior to and monitored after installation; and documenting all associated procedures, such as specific configurations required. The policies, procedures and controls must make use of the information AIM process described in the identification phase that provides information on the installed programs and binaries.

48. The FMI should consider using standardised configuration of IT resources to facilitate its patch management process.

49. The FMI should ensure that the installations of new patches have prior approval from the appropriate level of management.

50. 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.

51. The FMI should have policies and procedures to prohibit changes and patch installation to the information system that have not been pre-approved.

ADVANCING

52. The FMI should establish its change management process based on well-established and industry-recognised standards and best practices (e.g. the information technology infrastructure library).

53. The FMI should consider automating its patch management process when possible to guarantee that all its systems remain consistently up to date.

54. The FMI should consider building a segregated or separate environment that mirrors the production environment, allowing rapid testing and changes and patches to be implemented, and providing for rapid fall-back when needed.

INNOVATING

55. The FMI should implement automated mechanisms to prohibit changes and patches from being installed on the information system that have not been pre-approved.

3.2.2 People management

Human resources security

EVOLVING

56. The FMI should embed cybersecurity at each stage of the employment life cycle, specifying security-related actions required during the induction of each employee and their ongoing management, and upon the termination of their employment.

    (a) Prior to employment, the FMI should carry out background security checks on all candidates (employees and/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 cybersecurity 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 access rights that are related to his/her previous position and are not necessary for his/her new responsibilities are revoked in due time. Employees in sensitive positions (e.g. those who change to roles requiring privileged access to critical systems or who become high-risk staff) should be pre-screened.

    (c) The FMI should establish procedures to revoke all departing employees' access rights from the information assets in a timely manner. Upon termination of employment, staff should be required to return all assets that belong to the FMI, including important documentation (e.g. related to business processes, technical procedures and contact details), equipment, software and authentication hardware, etc.

57. The FMI should establish policies, procedures and controls for granting or revoking employees 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.

58. The FMI should establish capabilities, including people, processes and technologies to monitor privileged users' activity and access to critical systems in order to identify and deter anomalous behaviour and notify appropriate staff.

ADVANCING

59. The FMI should implement mechanisms that trigger automatic notifications to be sent to staff in charge of granting or revoking access to the information system upon change to employment status.

60. The FMI should implement automatic mechanisms to grant or revoke staff access to its information system upon change to employment status.

INNOVATING

61. The FMI should monitor and analyse pattern behaviour (e.g. network use patterns, work hours and known devices, etc.) to identify anomalous activities and evaluate the implementation of innovative solutions (e.g. data analytics, machine learning and artificial intelligence, etc.) to support detection and response to insider threat activity in real time.

Security awareness and training

EVOLVING

62. The FMI should ensure that its employees have a good understanding of the cyber risk they might face when conducting their jobs and that they understand their roles and responsibilities in protecting the FMI's assets.

63. On a regular basis, at least once a year, the FMI should provide its entire staff (employees and/or contractors) with training to support cybersecurity policy compliance and the incident reporting process. This training should include elements aimed at maintaining appropriate awareness of cyber-related risks and good practices for dealing with potential cyber incidents, including how to report unusual activity. Cybersecurity awareness training should be part of the onboarding programme for new staff.

64. The FMI should ensure that high-risk staff receive dedicated security awareness training that is relevant to their responsibilities.

65. Prior to going into service operations, staff operating new systems should receive appropriate user training and be familiar with the operating procedures.

ADVANCING

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

INNOVATING

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

Supplier and third-party security management

EVOLVING

68. 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.

69. The FMI's third-party risk assessment should be carried out regularly, taking into account the evolution of its threat landscape. The FMI should, using a risk-based approach, ensure that the provision of outsourced services are accorded the appropriate level of cyber resilience.

70. 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). Provision of settlement services to ancillary systems by overseen entities is not considered to be third-party service provision.

ADVANCING

71. The FMI should design security controls that detect and prevent intrusions from third-party connections.

72. 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.

73. The independent audit function should validate the FMI's third-party relationship management and outsourcing.

74. 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. ISAE 3402), summaries of test reports, service level agreements (SLAs) and KPIs, etc.

INNOVATING

75. 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.

4 DETECTION

4.1 Preamble

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

4.2 Expectations

EVOLVING

1. Based on the risk assessment performed in the identification phase, 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 and cybersecurity 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, in a controlled and authorised manner.
7. The FMI should ensure that its relevant staff (employees and/or contractors) are trained to be able to identify and report anomalous activity and events.
8. The FMI should build multilayered detection controls covering people, processes and technology which support 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.

ADVANCING

12. The FMI should develop and implement automated mechanisms (e.g. a security information and event management (SIEM) system), which correlates all the network and system alerts and any other anomalous activity across its business units in order to detect multifaceted attacks (e.g. simultaneous account takeover or a distributed denial of service (DDoS) attack).
13. The FMI should have a process to collect, centralise and correlate event information from multiple sources and log analysis to continuously monitor the IT environment (e.g. databases, servers and end points, etc.) 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 operations centre (SOC) or equivalent.
14. The FMI should have processes in place to monitor activities that are not in line with its security policy and might lead to data theft, integrity compromise or destruction.
15. The FMI's monitoring and detection capabilities should allow the appropriate staff who can respond to be alerted automatically.
16. The FMI should have the capabilities, in collaboration with other stakeholders, to detect cyber events and adapt its security controls swiftly. 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 connections among information assets and cyber risk levels throughout the information assets' life cycles, 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.

18. The FMI should continuously monitor and inspect the network traffic, including remote connections, and end point configuration and activity to identify potential vulnerabilities or anomalous events in a timely manner.

19. The FMI should compare the network traffic and the end point configuration with the expected traffic and configuration baseline profile and data flows.

INNOVATING

20. 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.

21. The FMI should develop threat detection capabilities which can detect both known and unknown threats, with a proactive identification of vulnerabilities, state-of-the art threat detection and correlation between vulnerabilities and threats.

22. The FMI should seek to continuously explore new technologies and techniques inhibiting lateral movement (e.g. deception mechanisms) which trigger alerts and inform the FMI of potential malicious activity when accessed. For example, the FMI could create and place fictitious sensitive data with alerting tags attached to them.

5 RESPONSE AND RECOVERY

5.1 Preamble

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

5.2 Expectations

5.2.1 Cyber resilience incident management

EVOLVING

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 how to 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 (RPOs) and its recovery time objectives (RTOs), commensurate to its business needs and systemic role in the ecosystem.

2. Based on Expectation 1 above, 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 reroute 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 incident response, resumption and recovery plans, to manage cybersecurity events or incidents in a way that limits damage and 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 cybersecurity incidents. The FMI should ensure all relevant business units (including communications) are integrated into the plans.

5. 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.

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

7. The FMI should define alert parameters and thresholds for detecting cybersecurity incidents, which trigger the incident management processes and procedures, which in turn include alerting and conveying information to the appropriate staff.

8. The FMI should regularly test its cyber contingency, response, resumption and recovery plans against a range of different plausible scenarios.

9. The FMI should have processes and procedures in place for collating and reviewing information from its cybersecurity incidents and testing results in order to continuously improve its contingency, response, resumption and recovery plans.

10. The FMI should have processes and procedures in place to conduct an ex post root cause analysis of its cybersecurity incidents. The FMI should integrate its findings from the root cause analysis into its cyber response, resumption and recovery plans, as set out in Expectation 4 above.

ADVANCING

11. The FMI should design and test its systems and processes to enable critical operations to be resumed safely within two hours of a cyber disruption and to enable it 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 undertake careful problem analysis and exercise judgement (in agreement with competent authorities and relevant stakeholders) when resuming operations so that risks to the FMI or its ecosystem do not escalate as a result, while taking into account the fact that completion of settlement by the end of day is crucial.

12. The FMI should plan for scenarios in which resumption within two hours cannot be achieved. The FMI should analyse critical functions, transactions and interdependencies to prioritise resumption and recovery actions, which may, depending on the design of the FMI, help critical transactions to be processed, for example, while remediation efforts continue. The FMI should also plan for situations in which critical people, processes or systems may be unavailable for significant periods – for example, by potentially reverting (where feasible, safe and practicable) to manual processing if automated systems are unavailable.

13. The FMI should implement an effective incident handling capability for cybersecurity incidents that includes preparation, detection and analysis, containment, eradication and recovery. Such capability should allow the FMI to perform, at an early stage, analysis of cybersecurity 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.

14. The FMI should define and develop functional and security dependency maps of identified information assets supporting critical functions to understand and prioritise the order in which they should be restored.

15. 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.

16. 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.

17. The FMI should continuously monitor, evaluate and consider technological developments and solutions in the market that may enhance its contingency, response, resumption and recovery capabilities.

INNOVATING

18. The FMI should implement processes to continuously improve 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.

19. 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.

20. The FMI should implement a computer security incident response team (CSIRT), whether in-house or outsourced, that is responsible for responding to security incidents and intrusions, and coordinating activities among the relevant internal and external stakeholders. Such a team should have the authority to direct the FMI to make the changes necessary to recover from the incident.

21. The FMI should establish and implement processes to manage cybersecurity incidents and enable automated responses, triggered by predefined 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.

5.2.2 Data integrity

EVOLVING

22. The FMI should develop a formal backup policy specifying the minimum frequency and scope of data, based on data sensitivity and the frequency with which that new information is introduced.

23. The FMI should develop backup and recovery methods and strategies to be able to restore system operations with minimum downtime and limited disruption.

24. The FMI should regularly back up all data necessary to replay participants' transactions.

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

ADVANCING

26. The FMI should store backup copies at an alternate site with a different risk profile to the main site, and with transfer rates consistent with actual RPOs. The alternate site and backups should be safeguarded by stringent protective and detective controls.

27. The FMI's information systems should implement transaction recovery mechanisms for transaction-based systems, which might include transaction rollback and logging.

28. The FMI should conduct frequent periodic reconciliation of participants' positions, with the assistance of participants where needed.

29. The FMI should develop capabilities to restore information system components within the actual RTOs using a predefined and standardised configuration of IT resources, the integrity of which is protected.

INNOVATING

30. 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.

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

32. The FMI should consider having a data-sharing agreement with third parties and/or participants in order to obtain uncorrupted data from them for recovering its business operations in a timely manner and with accurate data.

5.2.3 Communication and collaboration

Contagion

EVOLVING

33. The FMI should identify, document and regularly review systems and processes supporting its critical functions and/or operations that are dependent on external connectivity.

34. The FMI should develop policies and procedures that define how it should work together with relevant interconnected entities to enable operations to be resumed (the first priority being its critical functions and services) as soon as it is safe and practicable to do so.

ADVANCING

35. The FMI should closely cooperate with its interconnected entities within the ecosystem, establishing rollback processes in order to restore all its services accurately and safely. Moreover, the FMI should test the effectiveness of these procedures regularly.

INNOVATING

36. 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.

Crisis communication and responsible disclosure

EVOLVING

37. The FMI should identify and determine staff who are essential for mitigating the risk of a cyber incident, and make them aware of their roles and responsibilities regarding incident escalation.

38. 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.

39. 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.

40. 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.

41. The FMI should have a policy and procedures to enable potential vulnerabilities to be disclosed responsibly. In particular, the FMI should prioritise disclosures that

could help stakeholders to respond promptly and mitigate risk, which could benefit the ecosystem and broader financial stability.

42. The FMI should establish and regularly review information-sharing rules, agreements and modalities in order to control the publication and distribution of such information, and to prevent sensitive information that may have adverse consequences if disclosed improperly from being disseminated.

ADVANCING

43. After developing a range of cyber incident scenarios based on the incident criteria established in the evolving level, the FMI should develop appropriate incident response and communication plans and procedures to address the scenarios. These incident response and communication plans and procedures should take into consideration the legal and regulatory reporting requirements at a jurisdictional level.

INNOVATING

44. The FMI should develop mechanisms that instantaneously notify its senior management, relevant employees and relevant stakeholders (including oversight and regulatory authorities) of cyber incidents through appropriate 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.

5.2.4 Forensic readiness

EVOLVING

45. The FMI should identify the threat scenarios that might have a potential impact on its business and determine which pieces of digital evidence (e.g. types of logs) should be collected to facilitate forensic investigation.

46. The FMI should identify and document the digital evidence available on its systems and its location, and understand how the evidence should be handled throughout its life cycle.

47. Based on Expectations 45 and 46, the FMI should develop and implement a forensic readiness policy and the 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. The FMI may outsource the conduct of forensic investigations to external specialists.

48. The FMI should establish procedures for securely collecting digital evidence in a forensically acceptable manner and in accordance with the requirements defined in the forensic readiness policy, 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.

49. The FMI should establish policies for securely handling and storing the collected digital evidence, ensuring its authenticity and integrity. The FMI should develop procedures to demonstrate that the evidence's integrity is preserved whenever it is accessed, used or moved (i.e. chain of custody).

50. The FMI should train its staff so that all those involved in an incident understand their responsibilities related to handling the digital evidence, ensuring it is not compromised and remains valid as per the requirements of the local jurisdiction.

51. The FMI should ensure that staff specifically involved in the forensic investigation have the appropriate degree of competence in handling the digital evidence, ensuring its authenticity and integrity is not compromised and remains valid as per the requirements of the local jurisdiction.

ADVANCING

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

INNOVATING

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.

6 TESTING

6.1 Preamble

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

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

6.2 Expectations

EVOLVING

General:

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 the core components 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 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 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 help any type of exploitable weakness to be identified (technical, processual, organisational and emergent) in the critical functions, their supporting processes and information 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 or redeployment of new or 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 simulations.
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 of the extent to which internal skills, processes and procedures can adequately respond to extreme but plausible 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 using a risk-based approach and, at the very least, in cases of major changes and new system deployment.

20. The FMI should perform penetration tests, engaging all critical internal and external stakeholders in the penetration testing exercises: system owners, business continuity, and incident and crisis response teams.

ADVANCING

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, attackers' modus operandi and vulnerabilities.

23. The FMI should adopt best practices and automated tools to support the 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 assessments and tests when applicable at all phases of the SDLC and at 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 among 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 team testing:

29. The FMI should conduct red team 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 team exercises using reliable and valuable cyber threat intelligence, based on specific and plausible threat scenarios.

31. The FMI should conduct independent red team exercises, utilising regulatory and industry frameworks (e.g. the European Framework for Threat-Intelligence Based Ethical Red teaming (TIBER-EU Framework)).

32. The FMI should build its internal processes and capabilities to prepare for undertaking the independent red team 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, for example.

INNOVATING

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 exercises 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 the cooperation arrangements in place with relevant external entities at least annually (e.g. third-party security service providers, law enforcement agencies, computer emergency response teams (CERTs) or information sharing and analysis centres (ISACs), etc.) in order to validate their effectiveness.

38. The FMI should consider discussing relevant test conclusions with other 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.

Vulnerability assessments:

39. The FMI should develop and adopt a range of effective practices and tools (e.g. a Bug Bounty programme and static and dynamic code reviews, etc.) as part of its vulnerability management process, and have appropriate safeguards in place to manage them.

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, interdependencies and possible contagion 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 improving the ecosystem's resilience as a whole.

Red team testing:

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

7 SITUATIONAL AWARENESS

7.1 Preamble

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

7.2 Expectations

7.2.1 Cyber threat intelligence

EVOLVING

1. The FMI should identify cyber threats that could materially affect its ability to perform or provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its 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 IDSs; 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 ISAC 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 cybersecurity incidents experienced by other organisations (where available), 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 the purpose of implementing appropriate cybersecurity 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 cyber threat information and the production of cyber threat intelligence are reviewed and updated regularly.
7. The FMI should ensure that cyber threat intelligence is made available to appropriate staff who are responsible for mitigating 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.

ADVANCING

9. The FMI should continuously use its cyber threat intelligence to anticipate, as much as possible, a cyber attacker's capabilities, intentions and modus operandi, and subsequently possible future attacks.
10. The FMI should develop a cyber threat risk dashboard, which uses the cyber threat information and intelligence to outline, among 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 its reputation that could arise from such attacks;
    (e) the impact of attacks already conducted by such threat actors on the ecosystem;
    (f) the risk mitigation measures in place to manage a potential attack.
11. The cyber threat risk dashboard should be continuously reviewed and updated in the 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 review and update this analysis regularly.

INNOVATING

13. The FMI should ensure that the scope of cyber threat intelligence gathering includes 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 integrate and align its cyber threat intelligence process with its SOC. The FMI should use information gathered from its SOC to further enhance its cyber threat intelligence; and conversely, use its cyber threat intelligence to inform its SOC.

7.2.2 Information sharing

EVOLVING

15. 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 information in a timely manner 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.
16. The FMI should define the scope of information-sharing activities by identifying the types of information available to be shared (e.g. attackers' modus operandi, indicators of compromise, and 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 FMI's direct stakeholders such as critical service providers, participants and other interconnected FMIs, etc.), and how information provided to the FMI and other sector participants will be acted upon.
17. The FMI should establish and regularly review the information-sharing rules and agreements and implement procedures that allow information to be shared promptly and in line with the objectives and scope established above, while at the same time meeting its obligations to protect potentially sensitive data that may have adverse consequences if disclosed improperly.

18. The FMI should establish trusted and safe channels of communication with its direct stakeholders for exchanging information.

19. The FMI should have in place a process to access and share information with external stakeholders in a timely manner, such as regulators, law enforcement or other organisations within the FMI's ecosystem.

ADVANCING

20. 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.

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

22. 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 achieving cyber resilience.

INNOVATING

23. The FMI should make use of threat intelligence capabilities that provide internal and external threat and vulnerability information, analyse this information, and disseminate it to the relevant stakeholders in the ecosystem promptly, so as to help stakeholders to respond quickly and mitigate risks.

24. 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.

8 LEARNING AND EVOLVING

8.1 Preamble

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

8.2 Expectations

8.2.1 Cyber threat intelligence

EVOLVING

1. The FMI should have capabilities in place to gather information on common vulnerabilities, cyber threats, events and incidents 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, 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 cybersecurity awareness materials are made available to staff when prompted by highly visible cyber events or by regulatory alerts.

6. The FMI should incorporate lessons learned into the staff training, awareness programmes and materials, on an ongoing and dynamic basis. The FMI should utilise industry and authority initiatives related to 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: the percentage of the FMI's staff that have received cybersecurity training; the percentage of incidents reported within the required timeframe per applicable incident category; the percentage of vulnerabilities mitigated within a defined time period after discovery; and yearly reports monitoring progress of indicators, etc.

ADVANCING

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 could 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 and red team testing, etc.), exercises and external and internal intelligence in order to enhance and improve 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 its 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.

INNOVATING

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

ANNEX 1

Cyber Resilience Questionnaire

This questionnaire has been designed to identify the level of cyber resilience of Financial Market Infrastructures (FMIs) operated primarily by central banks or financial sector authorities following the Bank for International Settlements (BIS) Guidance on cyber resilience for financial market infrastructures, 2016 and the ECB's Cyber Resilience Oversight Expectations (CROE) for FMIs. It is structured in 6 sections; (i) Strategy and Governance, (ii) Identification, (iii) Protection, (iv) Detection, (v) Response and Recovery and (vi) Monitoring and Evaluation -including lessons learned. The objectives of each section of the questionnaire are listed below.

- **Strategy and Governance**: Having a framework that captures the objectives and arrangements in place to ensure the safe and efficient operation of FMIs is necessary. Operational resilience of an FMI can be measured against their readiness to identify, protect, detect, respond and recover from a cyber threat. Building on the CPMI-IOSCO Principles for FMIs, in particular the following: (i) P2 on Governance, (ii) P3 on framework for risk management, (iii) P8 on settlement finality, (iv) P17 on operational risks and (v) P20 on FMI links, the following guiding questions could help identify better the level of cyber resilience of a given FMI.
- **Identification**: It is important that FMIs identify critical business functions and information and technological assets that should be protected against compromise. An FMI as a networked ecosystem involves systems and processes that are interconnected with systems and processes of entities in the ecosystem (e.g. other infrastructures, vendors, system participants).
- **Protection**: Effective security controls should protect the confidentiality, integrity and availability of assets and its services. Data should be protected both in transit and at rest. Protective measures should balance threat landscape, the risk tolerance of the FMI and the systemic role of the FMI in the financial system. Management response can either contain or escalate the problem therefore governance is a key pillar of a cyber security framework for FMIs.

- **Detection**: Strong cyber resilience requires the ability of an FMI to detect anomalies (attempted infiltration, movement of an attacker, across systems, exploitation of vulnerabilities) unlawful or unauthorized access to data, data abuse) and events that indicate a potential cyber incident. This early warning allows FMIs to adopt countermeasures against a potential incident and proactive containment of actual breaches.
- **Response and Recovery**: FMIs to run smoothly must be able to settle obligations when they are due and at the minimum by the end of the value date. It is therefore important that critical operations resume within 2 hours after a cyber incident resulted in disruption. Effective continuity plans are essential to meet this objective. The capacity of an FMI to return to normal operations and limit damage to the organization and its stakeholders continue after the incident.
- **Monitoring the Effectiveness of the Framework**: FMIs should use tools such as testing, continuous situational awareness regarding the threat landscape as well as re-evaluating the adequacy of the framework to the evolving nature of the cyber threats to maintain adequate levels of cyber resilience preserving the safety and efficiency of the FMIs.

The guiding questions and assessment tool can be found below.

	GUIDING QUESTIONS: STRATEGY AND GOVERNANCE
1.1	Is there a Strategy on Cybersecurity already developed and supported by a framework?
1.2	Does the framework include technology, policies, procedures and training and is documented?
1.3	Are international Standards considered when defining the framework and strategy?
1.4	The Board approves the Strategy?
1.5	The organization's strategy is aligned with the National Strategy on Cyber Security?
1.6	Members of the Board understand key cybersecurity controls in place?
1.7	The Board includes one Director with clear understanding of information security and cybersecurity?
1.8	The Board reviews the Cybersecurity strategy on a yearly basis?
1.9	The Board reviews the Cybersecurity strategy whenever there is a change in the organization's information technology?
1.10	The Board reviews the Cybersecurity strategy whenever there is a new threat?
1.11	Cybersecurity Policies include a Chief Information Security Officer (CISO)?
1.12	Cybersecurity Policies include a clear definition of objectives, roles and responsibilities of Board and Management?
1.13	CISO reports to the CEO and is independent from areas using the organization's information technology assets?
1.14	Management and Staff are held accountable for complying with information security policies?
1.15	The organization's ICT strategy includes outsourcing critical information technology services (e.g. storage, data processing, data analytics) ?
1.16	The organization's Cybersecurity Strategy includes purchasing insurance against cyber incidents?
1.17	The Cybersecurity strategy includes data breach notification processes to stakeholders and authorities?
1.18	The strategy includes clear procedures (e.g. communication protocols, decision making processes) to make timely decisions in case of a cyber attack?
1.19	The organization has a specific budget covering cybersecurity related needs?
1.20	The Board discusses the cybersecurity resources needs (e.g. budget, technology and HHRR) once a year?
1.21	Is the Strategy communicated to all units within the organization?
1.22	Is collaboration with other FMIs and their stakeholders considered in the strategy?

1.23	Are key elements of the Strategy being discussed with other FMIs and stakeholders?
1.24	Is the FMI part of a CERT or other arrangement with stakeholders ensuring cooperation in cyber security aspects?

	GUIDING QUESTIONS: IDENTIFICATION
2.1	Is there an exhaustive asset inventory of all system accounts?
2.2	Does the inventory include all business functions, information and technologies?
2.2	Does the inventory take into consideration the interdependencies of functions and business processes?
2.3	Are business functions classified according to its relevance for the efficient performance of the FMI?
2.4	If yes, is the inventory updated on a regular basis?
2.5	Is there a simplified map of network resources, with associated IP addressing plan?
2.6	Are risk assessments conducted prior to the deployment of new technologies to identify potential vulnerabilities?
2.7	Are risk assessments conducted prior to the deployment of new products to identify potential vulnerabilities?
2.8	Are risk assessments conducted prior to the deployment of new services to identify potential vulnerabilities?
2.9	Are business processed dependent on third party service providers listed and documented?
2.10	Are access rights and credentials recorded and kept up to date?
2.11	Are other critical infrastructures identified (e.g. energy, telecommunications)?
2.12	Is there any coordination mechanism between the entities in the FMIs ecosystem?

	GUIDING QUESTIONS: PROTECTION
3.1	Are security measures in place to protect software, networks and hardware against cyber incidents?
3.2	Are those measures documented and based on International Standards?
3.3	Is the network segmented into multiple trust zones allowing for segregation of data and systems?
3.4	Are system users access profiles clearly defined and documented?
3.5	Automated processes detect and block unauthorized changes to software and hardware?
3.6	There is defense-in-depth strategy (i.e. multiple independent security controls to provide redundancy) applied?
3.7	Has a bespoke information security management system (ISMS) based on international standards (ISO) has been developed?
3.8	There is a secure boundary that protects the network infrastructure using network perimeter tools (e.g. router, firewall, IPS, proxies, VPN, DMZ)?
3.9	There are mechanisms in place to limit and terminate system and remote sessions after a pre-defined period of inactivity?
3.10	There are controls that prevent non-controlled devices to connect to its internal network (e.g. personal devices, rogue access point) and endpoints (e.g. removable media) from inside and outside the premises?
3.11	Legacy technologies are regularly scanned (at least every month) to identify potential vulnerabilities and seek upgrade opportunities?
3.12	Are there policies and controls that prevent users from installing unauthorized applications in systems and devices?
3.13	Are Remote access controls based on multifactor authentication (e.g. password, smart card, finger print)?

3.14	Is there a dedicated password policy that specify password characteristics such as complexity, renewal period, and limits to password attempts?
3.15	Have appropriate controls (e.g. end-to-end encryption, authentication and access control) to protect data at rest, in use and in transit been developed?
3.16	Are there dedicated controls to prevent unauthorized access to cryptographic keys?
3.17	A change management process is in place to request and approve changes to system configurations, hardware, apps and security tools?
3.18	Is there a comprehensive patch management policy and processes?
3.19	Are there policies, procedures and controls established for granting, revoking, employee physical and logical access to its systems?
3.20	Are there processes and technologies to monitor privileged user's activity and access to critical systems?
3.21	Is there training provided (at least once a year) to the entire staff to support information security policy compliance and incident reporting?
3.22	Does high risk staff (e.g. management, system administrators, software developers) receive dedicated security awareness training as relevant for their responsibilities?
3.23	Is there an inventory of participants and third-party service providers?
3.24	Are contractual arrangements between the FMI operator and third-party service providers in place?
3.25	Are contractual arrangements (service level agreements -SLA) between the FMI operator and third-party service providers in place?
3.26	SLAs include confidentiality provisions regarding data?
3.27	SLAs include accountability provisions regarding data (corruption, unauthorized access and loss), systems and networks failures related to the service provided?
3.28	Risks assessments are conducted to service providers before entering into contract with them?
3.29	Security measures allow the identification of anomalies that could result in data corruption, loss caused by legitimate users?
3.30	Do you have a cyber insurance policy?

	GUIDING QUESTIONS: DETECTION
4.1	Has your organization defined, considered and documented the baseline profile of system activities to help detect deviation from the baseline?
4.2	Are criteria, parameters and triggers to enable alerts in place?
4.3	Are there multi-layered detection controls covering people, processes and technology which support quick attack detection and isolation of infected points?
4.4	Are detection capabilities informed by threat or vulnerability information (public and not yet publicly known) ?
4.5	Are there alert thresholds defined for monitoring and detection systems in order to trigger and facilitate the incident response process?
4.6	Are logs with incident information in place and stored safely?
4.7	Are tools in place to monitor access by service providers?
4.8	Is there a cyber threat intelligence program in place?
4.9	Current processes monitor activities which are not in line with the security policy?

	GUIDING QUESTIONS: RESPONSE AND RECOVERY
5.1	Do you have in place an Incident Response Plan (IRP) and a Security Incident Response Team (SIRT)?
5.2	Are systems and processes of critical functions are designed to limit the impact of cyber incidents?
5.3	Do systems and processes allow the identification of the source of the attack?

5.4	Do policies, processes and procedures allow to contain the attack before it damages critical systems or business processes?
5.5	Are activity logs are maintained and available for future investigation?
5.6	Are procedures and policies are in place to facilitate a rapid investigation of cyber incidents?
5.7	Is the FMI able to determine the systems and data compromised after a cyber incident?
5.8	Does your Business continuity plan (BCP) and disaster recovery plan (DRP) take into consideration cyber-attacks?
5.9	Are penetration testing conducted frequently (at least once a year)?
5.10	Can systems and business processes be restored from a trusted back-up?
5.12	Is there an internal communication plan to address cybersecurity incidents that includes communication protocols for key internal stakeholders (e.g. relevant business units, senior management, risk management, board of directors, etc.)?
5.13	Is there an external communication plan to address cybersecurity incidents that includes communication protocols and draft pre-scripted communications for key external stakeholders (i.e. customers, media, critical service providers, etc.)?
5.14	Does your DRP have in place a change of all user credentials and access controls?
5.15	Do policies, procedures and systems allow the FMI to resume operations in 2 hours since the cyber incident?
5.16	Does the back-up system provide the same level of service to system participants than the primary site?
5.17	Do systems allow the quick recovery of data after a data breach ensuring data integrity?
5.18	Does the IRP include mechanisms to respond to requests from law enforcement agencies, consumers, partners, system participants and service providers?
5.19	The IRP designed involves the participation of the legal counsel, security and ICT and the Board?
5.20	The IRP designed includes mechanisms to analyze the damage and measure the loss exposure?
5.21	Laws and regulations allow the evidence (digital audit trail) to be presented in court?
5.22	Laws and regulations establish a specific timeline for data breach notification to authorities?
5.23	Laws and regulations establish a specific timeline for data breach notification to public at large?

	GUIDING QUESTIONS: MONITORING TOOLS
6.1	The FMI has a testing program in place?
6.2	The testing program is integrated in the risk management framework?
6.3	Tests are undertaken by independent parties (internal or external) ?
6.4	Weaknesses identified are classified and remedial actions prioritized?
6.5	Board and Senior Management incorporate the lessons learned into the cyber security strategy?
6.6	The testing program includes critical systems, applications and data and back-up solutions?
6.7	Tests are conducted at least once a year?
6.8	Vulnerability assessments take into consideration regulations, policy and configuration?
6.9	Tests performed are designed based on different scenarios (e.g. one of them including a potential financial loss)?
6.1	Penetration tests to external facing services and internal networks and systems are conducted once a year?
6.11	Ethical hacking is conducted to critical business processes, systems and networks?
6.12	A bug bounty program is in place?
6.13	FMI is part of a threat and vulnerability information sharing platform?
6.14	Information obtained is analyzed and made available to relevant staff?

6.15	Lessons learned are captured into the cyber security framework?
6.16	An information sharing policy is defined?
6.17	Does the information to be shared include?: (a) Attacker's name (b) Indicators for compromise (c) Threats and vulnerabilities (d) Modus operandi
6.18	Does the information policy include?: (a) Circumstances to share information (b) Recipients of the information (e.g. system participants, vendors, authorities, interconnected FMIs) (c) Actions to be taken based on information received

ANNEX 2

Guidance on the Senior Executive[5]

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 carries out the following tasks, in particular.
   (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 vs. cyber resilience).
   (b) Participating in cyber risk management.
   (c) Producing cyber resilience guidelines and, where appropriate, any other relevant rules, as well as checking compliance.
   (d) Influencing the FMI's cyber resilience processes, monitoring IT service providers' involvement and assisting in any related tasks.
   (e) Helping to produce and update 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 them to the senior management and the Board.
   (j) Continuously surveying threats applicable to IT assets.
   (k) Initiating and coordinating measures to raise awareness on cyber resilience and training sessions.
   (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.

5. Annexes from the ECB CROE

3. In terms of organisation and processes, the Senior Executive or CISO must be independent so as to avoid any potential conflicts of interest. Therefore, the following measures, in particular, are expected to be applied:
   (a) organisational set-up to ensure that 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[9] 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;
   (d) requirement for all employees in the FMI and IT service providers to report any incidents relevant to the cyber resilience of the FMI, according to the escalation procedure.
4. The FMI should have its own senior executive or CISO in-house, depending on the FMI's specific structure and organisational set-up. To the extent permitted by the national authority and in cases of group entities, this could include a group-wide CISO.

9. We do observe organizational 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.

ANNEX 3

Glossary[6]

The Glossary contains the definitions of the core terms used throughout the CROE. The terms have been largely adopted from the Guidance[6] and the Financial Stability Board's Cyber Lexicon.[7] For more technical terms, users should refer to glossaries produced by the international standard setters in this field, such as the International Organization for Standardization (ISO), ISACA (previously known as the Information Systems Audit and Control Association), the SANS Institute and the US National Institute of Standards and Technology.

Access control	Means to ensure that access to *assets* is authorised and restricted based on business and security requirements. *Source:* ISO/IEC 27000:2018/FSB Cyber Lexicon
Advanced persistent threat (APT)	A *threat actor* that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple *threat vectors.* The *advanced persistent threat:* (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to execute its objectives. *Source:* Adapted from NIST/FSB Cyber Lexicon
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: ISACA Fundamentals/FSB Cyber Lexicon
Authenticity/ authentication	Property that an entity is what it claims to be. Source: ISO/IEC 27000:2018/FSB Cyber Lexicon
Availability	Property of being accessible and usable on demand by an authorised entity. Source: ISO/IEC 27000:2018/FSB Cyber Lexicon

6. Annexes from the ECB CROE
7. See CPMI-IOSCO (June 2016), "Guidance on cyber resilience for financial market infrastructures".
8. See FSB (November 2018), "Cyber Lexicon"

Business process	A collection of linked activities that takes one or more kinds of input and creates an output that is of value to an FMI's stakeholders. A business process may comprise several assets, including information, ICT resources, personnel, logistics and organisational structure, which contribute either directly or indirectly to the added value of the service. *Source:* CPMI-IOSCO Guidance
Capabilities	People, processes and technologies used to identify, mitigate and manage its cyber risks to support its objectives. *Source:* CROE
Compromise	Violation of the security of an *information system.* *Source:* Adapted from ISO 21188:2018/FSB Cyber Lexicon
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. *Source:* Adapted from ISO/IEC 27000:2018/FSB Cyber Lexicon
Configuration management	The activity of managing the configuration of an information system throughout its life cycle. *Source:* ISO/IEC 10032:2003
Critical operations	Any activity, function, process or service, the loss of which, for even a short period of time, would materially affect the continued operation of an FMI, its participants, the market it serves, and/or the broader financial system. *Source:* CPMI-IOSCO Guidance
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and *information systems.* *Source:* Adapted from CPMI-IOSCO Guidance (citing NICCS)/FSB Cyber Lexicon
Cyber attack	The use of an exploit by an adversary to take advantage of a weakness(es) with the intention of achieving an adverse effect on the ICT environment. *Source:* CPMI-IOSCO Guidance
Cyber event	Any observable occurrence in an *information system. Cyber events* sometimes provide indication that a *cyber incident* is occurring. *Source:* Adapted from NIST (definition of "Event")/FSB Cyber Lexicon
Cyber governance	Arrangements an organisation puts in place to establish, implement and review its approach to managing cyber risks. *Source:* CPMI-IOSCO Guidance
Cyber incident	A cyber event that: (i) jeopardises the *cybersecurity* of an *information system* or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not. *Source:* Adapted from NIST (definition of "Incident")/FSB Cyber Lexicon
Cyber incident response plan	The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a *cyber incident.* *Source:* Adapted from NIST (definition of "Incident Response Plan") and NICCS/FSB Cyber Lexicon
Cyber resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incidents.* *Source:* Adapted from CERT Glossary (definition of "Operational resilience"), CPMI-IOSCO Guidance and NIST (definition of "Resilience")/FSB Cyber Lexicon
Cyber resilience framework	Consists of the policies, procedures and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces. *Source:* CPMI-IOSCO Guidance

Cyber resilience strategy	An FMI's high-level principles and medium-term plans to achieve its objective of managing cyber risks. *Source:* CPMI-IOSCO Guidance
Cyber risk	The combination of the probability of *cyber incidents* occurring and their impact. *Source:* Adapted from CPMI-IOSCO Guidance, ISACA Fundamentals (definition of "Risk") and ISACA Full Glossary (definition of "Risk")/FSB Cyber Lexicon
Cybersecurity	Preservation of *confidentiality, integrity* and *availability* of information and/or *information systems* through the *cyber* medium. In addition, other properties, such as *authenticity, accountability, non-repudiation* and *reliability* can also be involved. *Source:* Adapted from ISO/IEC 27032:2012/FSB Cyber Lexicon
Cyber threat	A circumstance with the potential to exploit one or more *vulnerabilities* that adversely affects *cybersecurity*. *Source:* Adapted from CPMI-IOSCO Guidance/FSB Cyber Lexicon
Data breach/ integrity	*Compromise* of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed. *Source:* Adapted from ISO/IEC 27040:2015/FSB Cyber Lexicon
Defence in depth	Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation. *Source:* Adapted from NIST and FFIEC/FSB Cyber Lexicon
Disruption	An event affecting an organisation's ability to perform its critical operations. *Source:* CPMI-IOSCO Guidance
Ecosystem	A system or group of interconnected elements, formed linkages and dependencies. For an FMI, this may include participants, linked FMIs, service providers, vendors and vendor products. *Source:* CPMI-IOSCO Guidance
Exploit	A defined way to breach the security of *information systems* through *vulnerability*. *Source:* ISO/IEC 27039:2015/FSB Cyber Lexicon
Financial market infrastructure (FMI)	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions. *Source:* CPMI-IOSCO Guidance
Forensic investigation	The application of investigative and analytical techniques to gather and preserve evidence from a digital device impacted by a cyber attack. *Source:* CPMI-IOSCO Guidance
Forensic readiness	The ability of an FMI to maximise the use of digital evidence to identify the nature of a cyber attack. *Source:* CPMI-IOSCO Guidance
Identity and access management (IAM)	Encapsulates people, processes and technology to identify and manage the data used in an *information system* to authenticate users and grant or deny access rights to data and system resources. *Source:* Adapted from ISACA Full Glossary/FSB Cyber Lexicon
Incident response team (IRT) [also known as CERT or CSIRT]	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle. *Source:* ISO/IEC 27035-1:2016/FSB Cyber Lexicon
Indicators of compromise (IoCs)	Identifying signs that a *cyber incident* may have occurred or may be currently occurring. *Source:* Adapted from NIST (definition of "Indicator")/FSB Cyber Lexicon

Information asset	Any piece of data, device or other component of the environment that supports information-related activities. In the context of this document, information assets include data, hardware and software. Information assets are not limited to those that are owned by the entity. They also include those that are rented or leased, and those that are used by service providers to deliver their services. *Source:* CPMI-IOSCO Guidance
Information sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events. *Source:* Adapted from NICCS/FSB Cyber Lexicon
Information system	Set of applications, services, IT *assets* or other information-handling components, which includes the operating environment. *Source:* Adapted from ISO/IEC 27000:2018/FSB Cyber Lexicon
Integrity	Property of accuracy and completeness. *Source:* ISO/IEC 27000:2018/FSB Cyber Lexicon
Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems. *Source:* Adapted from ISO/IEC 27032:2012/FSB Cyber Lexicon
Maturity model	A mechanism to have cyber resilience controls, methods and processes assessed according to management best practice, against a clear set of external benchmarks. *Source:* Adapted from CPMI-IOSCO Guidance
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities. *Source:* ISO 27000:2018/FSB Cyber Lexicon
Patch management	The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs. *Source:* NIST/FSB Cyber Lexicon
Penetration testing	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an *information system.* *Source:* NIST/FSB Cyber Lexicon
Recovery point objective (RPO)	Point to which information used by an activity is to be restored to enable the activity to operate on resumption. *Source:* Adapted from ISO 22300:2018
Recovery time objective (RTO)	Period of time following an incident within which a product or service or an activity is to be resumed, or resources are to be recovered. *Source:* Adapted from ISO 22300:2018
Red team testing	A controlled attempt to compromise the *cyber resilience* of an entity by simulating the *tactics, techniques and procedures* of real-life *threat actors.* It is based on targeted *threat intelligence* and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. *Source:* G-7 Fundamental Elements/FSB Cyber Lexicon
Reliability	Property of consistent intended behaviour and results. *Source:* ISO/IEC 27000:2018/FSB Cyber Lexicon
Resilience by design	The embedding of security in technology and system development from the earliest stages of conceptualisation and design. *Source:* CPMI-IOSCO Guidance

Resumption	To recommence functions following a cyber incident. An FMI should resume critical services as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability. *Source:* CPMI-IOSCO Guidance
Security operations centre (SOC)	A function or service responsible for monitoring, detecting and isolating incidents. *Source:* CPMI-IOSCO Guidance
Situational awareness	The ability to identify, process and comprehend the critical elements of information through a *cyber threat intelligence* process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. *Source:* CPMI-IOSCO Guidance/FSB Cyber Lexicon
Social engineering	A general term for trying to deceive people into revealing information or performing certain actions. *Source:* Adapted from FFIEC/FSB Cyber Lexicon
Tactics, techniques and procedures (TTPs)	The behaviour of a *threat actor.* A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. *Source:* Adapted from NIST 800-150/FSB Cyber Lexicon
Threat actor	An individual, a group or an organisation believed to be operating with malicious intent. *Source:* Adapted from STIX/FSB Cyber Lexicon
Threat intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. *Source:* NIST 800-150/FSB Cyber Lexicon
Threat vector	A path or route used by the threat actor to gain access to the target. *Source:* Adapted from ISACA Fundamentals/FSB Cyber Lexicon
Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats. *Source:* Adapted from CPMI-IOSCO Guidance and ISO/IEC 27000:2018/FSB Cyber Lexicon
Vulnerability assessment	Systematic examination of an *information system* and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. *Source:* Adapted from NIST/FSB Cyber Lexicon


THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP


EUROPEAN CENTRAL BANK