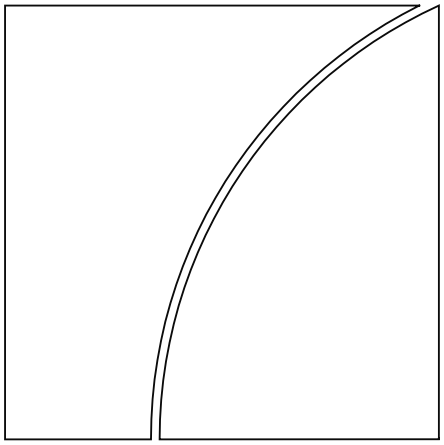
Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions

Consultative report

Guidance on cyber resilience for financial market infrastructures



November 2015

BANK FOR INTERNATIONAL SETTLEMENTS

OICV-IOSCO

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

ISBN 978-92-9197-288-3 (online)

Contents

Executive summary[1]

Purpose. The purpose of this document is to provide guidance for financial market infrastructures (FMIs)[2] to enhance their cyber resilience. The safe and efficient operation of FMIs is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In this context, the level of operational resilience of FMIs, including cyber resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy.

Outline. The guidance is presented in chapters that outline five primary risk management categories and three overarching components that should be factored across an FMI's cyber resilience framework. The risk management categories are: governance; identification; protection; detection; and response and recovery. The overarching components are: testing; situational awareness; and learning and evolving. In order to achieve resilience objectives, investments across these guidance categories can be mutually reinforcing and should be considered jointly.

Relationship with the PFMI. This document provides supplemental guidance to the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI), primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20). It is not intended to impose additional standards on FMIs beyond those set out in the PFMI, but instead the guidance details the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability.

Broad relevance. While the guidance is directly aimed at FMIs, it is important for FMIs to take on an active role in outreach to their participants and other relevant stakeholders to promote understanding and support of resilience objectives and their implementation. Given the extensive interlinkages and interdependencies in the financial system, adequate cyber security practices at an FMI do not necessarily ensure cyber resilience in the markets it serves. In particular, the markets' overall cyber resilience is dependent not only on the resilience of a single FMI, but also on that of interconnected FMIs, of service providers and of the participants.

Collaboration. Effective solutions may necessitate collaboration between FMIs and their stakeholders as they seek to strengthen their own cyber resilience. The outcome of such collaboration should be considered in their individual and collective strategic planning. Efforts to coordinate the design of resilience solutions may bring enhanced strategies forward in a more timely and efficient way. Increased resilience can be achieved if heightened resilience objectives are explicitly incorporated in the design and review of systems and processes. Because the cyber resilience of FMIs supports broader financial stability objectives and in light of significant interdependencies in clearing and settlement processes, it is important for authorities to cooperate, recognising that such cooperation may help authorities consider, where appropriate, consistency of direction in their oversight and supervision of both FMIs and their relevant stakeholders. Moreover, authorities and FMIs may need to call upon technology companies and other firms to help identify and develop efficient and effective solutions.

Governance. Consistent with effective management of other forms of risk faced by an FMI, sound governance is key. Cyber governance refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks. Effective governance should start with a clear

[1] Technical terms are explained in the glossary on page 23.

[2] Consistent with the definition in the PFMI, the term "FMI" refers to systemically important payment systems, central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs). Relevant authorities, however, may decide to apply this guidance to types of infrastructure not formally covered by this report.

and comprehensive cyber resilience framework that accords a high priority to the safety and efficiency of the FMI's operations while supporting broader financial stability objectives. The framework should define the FMI's cyber resilience objectives, as well as the requirements for people, processes and technology necessary to manage cyber risks. This framework should include timely communication and collaboration with relevant stakeholders. It is essential that the framework be supported by clearly defined roles and responsibilities of the FMI's board (or equivalent) and its management, and it is incumbent upon its board and management to create a culture which recognises that staff at all levels, as well as interconnected service providers, have important responsibilities in ensuring the FMI's cyber resilience. The chapter on governance includes guidance on the basic elements of an FMI's cyber resilience framework and how an FMI's governance arrangements should support that framework.

Identification. Given that FMIs' operational failure can negatively impact financial stability, it is important that FMIs identify their critical business functions and supporting information assets that should be protected, in order of priority, against compromise. The chapter on identification outlines how an FMI should identify and classify business processes, information assets, system access and external dependencies. This helps the FMI to better understand its internal situation, the cyber risks that it bears from and poses to entities in its ecosystem, and how it can coordinate with relevant stakeholders when designing and implementing its cyber resilience efforts.

Protection. Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of its assets and services. The chapter on protection urges FMIs to implement appropriate and effective controls and design systems and processes in line with leading cyber resilience and information security practices to prevent, limit and contain the impact of a potential cyber incident.

Detection. An FMI's ability to detect the occurrence of anomalies and events indicating a potential cyber incident 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. Given the stealthy and sophisticated nature of cyber attacks and the multiple entry points through which a compromise could take place, advanced capabilities to extensively monitor for anomalous activities are needed. The chapter on detection outlines monitoring and process tools to be used by an FMI for the detection of cyber incidents.

Response and recovery. Financial stability may depend on the ability of an FMI to settle obligations when they are due, at a minimum by the end of the value date. An FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a cyber disruption and to enable itself to complete settlement by the end of the day the disruption occurred, even in the case of extreme but plausible scenarios. Although authorities recognise the challenges that FMIs face in achieving cyber resilience objectives, it is also recognised that current and emerging practices and technologies may serve as viable options to attain those objectives.[3] Furthermore, the rationale for establishing this resumption objective stands irrespective of the challenge to achieve it. Continuity planning is essential in meeting related objectives. The chapter on response and recovery provides guidance on how an FMI should respond in order to contain, resume and recover from successful cyber attacks.

Testing. Once employed within an FMI, all elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness. Sound testing regimes produce findings that should be used to identify gaps against stated resilience objectives and provide credible and meaningful inputs to the FMI's management of cyber risks. The chapter on testing provides guidance on areas that should be included in an FMI's testing programme and how results from testing can be used to improve its cyber resilience framework.

[3] See CPMI, *Cyber resilience in financial market infrastructures*, Section 4.3.3, for potential solutions provided by FMIs during the CPMI industry interviews.

Situational awareness. Strong situational awareness can significantly enhance an FMI's ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber attacks that are not prevented. 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. The chapter on situational awareness provides guidance on how an FMI could proactively monitor the cyber threat landscape, and acquire and make effective use of actionable threat intelligence to validate its risk assessments, strategic direction, resource allocation, processes, procedures and controls with respect to building cyber resilience. This chapter also stresses the importance of an FMI's active participation in information-sharing arrangements and collaboration with trusted stakeholders within and outside the industry to enhance resilience of the FMI and its ecosystem.

Learning and evolving. The last chapter emphasises the importance of implementing an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and strategies to mitigate those risks. FMIs should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organisation.

1. Introduction

1.1 Purpose of the guidance

1.1.1 *Purpose*. The purpose of this document is to provide guidance for FMIs to enhance their cyber resilience. In the context of this guidance, "cyber resilience" is an FMI's ability to anticipate, withstand, contain and rapidly recover from disruption caused by a cyber attack. FMIs, which facilitate the clearing, settlement and recording of monetary and other financial transactions, play a critical role in fostering financial stability.[4] While safe and efficient FMIs contribute to maintaining and promoting financial stability and economic growth, FMIs may also concentrate risk. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In this context, the level of operational resilience of FMIs, including cyber resilience, can be a decisive factor in the overall resilience of the broader financial system.

1.1.2 *Cyber risks in the PFMI*. In April 2012, the Committee on Payment and Settlement Systems (CPSS (now CPMI)) and the Technical Committee of the International Organization of Securities Commissions (IOSCO) published the Principles for Financial Market Infrastructures (PFMI).[5] The main public policy objectives were "to enhance safety and efficiency in payment, clearing, settlement, and recording arrangements, and more broadly, to limit systemic risk and foster transparency and financial stability". The PFMI recognise operational risk, including cyber risk, as a specific key risk faced by FMIs, and state that an FMI should have governance arrangements and objectives to manage these risks within a comprehensive risk management framework.[6] The management of cyber risks is included in the expectations outlined in Principle 17 and its supporting key considerations.

1.1.3 *Cyber risks are unique*. While cyber risks should be managed as part of an FMI's overall operational risk management framework, some unique characteristics of cyber risk present challenges to FMIs' traditional operational risk management frameworks:

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

b. Second, there is a broad range of entry points through which an FMI could be compromised. As a result of their interconnectedness, cyber attacks could come through an FMI's participants, linked FMIs, service providers, vendors and vendor products. FMIs could themselves become a channel to further propagate cyber attacks – for example, via the distribution of malware to interconnected entities. Unlike physical operational disruptions, cyber risk posed by an interconnected entity is not necessarily related to the degree of that entity's relevance to the FMI's business. From a cyber perspective, the small-value/volume participant or a vendor providing non-critical services may be as risky as a major participant or a critical service provider. Internally, the risk of insider threat from rogue or careless employees opens up yet another avenue for possible compromises.

c. Third, certain cyber attacks can render some risk management and business continuity arrangements ineffective. For example, automated system and data replication arrangements that

[4] See also PFMI, paragraphs 1.3 and 1.20.

[5] See http://www.bis.org/cpmi/publ/d101.htm.

[6] Section 2.0, "Overview of key risks in financial market infrastructures"; paragraph 2.9, "Operational risk"; and Principle 3, "Framework for the comprehensive management of risks".

are designed to help preserve sensitive data and software in the event of a physical disruptive event might in some instances fuel the propagation of malware and corrupted data to backup systems. Overall, a cyber attack's potential to cause significant service disruptions to the broader financial system dictates the urgency of having an effective approach in place to manage it, and to ensure that service resumption does not introduce additional risks to an FMI or the wider financial sector.

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

1.1.4 *The most relevant principles from the PFMI.* This document is intended to provide supplemental guidance to the PFMI regarding cyber resilience, primarily in the context of those principles listed in Box 1. The guidance focuses on the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities, with the objective of limiting the increasing risks that cyber threats pose to their smooth operation and to financial stability.

Box 1

Key PFMI principles informing the guidance

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

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

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

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

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

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

a. Principle 8 on settlement finality states: "An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide

final settlement intraday or in real time."[7] The finality of settlement is important for the stability of the financial system. Credit, liquidity, market and legal risks are allocated among the parties to payments and securities transactions based on the principle of finality. The liquidity condition of financial institutions and their customers depends on the certainty of the assumption that transactions that are considered final will remain as such. In this guidance, the settlement finality principle is treated as a given.

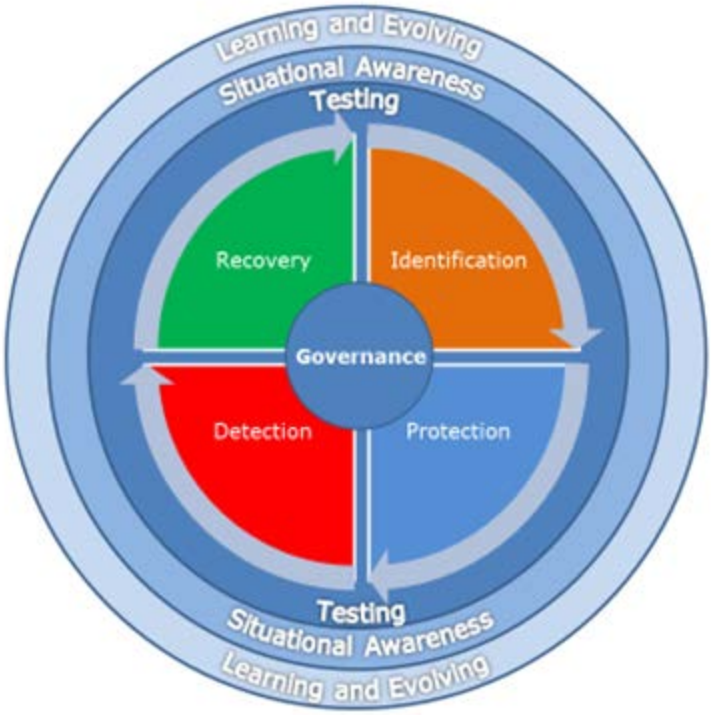
b. Since financial stability may indeed depend on FMIs to process transactions and settle obligations when they are due, the PFMI impose stringent expectations on FMIs in the area of operational risk. Of significant importance is an FMI's ability to resume critical operations rapidly. Specifically, Key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

1.2 Design and organisation of the guidance

1.2.1 *Design*. This guidance is presented in chapters that outline five primary risk management categories and three overarching components that should be factored across an FMI's cyber resilience strategy and framework. The risk management categories are: (i) governance; (ii) identification; (iii) protection; (iv) detection; and (v) response and recovery. The overarching components are: (i) testing; (ii) situational awareness; and (iii) learning and evolving. Categories similar to those used in commonly recognised cyber resilience frameworks have been used as a logical way to organise and articulate related expectations. Figure 1 below depicts the relationship among these cyber resilience guidance categories.

[7] See PFMI, paragraph 2.9, "Operational risk"; Principle 3, "Framework for the comprehensive management of risks"; and Principle 8, "Settlement finality".

Cyber resilience guidance components Figure 1



1.2.2 *Principles-based*. The guidance is principles-based, recognising that the dynamic nature of cyber threats requires evolving methods to mitigate these threats. Guidance requiring specific measures today may quickly become ineffective in the future. In some cases, however, specific examples are used to illustrate and clarify certain points.

1.2.3 *ICT controls should be present*. Importantly, the guidance is not intended to replace existing established information and communication technology (ICT) control guidance. A strong ICT control environment is fundamental and a critical component of an FMI's overall cyber resilience. Key consideration 5 of Principle 17 of the PFMI states that "an FMI should have comprehensive physical and information security policies that address all potential vulnerabilities and threats". In practice, in the context of cyber risk management, CPMI and IOSCO authorities expect FMIs to maintain robust ICT controls and consistently demonstrate effective control environments. This point is particularly important as many successful cyber attacks have been attributed to weak or inadequate ICT controls, even basic ones.

1.3 Expected usage

1.3.1 *Target group*. This guidance is first and foremost directed to FMIs as defined in the PFMI, namely: systemically important payment systems, central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs). Relevant authorities, however, may decide to apply this guidance to types of infrastructure not formally covered by this report.[8]

[8] In some cases, exchanges or other market infrastructures may own or operate entities or functions that perform centralised clearing and settlement processes that are covered by the guidance in this report. In general, however, this guidance is not

1.3.2 *Role of the board and senior management*. The guidance should be considered an important reference for an FMI's board of directors and senior management, given that active involvement on the part of the board and senior management is instrumental in ensuring cyber resilience. The guidance should also be regarded as a reference by all FMI personnel responsible for designing, implementing or overseeing elements of the FMI's cyber resilience framework.

1.3.3 *Stakeholder considerations*. While the guidance is directly aimed at FMIs, it is important for FMIs to promote among their participants, service providers and other relevant stakeholders an understanding of the FMIs' resilience objectives, and to require appropriate action to support their implementation. Given the extensive interlinkages and interdependencies in the financial system, adequate cyber resilience is dependent not only on the resilience of a single FMI, but also on that of interconnected FMIs, of service providers and of the participants. Achieving effective solutions may require FMIs to collaborate with their stakeholders as they seek to strengthen their own cyber resilience. Efforts to coordinate the design of resilience solutions may bring enhanced strategies forward in a more timely and efficient way. The outcome of such collaboration should be considered in their individual and collective strategic planning. Increased resilience can be achieved if heightened resilience objectives are explicitly incorporated in the ongoing improvement or redesign of systems and processes. Because the cyber resilience of FMIs supports broader financial stability objectives and in light of significant interdependencies in clearing and settlement processes, it is important for authorities to cooperate, recognising that such cooperation may help authorities consider, where appropriate, consistency of direction in their oversight and supervision of both FMIs and their relevant stakeholders. Moreover, authorities and FMIs may need to call upon technology companies and other service providers to help identify and develop efficient and effective solutions.

1.3.4 *Swift and sustained actions to enhance cyber resilience*. It is recognised that FMIs may be at different levels of cyber resilience capability, and enhancing resilience could take time. Nevertheless, concerted redesign strategies over a reasonable and definite time period can result in cost-effective improvements. Given FMIs' systemic importance and extensive interconnections, and hence potential for risk contagion between FMIs, their participants and their service providers as well as other stakeholders in the transaction chain, FMIs should take appropriate, swift and sustained actions to enhance their cyber resilience. Such efforts should take into account this guidance.

1.3.5 *Ongoing efforts to improve FMIs' cyber resilience.* No cyber resilience framework can be expected to fully mitigate all cyber risks. Therefore, FMIs should make ongoing efforts to adapt, evolve and improve their cyber resilience, to increase the level of difficulty for perpetrators to carry out their exploits, and to improve the FMIs' capabilities to resume critical operations and recover from successful cyber attacks (see Chapter 9, "Learning and evolving"). In order to achieve resilience objectives, investments across the guidance categories included in this document can be mutually reinforcing and should be considered jointly.

1.3.6 *Guidance implementation in the context of the relevant legal framework*. The guidance is also pertinent to relevant regulatory, supervisory and oversight authorities as they carry out their responsibilities. It is recognised that national laws, regulations and institutional differences may determine how the guidance is adopted to achieve the intended objectives of this document. Accordingly, relevant regulatory, supervisory and oversight authorities, in carrying out their responsibilities, are urged to implement the guidance within the context of the legal framework of the relevant jurisdiction.

addressed to market infrastructures such as trading exchanges, trade execution facilities or multilateral trade compression systems.

2. Governance

2.1 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 governance should start with a clear and comprehensive cyber resilience strategy and framework that prioritises the security and efficiency of the FMI's operations, and supports financial stability objectives. The framework should define the FMI's cyber resilience objectives, as well as the requirements for people, processes and technology necessary 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 be supported by clearly defined roles and responsibilities of the FMI's board (or equivalent) and its management, and it is incumbent upon its board and management to create a culture which recognises that staff at all levels have important responsibilities in ensuring the FMI's cyber resilience.

Strong cyber governance ensures that an FMI has a systematic and proactive approach to managing the prevailing and emerging cyber threats that it faces. It also ensures that cyber risks are appropriately considered and managed at all levels within the organisation and that appropriate resources and expertise are consistently brought to bear to deal with these risks. This chapter provides guidance on what basic elements an FMI's cyber resilience framework should include and how an FMI's governance arrangements should support that framework.

2.2 Cyber resilience strategy and framework

2.2.1 *Cyber resilience strategy*. An FMI's board should ratify a cyber resilience strategy that clearly articulates a vision of and principles on how the FMI intends to address cyber risks. The cyber resilience strategy should be closely aligned with, and complementary to, the resilience framework, ensuring it is capable of achieving its strategic objectives and outcomes.

2.2.2 *Cyber resilience framework*. Complementing the cyber resilience strategy, an FMI should establish a documented cyber resilience framework to clearly articulate how it plans to effectively identify the cyber risks that it faces, determine its cyber resilience objectives and risk tolerance, and mitigate and manage its cyber risks to support its objectives. The FMI's cyber resilience framework should support financial stability objectives while ensuring the ongoing efficiency, effectiveness and economic viability of its services to its users. Therefore, framework objectives should aim to maintain and promote the FMI's ability to anticipate, withstand, contain and recover from cyber attacks, so as to limit the likelihood or impact of a successful cyber attack on its operations or on the broader financial system. The FMI's cyber resilience strategy and framework should be reviewed and updated periodically to ensure that they remain relevant.

2.2.3 *Cyber is more than just ICT*. The strategies and measures in an FMI's cyber resilience framework should not be restricted to securing the viability of its information technology operations alone, but should also cover people and processes. The framework should, in addition, include timely communication to enable the FMI to collaborate with relevant stakeholders to effectively respond to and recover from cyber attacks, whether on the FMI or on the financial system as a whole.

2.2.4 *Enterprise risk management*. At the broader level, the FMI's cyber resilience framework should be consistent with its enterprise operational risk management framework. Such consistency is important, and recognises that an FMI's cyber resilience framework is likely to overlap with the policies, procedures and controls that it has established to manage other areas of risks. For example, cyber risk should also be a consideration in an FMI's physical security framework (eg to limit access to critical ICT infrastructure) and its human resource policies (eg to manage "insider" threats).

2.2.5 *An FMI's ecosystem*. An FMI should take an integrated and comprehensive view of the potential cyber threats it faces. In particular, an FMI's cyber resilience framework should consider how the FMI would regularly review and actively mitigate 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 in this document as an FMI's ecosystem.

2.2.6 *International and national standards*. There are many relevant international, national and industry-level standards, guidelines or recommendations that an FMI could use as a benchmark in designing its cyber resilience framework. Given FMIs' systemic importance, they should align themselves with leading standards, guidelines or recommendations, reflecting current industry best approaches in managing cyber threats, and incorporate the most effective cyber resilience solutions.

2.2.7 *Clear roles, responsibilities and accountability*. An FMI's cyber resilience framework should clearly define the roles and responsibilities within the organisation for managing cyber risk. In particular, an FMI should clearly define the responsibilities and accountability for decisions concerning cyber resilience, including in emergencies and in a crisis.

2.2.8 *Audits and compliance*. An FMI's internal processes should help the board and senior management assess and measure the adequacy and effectiveness of the FMI's cyber resilience framework. The adequacy of and adherence to an FMI's cyber resilience framework should be assessed and measured regularly through independent compliance programmes and audits carried out by qualified individuals. To assess and measure the effectiveness of its cyber resilience framework, an FMI is encouraged to use relevant metrics and maturity models as well as the results of its testing programme.[9]

2.3 Role of the board and senior management

2.3.1 *Ultimate responsibility*. An FMI's board is ultimately responsible for setting strategy and ensuring that cyber risk is effectively managed. The Board should endorse the FMI's cyber resilience framework, and set the FMI's tolerance for cyber risk. The board should be regularly apprised of the FMI's cyber risk profile to ensure that it remains consistent with the FMI's *risk* tolerance as well as the FMI's overall business objectives. As part of this responsibility, the board should consider how material changes to the FMI's products, services, policies or practices, and the threat landscape affect its cyber risk profile. Senior management should closely oversee the FMI's implementation of its cyber resilience framework, and the policies, procedures and controls that support it.

2.3.2 *Culture*. An FMI's 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 management should promote a culture that recognises that staff at all levels have important responsibilities in ensuring the FMI's cyber resilience, and lead by example.

2.3.3 *Skills*. In order for the board and senior management to have effective oversight of the FMI's cyber resilience framework and cyber risk profile, both groups should contain members with the appropriate skills and knowledge to understand and manage the risks posed by cyber threats, while ensuring that those skills remain current.

2.3.4 *Accountability*. In view of FMIs' growing reliance on ICT systems to support their businesses and operations, and the increasing cyber threat, FMIs should designate a senior executive to be responsible and accountable overall for the cyber resilience framework within the organisation. This role should have sufficient authority, independence, resources and access to the board. The senior executive performing this role should possess the requisite expertise and knowledge to competently plan and execute the cyber resilience initiatives.

[9] See Chapter 7, "Testing", and paragraph 9.3.1 in the "Learning and evolving" chapter.

3. Identification

3.1 Preamble

Given that FMIs' operational failure can negatively impact financial stability, it is crucial that FMIs identify which of their critical business functions 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 other dependencies to strengthen its overall cyber resilience posture. This chapter outlines areas where an FMI should identify and classify business processes, information assets as well as external dependencies.

3.2 Identification and classification[10]

3.2.1 *Identification of business functions and processes*. An FMI should identify its business functions and supporting processes and conduct a risk assessment to ensure that it thoroughly understands the importance of each function and supporting processes, and their interdependencies, in performing its functions. Identified business functions and processes should then be classified in terms of criticality, which in turn should guide the FMI's prioritisation of its protective, detective, response and recovery efforts.

3.2.2 *Identification of information assets and related access*. Similarly, an FMI should identify and maintain a current inventory of its information assets and system configurations, including interconnections with other internal and external systems, in order to know at all times the assets that support its business functions and processes. An FMI should carry out a risk assessment of those assets and classify them in terms of criticality. It should identify and maintain a current log of both individual and system credentials to know the access rights to information assets and their supporting systems, and should use this information to facilitate identification and investigation of anomalous activities.

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

3.3 Interconnections

Impact from and on an FMI's ecosystem. An FMI's systems and processes are directly or indirectly interconnected with the systems and processes of the entities within its ecosystem, eg participants, linked FMIs, settlement banks, liquidity providers, service providers, critical infrastructure such as energy and telecommunications, vendors and vendor products. Consequently, the cyber resilience of those entities could have significant implications in terms of the cyber risk that the FMI faces, particularly since the significance of the risks they may pose is not necessarily proportionate to the criticality of their business relationship with the FMI. Therefore, an FMI should identify the cyber risks that it bears from and poses to entities in its ecosystem and coordinate with relevant stakeholders, as appropriate, as they design and implement resilience efforts with the objective of improving the overall resilience of the ecosystem.

[10] See PFMI 3, Key Consideration 1.

4. Protection

4.1 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 and consistent with an FMI's risk tolerance, threat landscape and systemic role in the financial system. This chapter provides guidance on how FMIs should implement appropriate and effective measures in line with leading cyber resilience and information security practices to prevent, limit or contain the impact of a potential cyber event.

4.2 Protection of processes and assets

4.2.1 *Controls.* An FMI should implement appropriate protective controls that are in line with leading-practice cyber resilience standards to minimise the likelihood and impact of a successful cyber attack on identified critical business functions, information assets and data. Protective controls should be proportionate to and consistent with the FMI's risk tolerance, its threat landscape and its systemic role in the financial system.

4.2.2 *Resilience by design*. An FMI should consider cyber resilience from the ground up during system and process design, as well as service and product development, in order to minimise the probability of a successful cyber attack. A process to instil resilience by design should ensure that all software, network configurations and hardware, for example, are subject to rigorous testing against related security standards, that attack surfaces are limited to the extent practicable, and that common information security principles are adhered to, such as ensuring that access to systems is restricted to those with a legitimate business requirement.

4.2.3 *Strong ICT controls*. FMIs should consistently maintain a strong ICT control environment, this being a fundamental and critical component of an FMI's overall cyber resilience. While ICT controls are not comprehensively addressed in this guidance, elements in several areas are emphasised given FMIs' systemic importance:

a. Implementing appropriate measures to protect information (both in transit and at rest), commensurate with the criticality and sensitivity of the information held by and transmitted through the FMI. This should include, but not be restricted to, appropriate encryption (eg end-to-end encryption) and authentication measures (eg multifactor authentication).

b. Ensuring that the FMI has a comprehensive change management process that explicitly considers cyber risks, in terms both of residual cyber risks identified prior to and during change and of any new cyber risk created post-change.

c. Ensuring that a process exists to identify patches to technology and software assets, evaluate the patch criticality and risk, and test and apply the patch within an appropriate time frame.

d. Configuring ICT systems and devices with security settings that are consistent with the expected level of protection. FMIs should establish baseline system security configuration standards to facilitate consistent application of security settings to operating systems, databases, network devices and enterprise mobile devices within the ICT environment. Regular enforcement checks should also be performed to ensure that non-compliance with such standards is promptly rectified.

4.2.4 *Layered protection that facilitates response and recovery*. An FMI's protective controls should enable the monitoring and detection of anomalous activity across multiple layers of the FMI's infrastructure, which requires a baseline profile of system activity. Controls should be implemented in a

way that will assist in monitoring for, detecting, containing and analysing anomalous activities should protective measures fail. For example, (re-)designing processes to introduce more segmentation, intermediate checkpoints and intermediate reconciliations may allow quicker detection, identification and repair/recovery from a disruption. Similarly, segmenting networks in a manner that segregates systems and data of varying criticality may have multiple benefits, both by helping the FMI to insulate systems in one segment from a security compromise in other segments, and by facilitating more efficient recovery of services. The latter benefit is achieved because, in the event of such a compromise, only the affected segments have to be restored, rather than the entire ICT infrastructure and all data sets.

4.3 Interconnections

4.3.1 *Risks from interconnections*. An FMI should implement protective measures to mitigate the risks arising from the entities within its ecosystem. The appropriate controls for each entity will depend on the risk that arises from the connected entity and the nature of the relationship with the entity. In view of its systemic importance and unique position in the financial system, an FMI should implement measures to mitigate effectively the risk arising from its connected entities, including the following:

a. An FMI's participation requirements should be designed to ensure that they adequately support its cyber resilience framework.

b. The FMI's framework to manage its relationship with service providers should address and be designed to mitigate cyber risks. At a minimum, an FMI should ensure that its service providers meet the same high level of cyber resilience they would need to meet if their services were provided by the FMI itself. Cyber considerations should be integral part of the FMI's arrangements for managing vendors and vendor products in the areas of contracts, performance, relationships and risk. Contractual agreements between the FMI and its service providers should ensure that the FMI and relevant authorities are provided with or have full access to the information necessary to assess the cyber risk arising from the service provider.

4.4 Insider threats

4.4.1 *Security analytics*. An FMI should, within the relevant legal framework, implement measures to capture and analyse anomalous behaviour by persons with access to its systems. Data loss identification and prevention techniques should be employed to protect against the removal of confidential data from the FMI's network.

4.4.2 *Changes in employment status*. An FMI should conduct screening/background checks on new employees to mitigate insider threats. Similar checks should be conducted on all staff at regular intervals throughout their employment, commensurate with staff's access to critical systems. FMIs also should establish processes and controls to mitigate risks related to employees terminating employment or changing responsibilities.

4.4.3 *Access control*. Physical and logical access to systems should be permitted only for individuals who are authorised, and authorisation should be limited to individuals who are appropriately trained and monitored. FMIs should ensure that such access to systems is restricted only to those with a legitimate business requirement. In particular, FMIs should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication, and monitoring for anomalies should be implemented.

4.5 Training

4.5.1 *FMI staff*. An FMI should ensure that all relevant staff, be they permanent or temporary, receive training to ensure appropriate awareness of and competencies for detecting and addressing cyber-related risks. They should also be trained on how to report any unusual activity and incidents.

4.5.2 *High-risk groups*. High-risk groups, such as those with privileged system access or in sensitive business functions, should be identified and should receive targeted information security training.

5. Detection

5.1 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.

5.2 Detecting an attack

5.2.1 *Continuous monitoring*. An FMI should establish capabilities to continuously monitor (in real time or near real time) and detect anomalous activities and events. One tool to accomplish this is commonly referred to as a Security Operations Centre. These capabilities should be adaptively maintained and tested.

5.2.2 *Comprehensive scope of monitoring*. An FMI should monitor relevant internal and external factors, including business line and administrative functions and transactions. The FMI should seek to detect both publicly known vulnerabilities and vulnerabilities that are not yet publicly known, such as so-called zero-day exploits, through a combination of signature monitoring for known vulnerabilities and behaviourally based detection mechanisms. Detection capabilities should also address misuse of access by service providers or other trusted agents, potential insider threats and other advanced threat activity. These processes should be informed by and integrated with a strong cyber threat intelligence programme (see paragraphs 8.2.1 and 8.2.2 below).

5.2.3 *Layered detection*. The ability to detect an intrusion early is critical for swift containment and recovery. FMIs should take a defence-in-depth approach by instituting multi-layered detection controls covering people, processes and technology, with each layer serving as a safety net for preceding layers. In addition, an effective intrusion detection capability could assist FMIs in identifying deficiencies in their protective measures for early remediation.

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

5.2.5 *Security analytics*. An FMI should implement, within relevant legal boundaries, measures to capture and analyse anomalous behaviour by persons with access to the corporate network.

6. Response and recovery

6.1 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 systems rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them. Continuity planning is essential in meeting related objectives. This chapter provides guidance on an FMI's capabilities to respond to and recover from cyber attacks.

6.2 Incident response, resumption and recovery

6.2.1 *Incident response planning*. Upon detection of a successful cyber attack or an attack attempt, FMIs should perform a thorough investigation to determine its nature and extent as well as the damage inflicted. While the investigation is ongoing, FMIs should also take immediate actions to contain the situation to prevent further damage and commence recovery efforts to restore operations based on their response planning.

6.2.2 *Resumption within two hours*. An FMI should be able to resume critical operations rapidly. An FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios.[11]

6.2.3 *Contingency planning*. While FMIs should plan to safely resume critical operations within two hours of a disruption, they should also plan for scenarios in which this objective is not achieved. FMIs should analyse critical functions, transactions and interdependencies to prioritise resumption and recovery actions, which may, depending on the design of the FMI, facilitate the processing of critical transactions, for example, while remediation efforts continue. FMIs should also plan for situations where critical people, processes or systems may be unavailable for significant periods – for example, by potentially reverting, where feasible and practicable, to manual processing if automated systems are unavailable.

6.2.4 *Planning and preparation*. FMIs should develop and test response, resumption and recovery plans. These plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of its assets, and to meet its settlement obligations. Plans should be actively updated based on current cyber threat intelligence, information-sharing and lessons learned from previous events, as well as analysis of operationally and technically plausible scenarios that have not yet occurred. The FMI should consult and coordinate with relevant internal and external stakeholders during the establishment of its response, resumption and recovery plans.

6.3 Design elements

6.3.1 *Design and business integration*. System and process design and controls for critical functions and operations should support incident response activities to the extent possible. FMIs should design systems and processes to limit the impact of any cyber incident, resume operations within two hours of a disruption, complete settlement by day-end and preserve transaction integrity. The possibility to resume operations in a system that is technically different from the primary system may be one of the options taken into account. An FMI's incident response, resumption and recovery processes should be closely

[11] See PFMI 17, Key Consideration 6.

integrated with crisis management, business continuity and disaster recovery planning and recovery operations, and coordinated with relevant internal and external stakeholders.

6.3.2 *Data integrity*. Because contingency plans for all FMIs should ensure that the status of all transactions and member positions at the time of a disruption can be identified with certainty in a timely manner, FMIs should design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, FMIs' systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including, to the extent possible, application source code), to be used in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls. In addition, the FMI's cyber resilience framework should include data recovery measures, such as keeping a copy of all received and processed data (including the original intent of instructions being sent to the FMI for processing), maintaining transaction replay capability and conducting frequent periodic independent reconciliation of participants' positions.

6.4 Interconnections

6.4.1 *Data-sharing agreements*. In the event of a successful cyber attack that compromises the integrity of an FMI's data, a successful recovery may require clean data to be obtained from third parties and/or participants. FMIs should consider setting up data-sharing agreements with relevant third parties or participants in advance in order to enable such clean data to be received in a timely manner once a successful cyber attack has been identified.

6.4.2 *Contagion*. Because an FMI's systems and processes are often interconnected with the systems and processes of other entities within its ecosystem, in the event of a large-scale cyber incident it is possible for an FMI to pose contagion risk (ie propagation of malware or corrupted data) to, or be exposed to contagion risk from, its ecosystem. An FMI should work together with its interconnected entities to ensure they can resume operations (the first priority being its 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.

6.4.3 *Crisis communication*. FMIs should plan in advance for communications with participants, interdependent FMIs, authorities and others (such as service providers and, where relevant, the media). Communication plans should be developed through an adaptive process informed by scenario-based planning and analysis as well as prior experience. Because rapid escalation of cyber incidents may be necessary, FMIs should determine decision-making responsibilities for incident response in advance, and implement clearly defined escalation and decision-making procedures. FMIs should inform relevant oversight and regulatory authorities promptly of potentially material or systemic events.

6.4.4 *Responsible disclosure policy*. FMIs should have a policy and procedure to enable the responsible disclosure of potential vulnerabilities following a risk-based approach. In particular, FMIs should prioritise disclosures that could facilitate early response and risk mitigation by stakeholders for the benefit of the ecosystem and broader financial stability, following the possible approaches outlined in paragraph 8.3.2 below.

6.4.5 *Forensic readiness.* FMIs should have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process. In this regard, FMIs should establish relevant system logging policies that include the types of logs to be maintained and their retention periods. While forensic analysis may need to be postponed, eg in the event of contagion giving rise to financial stability concerns, and ICT resources may be focused on recovering critical systems, FMIs should ensure that investigations can still be performed post-event to the extent possible, eg through preservation of necessary system logs and evidence.

7. Testing

7.1 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 employed 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 and assets and to the stakeholders in the FMI's 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.

7.2 Comprehensive testing programme

7.2.1 *Testing programme*. An FMI should establish a comprehensive testing programme to validate the effectiveness of all elements of its cyber resilience framework. It should employ appropriate cyber threat intelligence to inform its testing methods – for example, by designing tests to simulate advanced threat agent capabilities and extreme but plausible scenarios (see paragraph 3.3 above). The results of the testing programme should be used by the FMI to support the ongoing improvement of its cyber resilience. Where applicable, these tests should include other stakeholders and functions within the organisation, such as business line management including business continuity, incident and crisis response teams, and the relevant external stakeholders in the ecosystem. An FMI should have proper procedures in place to ensure that its board and senior management are involved appropriately (eg as part of crisis management teams) and informed of test results.

7.2.2 *Methodologies and practices*. FMIs should employ a variety of effective testing methodologies and practices, including the following elements (which partly overlap and can be combined):

a. *Vulnerability assessment (VA).* FMIs should regularly perform vulnerability assessments to identify and assess security vulnerabilities in their systems and processes. FMIs should establish a process to prioritise and remedy issues identified in VAs and perform subsequent validation to assess whether gaps have been fully addressed.

b. *Scenario-based testing.* An FMI's response, resumption and recovery plans should be subject to periodic review and testing. Tests should address an appropriately broad scope of scenarios, including simulation of extreme but plausible cyber attacks, and should be designed to challenge the assumptions of response, resumption and recovery practices, including governance arrangements and communication plans. FMIs should use cyber threat intelligence and cyber threat modelling to the extent possible to imitate the unique characteristics of cyber threats. They should also conduct exercises to test the ability of their staff and processes to respond to unfamiliar scenarios, with a view to achieving stronger operational resilience.

c. *Penetration tests.* FMIs should carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. To provide an in-depth evaluation of the security of FMIs' systems, those tests should simulate actual attacks on the systems. Penetration tests on internet-facing systems should be conducted regularly and whenever systems are updated or

deployed. Where applicable, the tests could include wider business stakeholders, such as those involved in business continuity, incident and crisis response teams, as well as third parties, such as service providers and participants.

d. *Red team tests*. FMIs should challenge their own organisations and ecosystems through the use of so-called red teams to introduce an adversary perspective in a controlled setting. Red teams serve to test for possible vulnerabilities and the effectiveness of an FMI's mitigating controls. A red team may consist of an FMI's own employees and/or outside experts, who are in either case independent of the function being tested.

7.3 Coordination

7.3.1 *Coordination*. An FMI should, to the extent practicable/possible, promote, design, organise and manage exercises designed to test its response, resumption and recovery plans and processes. Such exercises should include FMI participants, critical service providers and linked FMIs. Where appropriate, FMIs should participate in exercises organised by relevant authorities and in industry-wide tests. Achieving market-wide timely recovery of operations calls for an added dimension to testing exercises. Traditional isolated testing implicitly assumes that all other players operate as usual. Removing that hypothesis helps an FMI to identify plausible complexities, dependencies and weaknesses that may have been overlooked in its recovery plans. Accordingly, testing should include scenarios that cover breaches affecting multiple portions of the FMI's ecosystem.

8. Situational awareness

8.1 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.

8.2 Cyber threat intelligence

8.2.1 *Identification of potential cyber threats*. An FMI should identify cyber threats that could materially affect its ability to perform or to provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects on its ecosystem. The FMI should regularly review and update this analysis. Cyber threats to be considered should include those which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. FMIs should consider threats to the confidentiality, integrity and availability of the FMI's business processes and to its reputation. Threats arising from internal and external sources, such as employees or third-party service providers respectively, should also be considered.

8.2.2 *Threat intelligence process*. An FMI should establish a process to gather and analyse relevant cyber threat information. Its analysis should be in conjunction with other sources of internal and external business and system information so as to provide business-specific context, turning the information into usable cyber threat intelligence that provides timely insights and informs enhanced decision-making by enabling the FMI to anticipate a cyber attacker's capabilities, intentions and modus operandi.

8.2.3 *Scope of cyber threat intelligence gathering*. The scope of cyber threat intelligence gathering should include the capability to gather and interpret information about relevant cyber threats posed by 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.[12] In this context, relevant cyber threat intelligence could include information on geopolitical developments that may trigger cyber attacks on any entity within the FMI ecosystem.

8.2.4 *Effective use of information*. FMIs should ensure that cyber threat intelligence is made available to appropriate staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels within the FMI. Cyber threat intelligence should be used to ensure that the implementation of any cyber resilience measures is threat-informed. When properly contextualised, cyber threat information enables an FMI to validate and inform the prioritisation of resources, risk mitigation strategies and training programmes.

[12] See PFMI 17, Key Consideration 7: "An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations."

8.3 Information-sharing

8.3.1 *Planning ahead*. To facilitate sector-wide response to large-scale incidents, FMIs should plan for information-sharing through trusted channels in the event of an incident, collecting and exchanging timely information that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber attack. FMIs should, as part of their response programmes, determine beforehand which types of information will be shared with whom and how information provided to the FMI will be acted upon. Reporting requirements and capabilities should be aligned with relevant national laws and regulations as well as information-sharing arrangements within the FMI's communities and the financial sector.

8.3.2 *Information-sharing groups*. FMIs should participate actively in information-sharing groups and collectives, 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. FMIs should, where appropriate, share information both bilaterally and multilaterally. An FMI should consider exchanging information on its cyber resilience framework bilaterally with the key stakeholders in its ecosystem so as to promote mutual understanding of each other's approach to securing systems that are linked or interfaced. Such information exchange would facilitate an FMI's and its stakeholders' efforts at dovetailing their respective security measures to achieve greater cyber resilience. Multilateral information-sharing arrangements should be designed to facilitate a sector-wide response to large-scale incidents.

9. Learning and evolving

9.1 Preamble

An FMI's cyber resilience framework needs to ensure 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.[13] 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.

9.2 Continuous learning

9.2.1 *Lessons from cyber events*. An FMI should systematically identify and distil key lessons from cyber events that have occurred within and outside the organisation in order to advance its resilience capabilities. Useful learning points can often be gleaned from successful cyber intrusions and near misses in terms of the methods used and vulnerabilities exploited by cyber attackers.

9.2.2 *Acquiring new knowledge and capabilities*. An FMI should actively monitor technological developments and keep abreast of new cyber risk management processes that can effectively counter existing and newly developed forms of cyber attack. An FMI should consider acquiring such technology and know-how to maintain its cyber resilience.

9.2.3 *Predictive capacity*. FMIs' cyber risk management practices should go beyond reactive controls and include proactive protection against future cyber events. Predictive capabilities and anticipation of future cyber events are based on analysing activity that deviates from the baseline. FMIs should work towards achieving predictive capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity.

9.3 Cyber resilience benchmarking

9.3.1 *Metrics*. Metrics and maturity models allow an FMI to assess its cyber resilience maturity against a set of predefined criteria, typically its operational reliability objectives. This benchmarking requires an FMI to analyse and correlate findings from audits, management reviews, incidents, near misses, tests and exercises as well as external and internal intelligence gathered. The use of metrics can help an FMI to identify gaps in its cyber resilience framework for remediation, and allow an FMI to systematically evolve and achieve more mature states of cyber resilience.

[13] See PFMI 17, Key Consideration 7: "An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations."

Glossary[14]

actionable intelligence	The necessary information immediately available to address, prevent or mitigate a cyber threat.
attack surface	The sum of an information system's characteristics in the broad categories (software, hardware, network, processes and human) which allows an attacker to probe, enter, attack or maintain a presence in the system and potentially cause damage to the FMI. A smaller attack surface means that the FMI is less exploitable and an attack less likely.[15] However, reducing attack surfaces does not necessarily reduce the damage an attack can inflict.[16]
availability	The property of being accessible and usable as expected upon demand.[17]
business process	A collection of linked activities that takes one or more kinds of input and creates an output that is of value to the 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.
cyber	Refers to the interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.[18]
cyber anomaly	Behaviour on digital systems that deviates from typical values, rules or processes.
cyber attack	An attempt to infiltrate that might result in a circumstance or event having an actual adverse effect on cyber resilience.
cyber event	An observable occurrence in an information system or network.[19]
cyber governance	A process involving the establishment of cyber resilience objectives, policies and standards; the implementation of controls; the exercise of oversight through audits and assessments; and the raising of cyber awareness within the organisation.
cyber 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.[20]

[14] For general definitions of terms not found in this glossary, please see CPSS, *A glossary of terms used in payments and settlement systems*, March 2003; and European Central Bank and Eurosystem, *Glossary of terms related to payment, clearing, and settlement systems*, December 2009.

[15] NICCS, *Glossary of common cybersecurity terminology*, http://niccs.us-cert.gov/glossary.

[16] CPMI, *Cyber resilience in financial market infrastructures*, November 2014.

[17] NICCS, *Glossary of common cybersecurity terminology*, http://niccs.us-cert.gov/glossary.

[18] NICCS, *Glossary of common cybersecurity terminology*, http://niccs.us-cert.gov/glossary.

[19] NICCS, *Glossary of common cybersecurity terminology*, http://niccs.us-cert.gov/glossary.

[20] Adapted from APMG International Definition, http://www.apmg-international.com/en/consulting/what-maturity-model.aspx.

cyber resilience	An FMI's ability to anticipate, absorb, adapt to, rapidly respond to and recover from disruption caused by a cyber attack.
cyber resilience framework	Consists of the policies, procedures and controls the FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces.
cyber resilience strategy	The high-level and long-term plan an FMI establishes to ensure that it is able to perform its major business functions and safeguard data confidentiality during a cyber attack.
cyber risk	The combination of the probability of an event occurring within the realm of an organisation's or person's information assets, computer and communication resources and the consequences of that event for an organisation or person.
cyber risk management	The process used by an FMI to establish an enterprise-wide framework to manage the likelihood of a cyber attack and develop strategies to mitigate, respond to, learn from and coordinate its response to the impact of a cyber attack. The management of an FMI's cyber risk should support the business processes and be integrated in the FMI's overall risk management framework.
cyber risk profile	The cyber risk actually assumed, measured at a given point in time.
cyber risk tolerance	The propensity to incur cyber risk, being the level of cyber risk that an FMI intends to assume in pursuing its strategic objectives.
cyber security	In this report, refers to strategies, policies and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities and policies regarding the security of an FMI's operations.
cyber threat	A circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in an FMI's systems, resulting in a loss of confidentiality, integrity or availability.
cyber threat intelligence	Information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event (may also be referred to as "cyber threat information").[21]
defence in depth	The defensive security controls deployed throughout the various layers of the network so as to provide redundancy in the event of the failure of another control or the exploitation of a vulnerability (may also be referred to as "layered protection").
detect	To develop and implement the appropriate activities in order to identify the occurrence of a cyber event.[22]
disruption	A disruption is an event affecting an organisation's ability to deliver the services it intends to provide for its customers.

21 Bank of England – CBEST, *Qualities of a threat intelligence provider*.

22 NIST, *Framework for improving critical infrastructure cybersecurity*, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

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, etc.
forensic investigation	The application of investigative and analytical techniques to gather and preserve evidence from a digital device impacted by a cyber attack.
forensic readiness	The ability of an FMI to maximise the use of digital evidence to identify the nature of a cyber attack.
golden copy	The recorded point from which affected ICT environment components, data or applications can be restored to the state they were in prior to the attacker's presence (may also be referred to as "golden point" or "golden record").
ICT	Information and communications technologies. ICT can also be read as IT (information technology) in this document.
identify	To develop the organisational understanding required to manage cyber risk to systems, assets, data and capabilities.[23]
indicator	An occurrence or sign which reveals that an incident may have occurred or be in progress.[24]
information asset	Any piece of data, device or other component of the environment that supports information-related activities. In the context of this report, information assets include data, hardware and software.[25] 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.
integrity	With reference to information, an information system or a component of a system, the property of not having been modified or destroyed in an unauthorised manner.[26]
layered protection	As any single defence against a cyber threat may be flawed, an FMI can use a series of different defences to cover the gaps in the others' protective capabilities. For example, the use of firewalls, intrusion detection systems, malware scanners, integrity auditing procedures and local storage encryption tools can each serve to protect information technology resources in ways the others cannot. (May also be referred to as "defence in depth".)
leading standards, guidelines and practices	Standards, guidelines and practices which reflect industry best approaches to managing cyber threats, and which incorporate what are generally regarded as the most effective cyber security solutions.
malware	Malicious software used to disrupt the normal operation of an information system that adversely impacts its confidentiality, availability or integrity.

[23] NIST, *Framework for improving critical infrastructure cybersecurity*, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[24] NICCS, *Glossary of common cybersecurity terminology*, http://niccs.us-cert.gov/glossary.

[25] UK National Archives, *What is an information asset?*, http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf.

[26] NICCS, *Glossary of common cybersecurity terminology*, http://niccs.us-cert.gov/glossary.

operational resilience	The ability of an FMI to: (i) maintain essential operational capabilities (resumption) under adverse conditions or stress, even if in a degraded or debilitated state; and (ii) recover to effective operational capability in a time frame consistent with the provision of critical economic services (recovery).
protect	To develop and implement appropriate safeguards, controls and measures to ensure delivery of critical infrastructure services.
recover	To restore any capabilities or services that have been impaired due to a cyber event.
red team	An independent group that challenges the cyber resilience of an organisation to test its defences and improve its effectiveness. A red team views the cyber resilience of an FMI from an adversary's perspective.
resilience by design	The embedding of security in technology and system development from the earliest stages of conceptualisation and design.
respond	Of an FMI, to develop and implement appropriate activities to be able to take action when it detects a cyber event.
resume	To recommence critical functions following a cyber incident. An FMI should resume critical services as soon as it is safe and practicable to do so without causing unnecessary risk to the wider sector or further detriment to financial stability. The plan of action should incorporate the use of a secondary site and be designed to ensure that critical ICT systems can resume operations within two hours following a disruptive event.
risk tolerance	The amount and type of risk that an organisation is willing to take in order to meet its strategic objectives (may also be referred to as "risk appetite").
security operations centre (SOC)	A location or service responsible for monitoring, detecting and isolating incidents and for managing an FMI's security products, network devices, end-user devices and systems.
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 and sufficient to mitigate the impact of a potentially harmful event.
threat	A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organisational operations, organisational assets (including information and information systems), individuals, other organisations or society.[27]
vulnerability	A weakness, susceptibility or flaw in a system that an attacker can access and exploit to reduce the system's information assurance. Vulnerability arises from the confluence of three elements: the presence of a susceptibility or flaw in a system; an attacker's access to that flaw; and an attacker's capability to exploit the flaw.

[27] NICCS, http://niccs.us-cert.gov/glossary#letter_t.