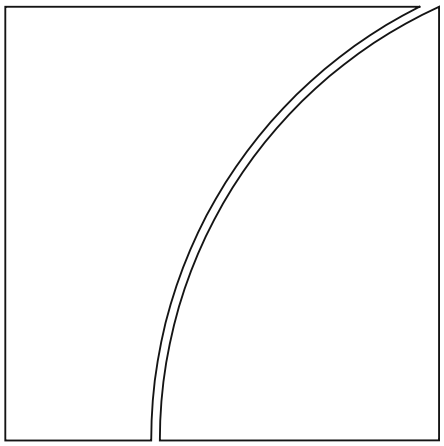
Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions



Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience

November 2022

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 978-92-9259-605-7 (online)

Contents

Abbreviations

AT	Assessment Team
BIS	Bank for International Settlements
BYOD	bring your own device
CCPs	central counterparties
CIO	chief information officer
COBIT	Control objectives for information and related technology
COO	chief operating officer
CPMI	Committee on Payments and Market Infrastructures
CRF	cyber resilience framework
CRO	chief risk officer
CRS	cyber resilience strategy
CSDs	central securities depositories
CTO	chief technology officer
FMI	financial market infrastructure
IMSG	Implementation Monitoring Standing Group
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
NIST	US National Institute of Standard and Technology
PFMI	Principles for financial market infrastructures
PS	payment system
SSS	securities settlement system
TR	trade repository
2hRTO	two-hour recovery time objective

1. Executive summary

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

Following the publication of the PFMI, the CPMI and IOSCO agreed to monitor their implementation in 28 CPMI and IOSCO member jurisdictions via a dedicated standing group, the Implementation Monitoring Standing Group (IMSG). Implementation is being monitored on three levels. Level 1 self-assessment reports on whether a jurisdiction has completed the process of adopting legislation and other policies that will enable it to implement the Principles and Responsibilities. Level 2 assessments are peer reviews of the extent to which the content of the jurisdiction's implementation measures is complete and consistent with the PFMI. Level 3 (L3) peer reviews examine consistency in the outcomes of implementation of the Principles by FMIs and implementation of the Responsibilities by authorities.

This report represents the fourth L3 assessment of consistency in the outcomes of FMIs' implementation of the PFMI.[1] It focuses on cyber resilience and was carried out during 2020–22 by the IMSG and a team of experts from CPMI and IOSCO member jurisdictions.

While Level 3 assessment reports do not include ratings, they do include key findings. In this vein, the IMSG has identified one *serious issue of concern* in the area of cyber response and recovery plans to meet the two-hour recovery time objective (2hRTO) and four *issues of concern* in the area of cyber resilience planning and testing. The IMSG has also noted some *observations*.

1.1 Scope of the assessment

This assessment was based on Principles 2, 3 and 17 (and relevant Key Considerations) of the PFMI. It is informed by the *Guidance on cyber resilience for financial market infrastructures* ("Cyber Guidance") and covers three important components of the cyber resilience framework: (i) governance; (ii) testing; and (iii) learning and evolving.

The overarching objective of this assessment was to review the current state of cyber resilience of FMIs as informed by the Cyber Guidance. It aimed to understand how and to what degree the Cyber Guidance has been used by FMIs. The assessment found that there was a reasonably high adoption of the Cyber Guidance, with a significant majority of FMIs indicating that they had adopted or referred to parts of the Cyber Guidance when designing their cyber resilience frameworks.

A total of 37 FMIs from 29 jurisdictions participated in the assessment, consisting of systemically important PSs, CSDs/SSSs, CCPs and TRs.

[1] The previous Level 3 reports are: CPMI-IOSCO, *Implementation monitoring of PFMI: Level 3 assessment – report on the financial risk management and recovery practices of 10 derivatives CCPs*, August 2016; CPMI-IOSCO, *Implementation monitoring of PFMI: follow-up Level 3 assessment of CCPs' recovery planning, coverage of financial resources and liquidity stress testing*, May 2018; and CPMI-IOSCO, *Implementation monitoring of the PFMI: Level 3 assessment of FMIs' business continuity planning,* July 2021. These reports are available on the CPMI and IOSCO websites.

The FMIs participated on a voluntary basis and responded to a self-assessment questionnaire, and responses were received between February and early April 2021. This was complemented by several rounds of follow-up questions as well as a workshop held on 28 June 2021, in which pertinent issues were discussed with the FMIs and additional inputs received. The CPMI-IOSCO IMSG and its Assessment Team (AT) would like to thank the participating FMIs – and their supervisors and overseers – for their cooperation during this exercise.

Importantly, as L3 assessments are peer benchmarking exercises and not supervisory exercises, the assessment focuses on the consistency in outcomes of implementation of the relevant Principles and Key Considerations (KCs) across the group of FMIs as a whole, rather than on each individual FMI's specific implementation outcomes. As noted in Responsibility D of the PFMI, it is the responsibility of the relevant supervisory authorities to ensure that the Principles are applied by individual FMIs. Furthermore, the findings in this report are based on the IMSG's review of the 37 FMIs alone and may not necessarily be representative of all FMIs. It is further acknowledged that the use of a survey also has the limitation that FMIs may interpret the questions in different ways.

1.2 Key findings of the assessment

Despite a reasonably high adoption of the Cyber Guidance, the IMSG identified one serious issue of concern and four issues of concern which could be subject to further analysis. All FMIs (including those not part of the sample), as well as their supervisors, regulators and overseers, should consider whether any issues of concern identified in this report are relevant to them. In keeping with their respective regulation, supervision and oversight responsibilities, authorities are expected to ensure that the PFMI are applied consistently in their respective jurisdictions and implemented by individual FMIs, as noted in Responsibility D of the PFMI.[2] However, the key findings of the exercise are summarised below.

Serious issue of concern[3]

1. A small number of FMIs had not yet developed their cyber response and recovery plans to meet the two-hour recovery time objective (2hRTO) in line with Principle 17 KC 6. Within this small number, there were FMIs that did not have plans to address scenarios, which resulted in an inability to meet their recovery time objectives. This finding casts doubt over the level of cyber resilience and preparedness of these FMIs, and is flagged as a serious issue of concern that should be addressed with the highest priority.

Issues of concern

1. In addition to the small number of FMIs for which the serious issue of concern is relevant, another small number of FMIs which had established their cyber response and recovery plans to meet the 2hRTO recognised that their plans were not able to meet the 2hRTO under extreme cyber attack scenarios. This is a gap or shortcoming in FMIs' implementation outcomes relevant to Principle 17 KC 6, which should be addressed.
2. A number of FMIs are not conducting cyber resilience testing after a significant change in their systems. For example, a significant majority of FMIs indicated that they do not test the integrity of backup data, some do not perform vulnerability assessments and most do not perform

[2] As the IMSG only had access to anonymised survey results, the CPMI and IOSCO are unable to raise the concerns identified in this assessment with specific relevant authorities.

[3] The findings of the assessment are described as *(serious) issues of concern* if they relate to an identified gap or shortcoming in the FMIs' implementation outcomes against the standards in the Principles and KCs in the PFMI. While all "issues of concern" should be addressed, a "serious issue of concern" is an identified gap or shortcoming that should be addressed with the highest priority. This is consistent with the categorisation and approach taken in previous Level 3 assessments and with the premise of paragraph 1.36 of the PFMI and paragraph 1.1.1 of the Cyber Guidance, which state that the standards are contained in the Principles and KCs.

penetration testing after a significant change has occurred. This is a gap or shortcoming in FMIs' implementation outcomes relevant to Principle 17 KC 2, which should be addressed.

3. Multiple FMIs may not be conducting comprehensive scenario-based testing, which calls into question whether these FMIs have adequately validated their ability to recover and resume operations following a cyber disruption. For example, some FMIs indicated that they are not testing governance arrangements in scenario-based testing exercises. This is a gap or shortcoming in FMIs' implementation outcomes relative to Principle 17 KC 6, which should be addressed.

4. Some FMIs did not include FMI participants, and most did not include critical service providers and linked FMIs in the testing of their response, resumption and recovery plans and processes with respect to cyber incidents. This calls into question FMIs' ability to meet Principle 17 KC 7 with regard to identifying, monitoring and managing risks from external parties. This may also affect whether an FMI is able to demonstrate its ability to recover and resume operations following a cyber incident as foreseen in Principle 17 KC 6. These are issues of concern that should be addressed.

Regarding the above-mentioned (serious) issues of concern, it should be noted that the AT only had access to anonymised survey results, and therefore the CPMI and IOSCO are unable to raise the findings identified in this assessment with specific relevant authorities. However, considering the impact of these (serious) issues of concern in aggregate, they collectively seem to highlight clear challenges for FMIs' cyber resilience that should be addressed with the highest priority.

It should also be noted that L3 assessments are peer benchmarking exercises and not supervisory exercises. Accordingly, the focus of the report is on the consistency of outcomes of implementation of the relevant Principles and KCs across the group of FMIs as a whole, rather than on specific implementation outcomes for each individual FMI.

As noted in Responsibility D of the PFMI, it falls within the responsibility of the relevant supervisory authorities to ensure that the Principles are implemented by individual FMIs. Furthermore, the findings in this report are based on the IMSG's review of the 37 FMIs' responses to the survey questionnaire and may not necessarily be representative of all FMIs.

The use of a survey also has the limitation that FMIs may have interpreted the questions in different ways. For example, a large number of FMIs did not identify any extreme cyber attack scenarios under which they could not meet the 2hRTO, but this may have been because they considered less extreme scenarios than those FMIs that indicated they could not meet the 2hRTO for some scenarios.

Observations[4]

1. Some FMIs did not clearly define acceptable risk levels using quantitative metrics. This may call into question whether concrete and tangible metrics are being used by FMIs to clearly articulate their risk tolerances.

2. There are a wide range of practices around the party or parties responsible for approving the acceptable level of cyber risk for FMIs. Some FMIs indicated that their board was ultimately accountable.

3. Some FMIs did not provide a description of the process or metrics through which they assess the level of cyber risk-related skills of their board members. Where such assessments are absent,

[4] The findings of the assessment are described as *observations* when they relate to the Explanatory Notes in the PFMI and/or the Cyber Guidance. The Explanatory Notes in the PFMI and the related guidance (eg Cyber Guidance) do not represent additional requirements beyond those set forth in the PFMI. Observations relate to differences in implementation outcomes across FMIs (rather than consistency with the PFMI) which could result in material differences in resilience across FMIs.

there may be a lack of visibility and assurance over whether board members have the knowledge and capacity to comprehend the potential impact of cyber events and their risks to the organisation and its ecosystem to provide effective oversight.

4. Multiple FMIs may not be retesting and/or validating the remediation of vulnerabilities identified through testing.

5. A small number of FMIs indicated that red team testing is currently not part of their cyber testing strategy; however, the majority of these FMIs have plans to incorporate it in the near future.

6. Some FMIs included only phishing (and not social engineering and physical penetration) as part of their penetration testing programmes. In addition, a small number of FMIs did not incorporate threat intelligence as part of penetration testing.

7. Some of the FMIs' industries and a small number of the FMIs' relevant authorities had not conducted industry-wide tests or organised market-wide exercises in the last three years.

8. While all FMIs confirmed participation in broader forums to exchange information on lessons learnt, some FMIs indicated that they were not required to share cyber information with a centralised agency, although the FMIs may still do so on a voluntary basis.

9. Among the small number of FMIs that do not use cyber tests or other lessons learnt to improve their operational resilience objectives, there are FMIs that are considering using their cyber tests to meet this goal.

2. Introduction

2.1 Objective of the L3 assessment

The IMSG monitors the implementation of the PFMI[5] by FMIs across jurisdictions. This work is structured according to a monitoring framework that involves three phases:

(i) Level 1 (L1) to assess whether jurisdictions have completed the process of adopting the legislation, regulations and other policies that will enable them to implement the PFMI.

(ii) Level 2 (L2) to assess whether the content of legislation, regulations and policies is complete and consistent with the PFMI.

(iii) Level 3 (L3) to assess whether there is consistency in PFMI implementation outcomes.

The L3 assessments are peer benchmarking exercises and not supervisory exercises. The reviews focus on the consistency in outcomes of implementation of relevant Principles and Key Considerations (KCs) across the group of participating FMIs as a whole rather than on each individual FMI's specific implementation outcomes. As a result, in contrast to other implementation monitoring assessments carried out by CPMI and IOSCO, this L3 review does not include formal ratings of observance. There are three key inputs to the assessment:

- identification of implementation measures and approaches across FMIs;
- consideration of implementation outcomes' consistency with relevant Principles and the KCs they are based upon; and
- comparison of implementation outcomes across FMIs, with attention paid, where possible, to the drivers, degree and implications of observed variations.

2.2 Scope of this review

Prior to the L3 on cyber resilience, the IMSG conducted a Level 3 assessment of business continuity planning (L3 BCP) based on Principle 17 (Operational risk) with a focus on KCs 3, 6 and 7. Although that assessment covered some cyber-related aspects, CPMI and IOSCO decided to undertake more focused implementation monitoring of FMIs' cyber resilience.

The overarching objective of this L3 assessment was to review the current state of cyber resilience of FMIs as informed by the *Guidance on cyber resilience for financial market infrastructures*[6] ("Cyber Guidance"), with the aim of understanding how and to what degree the Cyber Guidance has been used by FMIs. This L3 assessment focuses on Principles 2 (Governance), 3 (Comprehensive framework for the management of risks) and 17 (Operational risk) informed by three of the key elements in the Cyber Guidance, namely governance, learning/evolving and testing (Graph 1).

[5] Available at www.iosco.org/library/pubdocs/pdf/IOSCOPD377-PFMI.pdf and www.bis.org/cpmi/publ/d101a.pdf.

[6] Available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf and https://www.bis.org/cpmi/publ/d146.pdf

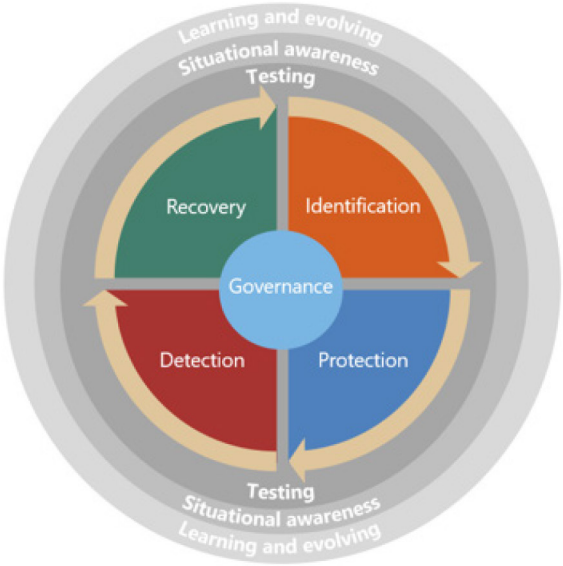
Principles for financial market infrastructures

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 (Comprehensive framework for the management of risks): An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational and other risks.

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.

Elements of the cyber resilience guidance — Graph 1



Source: CPMI-IOSCO Cyber Guidance (2016).

The approach taken for the assessment also considered the premise that the Cyber Guidance is one (but not the only) way to achieve cyber resilience.

3. Process and methodology

This L3 assessment proceeded in three main stages over the course of 19 months: (i) setting the jurisdictional and FMI coverage of the exercise; (ii) data collection and analysis by the IMSG; and (iii) review of assessment findings by the IMSG and the CPMI-IOSCO Steering Group (SG). Since FMIs' cyber resilience may involve sensitive information, the data were anonymised, with only a limited number of IOSCO staff members (previously selected by the CPMI and the IOSCO secretariats) having access to the raw data from the FMIs.

3.1. Jurisdictional/FMI coverage

A total of 37 FMIs from 29 jurisdictions participated in the L3 cyber resilience assessment. They consisted of systemically important payment systems (PSs), central securities depositories (CSDs)/securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs). Participating FMIs were selected based on a number of criteria, including:

- One (or more) FMI per jurisdiction;
- balancing jurisdictional and FMI coverage on the one hand, and complexity and volume of work on the other hand;
- a mix of both public and privately operated FMIs; and
- ensuring a sample of sufficient size to ensure that anonymisation is practical.

The FMIs participated on a voluntary basis and responded to a self-assessment questionnaire with information as of 10 February 2021. The participating FMIs were asked not to include any information that may allow for their identification in their responses to the self-assessment questionnaire. After verifying the anonymity of the responses, the AT was given access to the information.

3.2 Data collection and analysis

In this context, the Level 3 assessment on FMIs' cyber resilience was launched on 4 December 2020 with the distribution of self-assessment questionnaires to the participating FMIs. The questions were based on Principles 2, 3 and 17 of the PFMI, and some elements of the Cyber Guidance, focusing on the following components of cyber resilience framework: (i) governance; (ii) testing; and (iii) learning and evolving. The survey contained both open-ended and closed-form questions (Annex A). It had a total of 85 questions, with the majority of questions (75) covering either the Principles/KCs or the Cyber Guidance. The remaining 10 questions related to FMIs' familiarity with the Cyber Guidance and the impact of the Covid-19 pandemic on various aspects of FMIs' cyber resilience programmes. Policy, procedural or methodological documents were not requested. It should be emphasised that the evidence base for this exercise was non-exhaustive.

Since FMIs' cyber resilience may involve sensitive information, survey responses were handled with due regard to confidentiality. To preserve the anonymity of the participating FMIs, but with a view to helping the AT with the analysis of the information, a random ID number was assigned to each FMI. Only a limited number of IOSCO staff members (previously identified by the CPMI and IOSCO secretariats) had access to identifying information about the FMIs. The AT received and analysed the information on this basis. The free-form responses were screened to remove any identifying information. The FMI's jurisdiction was not identified; however, information on FMI type was retained in the data in order to allow for potential FMI-type specific findings. This approach was made clear to the FMIs prior to their completion of the survey.

The AT discussed the initial findings with the participating FMIs in a virtual workshop held on 28 June 2021, which provided additional input for the analysis of the information. The AT also received feedback and direction from the IMSG throughout the assessment process.

4. Analysis of results

This section presents the IMSG's review for each of the three elements of the Cyber Guidance that were analysed as part of this assessment exercise. As noted earlier, in considering the implementation of the PFMI by these FMIs, the IMSG has not conducted a supervisory review or examination. Accordingly, this

section focuses on the consistency in the outcomes of implementation of relevant Principles and KCs across FMIs.

Consistent with past Level 3 reports, the IMSG's findings (ie identified gaps or shortcomings) are structured as "issues of concern" or "serious issues of concern". An "issue of concern" is an identified gap or shortcoming in FMIs' implementation outcomes relative to standards pertaining to the relevant KC which must be addressed. While all "issues of concern" should be addressed, a "serious issue of concern" is an identified gap or shortcoming that must be addressed with the highest priority.

In addition to (serious) issues of concern, the report also identifies "observations" and "other observations" that relate to differences in implementation outcomes across FMIs (rather than consistency with the PFMI). They are considered "observations" when different implementations could result in material differences in resilience across FMIs. When differences in implementation are not expected to result in material differences in resilience, they are classified as "other observations".[7] In some cases, variations exist because individual FMIs have chosen to exceed relevant minimum standards in the PFMI or have done so in accordance with specific implementations of the PFMI in their home jurisdiction.

This distinction in the characterisation of the findings is consistent with the approach taken in previous Level 3 assessments and is also consistent with the premise of paragraph 1.36 of the PFMI and paragraph 1.1.1 of the Cyber Guidance. These paragraphs indicate that the standards are contained in the Principles and Key Considerations, while the Explanatory Notes in the PFMI and the related guidance (eg Cyber Guidance) do not represent additional requirements beyond those set out in the PFMI.

4.1 General topics

4.1.1 Adopting Cyber Guidance and other relevant cyber resilience frameworks and standards

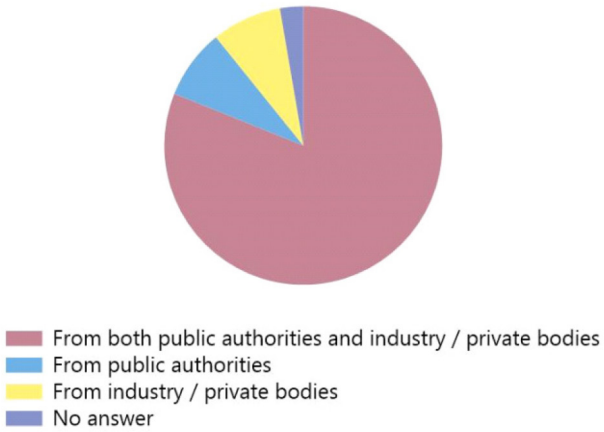
Adoption of the Cyber Guidance was reasonably high, with a significant majority of the FMIs indicating that they had adopted or referred to parts of the Cyber Guidance when designing their cyber resilience frameworks. In addition, almost all FMIs used or referenced some form of guidance from public authorities and/or industry standards when designing their cyber resilience framework (CRF) (Graph 2, left-hand panel). The most common industry standards adopted or referenced by FMIs were from the International Organisation for Standardisation (eg ISO 27001 or ISO 22301), followed by the US National Institute of Standard & Technology (NIST) standards (Graph 2, right-hand panel).

[7] Indeed, the principles-based approach in the PFMI (and the Cyber Guidance) explicitly acknowledges that a variety of implementation approaches can lead to equivalent resilience.

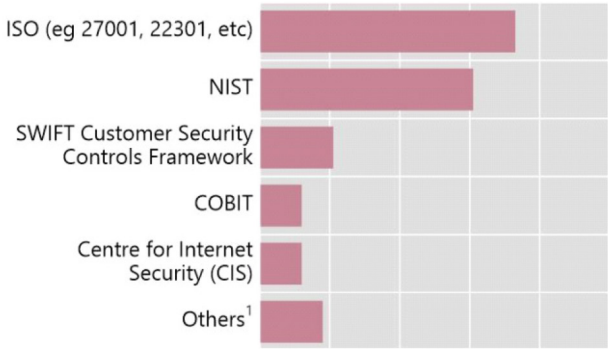
Adoption of Cyber Guidance and other relevant cyber resilience frameworks and standards

Graph 2

Adoption of other cyber guidance and standards



Common industry standards adopted by FMIs



[1] Others: MITRE; Payment Card Industry (PCI); Open Web Application Security Project (OWASP); Forum of Incident Response and Security Teams (FIRST).

Source: CPMI-IOSCO survey on the cyber resilience of FMIs, 2021.

4.1.2 Developing concrete cyber response and recovery plans to meet the 2hRTO for the safe and timely resumption of critical operations

Serious issue of concern

- There were a small number of FMIs that had not yet developed their cyber response and recovery plans to meet the two-hour recovery time objective (2hRTO) in line with Principle 17 KC 6. Within this small number, there were FMIs that did not have plans to address scenarios which resulted in an inability to meet their recovery time objectives. This casts doubt over the level of cyber resilience and preparedness of these FMIs, and this finding is flagged as a serious issue of concern that should be addressed with the highest priority.

Issue of concern:

- In addition to the small number of FMIs noted under the serious issue of concern, another small number of FMIs which have established their cyber response and recovery plans to meet the 2hRTO recognised that their plans were not able to meet the 2hRTO under extreme cyber attack scenarios. This is a gap or shortcoming in FMIs' implementation outcomes relevant to Principle 17 KC 6, which should be addressed.

A significant majority of FMIs indicated that they have the necessary plans in place that are incorporated within their business continuity plans, disaster recovery plans, incident response plans and/or crisis management plans to meet 2hRTO for cyber-attack scenarios. However, within this significant majority, a few of these FMIs had highlighted that the 2hRTO could only be achieved for certain cyber scenarios under their planning assumptions, and not more extreme scenarios (eg, cyber-attack compromised the integrity of the data). This would deviate from the expectations outlined in Principle 17 Key Consideration 6 of the PFMI and paragraphs 6.2.2 and 6.3.1 of the Cyber Guidance, which set the expectation for FMIs to meet 2hRTO even in the case of extreme but plausible scenarios.

PFMI – Principle 17 KC 6

An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a widescale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements.

Cyber Guidance

6.2.2 Resumption within two hours (ie two-hour RTO). Objectives for resuming operations set goals for, ultimately, the sound functioning of the financial system, which should be planned for and tested against. In line with Key Consideration 17.6 of the PFMI, 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. Notwithstanding this capability to resume critical operations within two hours, FMIs should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, while taking into account that completion of settlement by the end of day is crucial.

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 critical operations within two hours of a disruption, complete settlement by day-end and preserve transaction integrity. The possibility to resume critical operations in a system that is technically different from the primary system or in a system that performs those operations and completes settlement in a non-standardised way may be among the options for an FMI to consider. An FMI's incident response, resumption and recovery processes should be closely integrated with crisis management, business continuity and disaster recovery

For the few FMIs that did not have the necessary cyber response and recovery plans to achieve the 2hRTO, all of them were in the midst of developing their plans to meet the objective. Within this few FMIs, there were FMIs which also highlighted that they did not have any contingency plans to address cyber scenarios that lead to them not meeting their intended recovery time objectives. These FMIs were deemed to have failed to meet Principle 17 KC 6 of the PFMI and paragraph 6.2.3 of the Cyber Guidance, and this puts their cyber preparedness and operational resilience into question.

Cyber Guidance

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, safe and practicable, to manual processing if automated systems are unavailable.

During the industry workshop on 28 June 2021, the AT sought to understand some examples of extreme scenarios in respect of which FMIs found it challenging to meet the 2hRTO. One such scenario provided by the workshop participants was a cyber attack that compromises data integrity (eg from a ransomware attack), and, as a result, impedes the safe resumption of services. Under such circumstances, trade-offs would have to be made between restoring data integrity in the infected system and ensuring the timeliness of the resumption. These "extreme" scenarios are becoming increasingly plausible in the rapidly evolving cyber threat landscape that FMIs are facing today, and it is therefore important for FMIs to continue reviewing their recovery strategies and developing capabilities to maintain their operational

resilience. It is also important that FMIs incorporate sufficiently extreme scenarios into their cyber response and recovery planning. One limitation of the survey is that it was unable to identify which scenarios each FMI used in its recovery planning. Hence, it is possible that some FMIs indicated their readiness to recover within two hours in all extreme but plausible cyber attack scenarios because they did not consider scenarios as extreme as those considered by FMIs that identified gaps in their ability to meet the 2hRTO.

4.1.3 Impact of the Covid-19 pandemic on cyber resilience

The FMIs generally recognised the heightened cyber risks due to increased remote working arrangements and the use of personal devices belonging to staff for work (ie bring your own device, or "BYOD") during the Covid-19 pandemic. While almost all FMIs indicated that their cyber resilience abilities and controls were not affected by the pandemic, a few FMIs who felt that they had experienced some impact highlighted the following issues:

- increased dependency on remote access infrastructure magnified operational impact if the infrastructure comes under attack;
- BYOD risk rises as more employees use their own devices for work if these personal devices are not subject to the same level of security measures as corporate devices;
- staff were subjected to more phishing and social engineering attacks during the pandemic; and
- operational recovery in certain scenarios may take longer due to staff working offsite.

Most FMIs indicated that they had either adjusted or were considering adjustments to their cyber resilience postures, such as implementing additional measures (eg additional remote access controls, stepping up security awareness campaigns, monitoring for Covid-19 email threats and web surfing etc) to address the cyber risks. Some FMIs felt that their operations and cyber resilience posture had not fundamentally changed because (i) working remotely was already part of their normal business operations before the pandemic; (ii) they were able to leverage existing technology and processes to maintain business as usual; and/or (iii) the plans and procedures established for operating in a pandemic scenario had been developed and robustly tested prior to Covid-19.

Some FMIs had to make changes to controls and measures, including those related to third-party providers, due to the Covid-19 pandemic. Among the FMIs that changed policies due to the pandemic, most of them had changed their priority of deliverables within the strategy or replanned how the strategy was implemented. Among those FMIs that did make a trade-off between security and continuity, many cited the security risk of remote working. Many of these FMIs had also instituted compensating controls to mitigate the risks.

FMIs appeared to be split over whether they observed an increase in cyber attacks during the Covid-19 pandemic. The ones that witnessed an increase in cyber attacks noted an increase in phishing, ransomware and distributed denial of service attacks. Furthermore, some FMIs that did not witness an increase in cyber attacks were aware of other entities that did face increased cyber attacks.

A significant majority of FMIs indicated that they had incorporated or were considering whether to incorporate lessons learnt with respect to structures for coordination and information-sharing. They felt the need for close cooperation, and they participated more frequently in information-sharing events during the pandemic. Some of these FMIs also highlighted that the Covid-19 pandemic had provided a practical exercise of FMIs' crisis response protocols and collaborations with other stakeholders in the industry.

4.2 Governance

Observations

- Some FMIs did not clearly define acceptable risk levels using quantitative metrics. This may call into question whether concrete and tangible metrics are being used by FMIs to clearly articulate their risk tolerances.
- There are a wide range of practices around the party or parties responsible for approving the acceptable level of cyber risk for FMIs. Some FMIs indicated that their board was ultimately accountable.
- Some FMIs did not provide a description of the process or metrics through which they assess the level of cyber risk-related skills of their board members. Where such assessments are absent, there may be a lack of visibility and assurance over whether board members possess knowledge and capacity sufficient to comprehend the potential impact of cyber events, and their risks to the organisation and to its ecosystem to provide effective oversight.

4.2.1 Cyber resilience objectives, governance arrangements and risk appetite

All FMIs indicated that their cyber resilience programmes included statements on cyber resilience objectives. Cyber risk management is part of the enterprise risk management process for almost all FMIs (only a few FMIs indicated that it is not part of the enterprise risk management process, but the general principles are aligned). All FMIs indicated that they periodically assess their performance in meeting cyber resilience objectives through identified metrics (a significant majority of FMIs), monitoring activities (a significant majority of FMIs) and/or using two or more options to assess their performance (a significant majority of FMIs).

FMIs responses indicated that they define "acceptable risk levels" in various ways. Some FMIs tie acceptable risk level (or risk appetite) to quantitative metrics on impact and probability. While a few FMIs use parameters such as percentage of financial loss and availability/RTO. The rest use either a more qualitative approach or broad statements such as "low risk appetite for cyber", "zero tolerance" or no explicit definition at all.

Not using concrete or quantitative metrics may hinder FMIs from effectively monitoring and managing their cyber risks, or from presenting an accurate picture of their cyber risk profile when briefing their boards. These are important elements for supporting the respective roles and responsibilities of the board and senior management, as stated in paragraph 2.3.1 in the Cyber Guidance.

Cyber Guidance

2.3.1 Board and senior management responsibilities. An FMI's board is ultimately responsible for setting the cyber resilience framework 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.

The individual or unit in the FMI responsible for approving risk levels and risk appetite also varies widely. Some FMIs indicated that their board is ultimately accountable, while others noted a range of positions from "executive board" all the way down to various management positions.

4.2.2 Cyber resilience framework and strategy

Almost all FMIs indicated that they have a documented CRF that was established in line with international standards. A significant majority of FMIs cover cyber risk tolerance policy in their CRF. FMIs have adopted different practices and approaches in setting their risk tolerances, but they are based largely on industry best practices.

All FMIs indicated that they have defined roles and responsibilities including designated key decision-makers in both business-as-usual conditions and in cyber-related crises or emergencies. Almost all FMIs indicated that they include requirements and arrangements for timely communication and coordination to enable collaboration with relevant stakeholders to effectively respond and recover from cyber attacks.

In general, the information on the CRF is documented in enterprise/operational/cyber risk management policies, information security standards/policies/guidelines, audit/risk committee charters, business continuity plans, disaster recovery plans, IT contingency plans, and/or cyber resilience response plans and procedures.

A significant majority of FMIs have a cyber resilience strategy (CRS) in place and subject the CRS to regular review, mostly on an annual or biennial basis. However, there were three subsets of outliers in terms of review frequency. Regarding the first subset, in at least one FMI, the CRS was reviewed every five years, in accordance with the business strategy review timeline. In the second subset, a few FMIs reviewed the CRS "according to the relevant changes in the FMI infrastructure and the scenario of cyber threats." In the third case or subset, the CRS was adapted as needed, with no defined period of review. Further, a significant majority of FMIs had the CRS approved by the board, except for a few FMIs.

A few FMIs indicated that the development of their CRS did not involve relevant business units (eg business, finance, risk management, internal audit, operations, cyber security, information technology, communications, legal and human resources). For at least one FMI, the CRS was developed with inputs from the IT and cyber security units, was reviewed by the chief information security officer (CISO), chief technology officer (CTO) and chief executive officer (CEO) and was subsequently approved by the board, but it plans to include other business units in the future. In at least one case, the FMIs will include other business units in the next update of the CRS. Finally, other FMIs developed their CRS in conjunction with strategically focused business areas and the corporate risk committee.

4.2.3 Reporting to the board (or equivalent management body)

There is a clear consensus among respondents that the board's role in cyber resilience is largely strategic, while senior management are primarily responsible for operationalising and maintaining that strategy and vision.

During the industry workshop in June 2021, some FMIs mentioned that providing the board with sufficient information at the right level of depth and breadth was critical to enabling the board to form a holistic view of the FMI's cyber programme. This would, in turn, facilitate sound decision-making at the board level to advance the FMI's resilience programme. Internal/external reviews and testing performed by security experts are key activities that would help to apprise the board of the FMI's security posture.

Regarding their reporting practices, some FMIs provide their audit and risk committees with summaries of the reviews and testing performed by internal and external cyber security specialists in board meeting packages. Industry workshop participants also indicated that while the board receives various reports from audit, IT, cyber/information security and risk functions, most of this reporting is conducted separately – resulting in information that is relevant for board decision-making on cyber resilience being fragmentary in nature. It is crucial to have a process to synthesise all relevant information so that the board has a holistic view of the risks. This industry perspective sheds some light on the complexity of cyber

reporting and the potential impact it could have on FMIs' capacity to evolve and learn from internal and external experiences.

4.2.4 Experience and ability of the board (or equivalent management body) members

Some FMIs reported that they rely on information about the past work experience of board and senior management members. However, a few explicitly mentioned reliance on periodic mandatory training and awareness activities that have been undertaken (eg information presented to the board and senior management) to determine their skill level for managing cyber risks. Some FMIs did not describe the process or metrics with which the FMI assesses the cyber risk-related skills, knowledge and awareness of its board members (or the equivalent management body). At least one FMI stated that no such metrics exist.

Many FMIs did not provide a description of the process or metrics through which they assess the level of cyber risk-related skills of its board members. Where such assessments are absent, there may be a lack of visibility and assurance over whether board members have the knowledge and capacity needed to understand the potential impact of cyber events, and their risks to the organisation and to its ecosystem to provide effective oversight. Given the importance of training to help the board better understand and manage cyber risk, examples of training programmes conducted by some FMIs are set out below (taken from the responses to the survey):

- awareness and security training sessions (eg annual training) on cyber issues conducted by external firms;
- new directors receive a comprehensive introduction to relevant cyber topics by internal cyber experts;
- "on the job" training (eg information presented to the board/senior management);
- regular IT/cyber briefings;
- dedicated workshops; and
- annual evaluations facilitated by external consultants.

4.2.5 Senior executive responsible for cyber resilience and CISO reporting line

Almost all FMIs confirmed that a senior executive is responsible and accountable for cyber resilience where the level of authority and independence necessary to execute the cyber strategy and bolster a firm's resilience posture is typically mandated in the charter and approved by relevant committees of the board. A small number of FMIs noted that the chief risk officer (CRO) is responsible for managing an FMI's risks, including cyber risk. Other FMIs noted that the CISO commonly reports to the CTO, the chief operating officer (COO) or the chief information officer (CIO) in the first line of defence. In some instances, the CISO even reports to board level committees such as the audit committee as the overseer of the third line of defence, along with other combinations of reporting arrangements.

The diversity among FMIs on the CISO's reporting structure provides some insight about how various reporting structures might ensure or compromise the CISO's independence and ability to effectively execute the FMI's cyber resilience programme. The CISO's authority and influence could differ depending on whether they are in the first line of defence (eg reporting to CTO/CIO) or in the second line of defence (eg reporting to CRO). In addition, the reporting structure may also affect the CISO's ability to operationalise the cyber strategy. Hence, it is important to consider how to ensure that the CISO has sufficient independence, authority, resources and access to the board – or to committees designated by the board – to execute the cyber resilience strategy.

4.3 Testing

Issues of concern

- A number of FMIs are not conducting cyber resilience testing after a significant change in their systems. For example, a significant majority of FMIs do not test the integrity of backup data, some do not perform vulnerability assessments and most do not perform penetration testing after a significant change has occurred. This is a gap or shortcoming in FMIs' implementation outcomes relevant to Principle 17 KC 2, which should be addressed.

- Multiple FMIs may not be conducting comprehensive scenario-based testing, which calls into question whether these FMIs have adequately validated their ability to recover and resume operations following a cyber disruption. For example, some FMIs indicated that they are not testing governance arrangements in scenario-based testing exercises. This is a gap or shortcoming in FMIs' implementation outcomes relative to Principle 17 KC 6, which should be addressed.

- Some FMIs did not include FMI participants, and most did not include critical service providers and linked FMIs in the testing of their response, resumption and recovery plans and processes with respect to cyber incidents. This calls into question FMIs' ability to meet Principle 17 KC 7 with regard to identifying, monitoring and managing risks from external parties. This may also impact whether an FMI is able to demonstrate its ability to recover and resume operations following a cyber incident as foreseen in Principle 17 KC 6. These are issues of concern that should be addressed.

Observations

- Multiple FMIs may not be retesting and/or validating the remediation of vulnerabilities identified through testing.

- A small number of FMIs indicated that red team testing is currently not part of their cyber testing strategy; however, the majority of these FMIs had plans to incorporate it in the near future.

- Some FMIs included only phishing (and not social engineering and physical penetration) as part of their penetration testing programmes. In addition, a small number of FMIs did not incorporate threat intelligence as part of penetration testing.

- Some FMIs' industries and a small number of FMIs' relevant authority or authorities had not conducted industry-wide tests or organised market-wide exercises in the last three years.

4.3.1 Cyber testing programme

The FMIs generally consider cyber testing to be a critical aspect of their overall cyber resilience strategy. Their cyber testing programmes are, for the most part, guided by international, national or commonly accepted industry standards.[8] In general, setting a cyber testing strategy, and reviewing the results of periodic exercises, are overseen at the board level for a significant majority of FMIs.[9] However, there is a high degree of variance among FMIs in terms of how often their management bodies and/or boards receive updates on their firms' cyber testing plans and activities.

[8] The exception was at least one FMI, which did not provide information on whether commonly accepted standards and guidelines are the basis for its cyber resilience strategy.

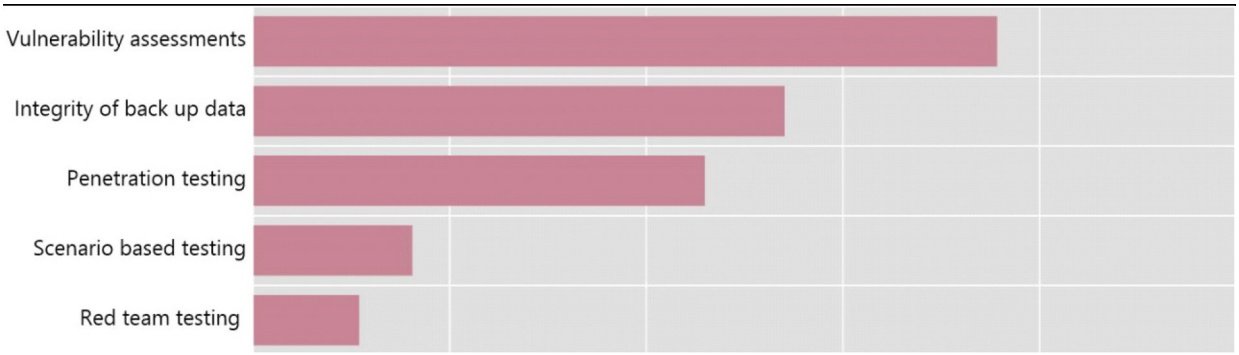
[9] The remainder of the FMIs indicated that cyber testing exercises are reported to senior management bodies/groups other than the firm's board. Examples of alternative approaches include the following examples: an FMI's testing programme is overseen by the FMI group continuity and risk committee, which reports to the FMI group management committee which is separate from the board. An FMI reports results to its information security management forum, which is chaired by senior management on a quarterly basis. An FMI reported that the board is not involved other than receiving regular update reports.

The discussion during the industry workshop in June 2021 also highlighted difficulties in providing the appropriate level of detail when presenting the test results to FMIs' boards. It was noted that highly technical presentations may confuse the board, detracting from the broader risk management focus, while on the other hand, too little detail could potentially result in misguided actions and decisions. Some workshop participants felt that the area of testing received less attention from the board than audit findings or reports of actual incidents. They also suggested that further upskilling of board members would be desirable.

While all FMIs responded that they test and verify the integrity of their backup data on an annual basis at a minimum, a significant majority of FMIs stated that they test this on a more frequent periodic basis ie semiannually, quarterly or monthly.[10] All but at least one FMI reviewed and adjusted their cyber testing programmes at least annually or after significant changes.[11]

However, multiple FMIs were not conducting cyber resilience testing after significant changes: a significant majority of FMIs did not conduct integrity of backup data testing, some did not conduct vulnerability assessments and most did not perform penetration testing after a significant change (Graph 3).

Testing after significant changes or on a monthly (more frequent) basis — Graph 3



Source: CPMI-IOSCO survey on cyber resilience of FMIs, 2021.

4.3.2 Vulnerability assessments

All FMIs stated that vulnerability assessments are part of their cyber resilience testing programmes. All FMIs affirmed that they conduct vulnerability assessments at least annually. However, most FMIs[12] indicated that they conduct vulnerability assessments following significant changes.

Additionally, some FMIs reported excluding subsets of external-facing and/or internal-facing systems from vulnerability assessments (Graph 4, left-hand panel). Of these FMIs, most stated that a risk-based approach is used to determine the scope of the scans, ensuring that critical or core systems, as well as external-facing systems, are included. At least one FMI stated that its internal-facing systems are excluded from vulnerability assessments. An FMI responded that certain excluded non-critical systems are managed by a third party, and that the vulnerability assessment could be conducted by the FMI or the third party.

It was noted that most FMIs repeat the vulnerability assessments to verify and validate the remediation of the vulnerabilities identified (Graph 4, right-hand panel).

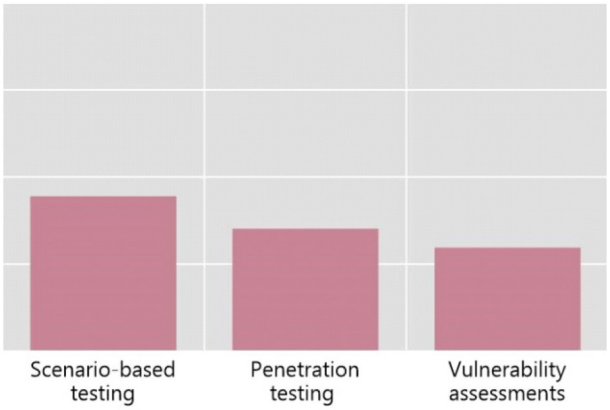
[10] A few FMIs test only the integrity of backup data on an annual basis.

[11] At least one FMI reviews its testing programme only every two years; at least one FMI reviews only after significant changes.

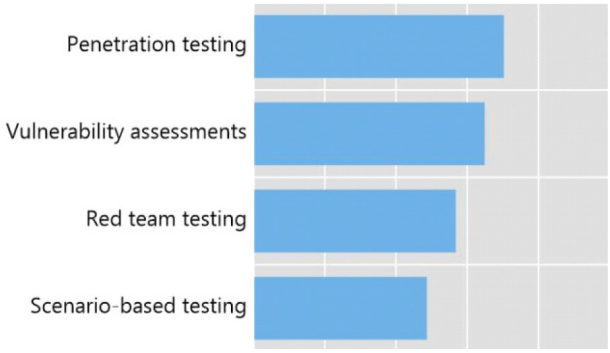
[12] Some FMIs stated that they did not conduct vulnerability assessments after major changes.

Vulnerability assessments Graph 4

FMIs that exclude systems from testing



FMIs that retest or validate the remediation of vulnerabilities identified by testing



Source: CPMI-IOSCO survey on cyber resilience of FMIs, 2021.

4.3.3 Scenario-based testing

FMIs generally indicated that they conduct scenario-based testing as part of their cyber resilience testing programme. At least one FMI highlighted that it is in the process of determining the effectiveness of such testing and will decide whether scenario-based testing should be incorporated into the FMI's cyber resilience framework. A few FMIs are in the early stages of rolling out scenario-based testing and are either beginning to operationalise such tests or have recently conducted a scenario-based tabletop. For FMIs that conduct scenario-based testing, they do so at least annually. Only a few of the FMIs conduct such tests after significant changes, or on a monthly or more frequent basis.

In terms of the scope of such testing, a few FMIs specifically noted that they covered extreme but plausible cyber attack scenarios, although this was not specifically asked as part of the survey. The Cyber Guidance advocates the use of cyber threat modelling to the extent possible to imitate cyber threat characteristics in FMIs' scenario-based testing. A significant majority make use of cyber threat intelligence, while some FMIs currently use threat modelling to imitate the unique characteristics of cyber threats. During the June 2021 industry workshop, some FMIs highlighted that more guidance is needed in relation to areas of focus for testing to ensure their cyber security defences and testing programmes are sufficiently comprehensive to keep up with the latest threats, especially following recent events (eg the SolarWinds incident).

Although FMIs are expected to test their resilience arrangements in relation to people, processes and technology as per Principle 17 KC 6 and as described in the Cyber Guidance, some FMIs surveyed include all of the components below in their scenario-based testing programmes (Graph 5):

- data destruction;
- data integrity corruption;
- data leakage;
- system or data unavailability;
- incident detection;
- incident response plans and communication protocols; and

- system recovery plans and governance arrangements.

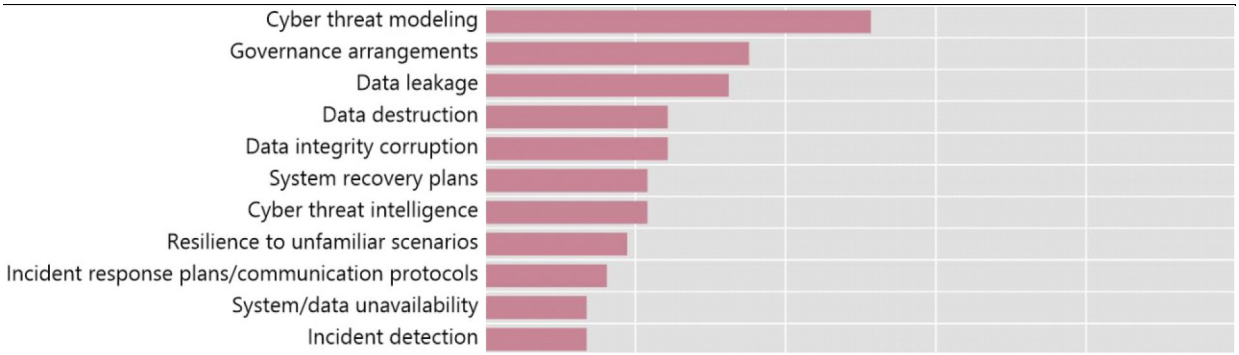
Particularly lacking for some FMI respondents was the testing of governance arrangements, which is conducted by most FMIs. The lack of more comprehensive scenario-based testing calls into question whether FMIs are meeting risk management expectations around testing the ability to recover from a cyber event within the expected 2hRTO.

During the June 2021 industry workshop, participants highlighted time and resource constraints in conducting testing beyond their IT operations staff, and recognised the need to have a good strategy and plan to cover the other dimensions (eg crisis communication and response, business areas and industry stakeholders) in their testing programmes without overburdening themselves.

A few FMIs were observed to be using more advanced technology (eg governance, risk and compliance tools) to manage their testing programmes. However, a few FMIs do not meet expectations contained in the Cyber Guidance around cyber resilience testing for unfamiliar scenarios. Additionally, most FMIs retest and/or validate vulnerabilities identified during scenario-based testing.

Finally, some FMIs exclude a subset of systems from scenario-based testing. Of these FMIs, many cite resource constraints and/or the use of a risk-based approach to determine the criticality of systems for inclusion in testing.

Scenario-based testing Graph 5



Source: CPMI-IOSCO Survey on cyber resilience of FMIs, 2021.

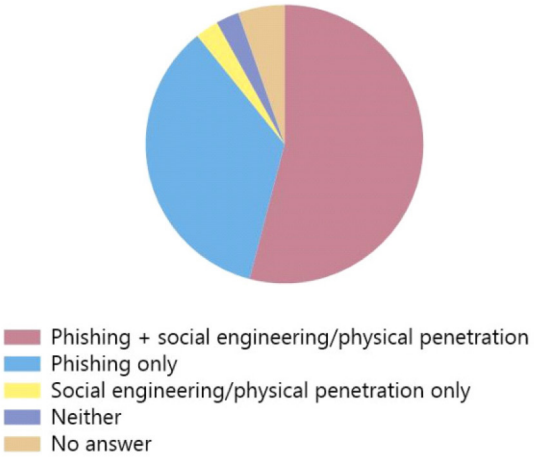
4.3.4 Penetration testing

All FMIs perform penetration testing at least annually as part of their cyber testing programme. However, some FMIs surveyed conduct testing after a significant change in their IT environment, or on a monthly or more frequent basis. Most FMIs conduct tests that include both phishing and social engineering/physical penetration scenarios, although it should be noted that FMIs responded that these scenarios are often covered by red team testing (Graph 6, left-hand panel). In addition, a small number of FMIs responded that threat intelligence is not incorporated as part of penetration testing.

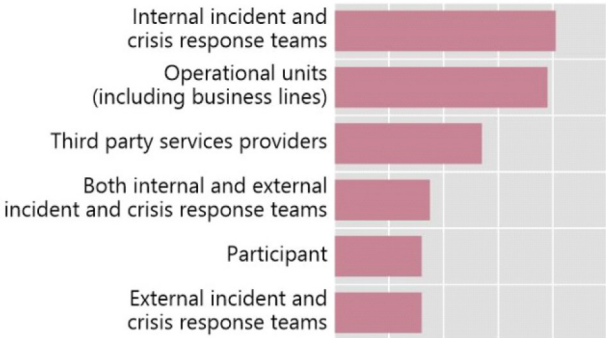
Penetration testing

Graph 6

Penetration testing scope



FMIs including internal and external stakeholders in penetration testing



Source: CPMI-IOSCO survey on cyber resilience of FMIs, 2021.

Some FMIs surveyed indicated that a portion of either external or internal systems were excluded from penetration testing. A significant majority indicated that they include both internal and external operational units, including business lines, in their penetration testing exercises. A significant majority incorporate internal response teams, while some include external response teams. Some FMIs include both internal and external response teams. With regard to critical service providers and FMI participants, most include third-party service providers, and some FMIs involved their participants in penetration testing (Graph 6, right-hand panel).

4.3.5 Red team tests

A significant majority of FMIs[13] include red team tests in their testing programme. A few FMIs indicated plans to start red team testing (some of which were in conjunction with the rollout of national red team testing frameworks). The predominant testing frequency is annual, while a few FMIs indicated that they performed red team testing after significant changes or on a different frequency basis. A few respondents mentioned that their red team testing is guided by regulatory requirements (eg national testing frameworks).

A significant majority of FMIs[14] employed external experts to execute the test and some[15] also included (or planned to include) internal staff. While the distribution of tasks between internal and external staff was not expressly covered in the survey, those FMIs that elaborated on their red team processes indicated that internal experts typically assist in scoping the tests, which were then executed by external personnel. This is in line with the Cyber Guidance 7.2.2-d, which states that 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. In terms of prioritisation of the test findings for remediation, FMIs generally use risk-scoring of the

[13] A small number of FMIs indicated that red team testing is currently not part of their cyber strategy, of which; a few FMIs planned to incorporate it into their cyber strategies in the near future; a few FMIs indicate no plans to do so.

[14] A significant majority of FMIs were engaging in red team testing; and a few FMIs were planning to roll out red team testing employing external experts.

[15] Of these FMIs, at least one only planned to include internal experts in the future.

identified threats/vulnerabilities, based on likelihood of risk event and impact on the business functions. Some of them follow industry practices and methodologies (eg Vulnerability Priority Rating, Common Vulnerability Scoring System, Open Web Application Security Project), while others apply internal methodologies (eg internal audit charter).

In relation to remediation monitoring, FMIs often employ project management tools to create projects and workplans for remediation, set the deadlines, and assign responsibilities to business owners. Some FMIs indicated that the status of their remediation is monitored by a standing committee with senior management and/or regulator involvement. A few FMIs indicated that they use IT tools (such as databases and risk management tools) to support the remediation tracking processes. Most indicated that follow-up tests were conducted to verify the effectiveness of remedial measures.[16]

4.3.6 Other testing practices or methodologies

FMIs generally acknowledged that they follow the categories of tests described in the Cyber Guidance (ie vulnerability, scenario-based, penetration and red team assessments) in their practices. For the most part, FMIs indicated that they did not adopt other testing practices or methodologies aside from those described in the Cyber Guidance. Among the FMIs that had indicated that they were employing other testing practices or methodologies, a few mentioned training exercises and testing on disaster recovery.

4.3.7 Coordination

Principle 17 KC 7, supplemented by the Cyber Guidance, emphasises the importance of identifying, monitoring and managing the risks posed by external parties including participants, other FMIs and service providers. However, some FMIs do not include external parties (eg FMI participants, critical service providers or linked FMIs) in the testing of their cyber response, resumption and recovery plans or processes (Graph 7). A lack of testing coordination with external parties calls into question the overall comprehensiveness of an FMI's cyber resilience testing programme and, in particular, the ability to recover and resume operations following a cyber incident.

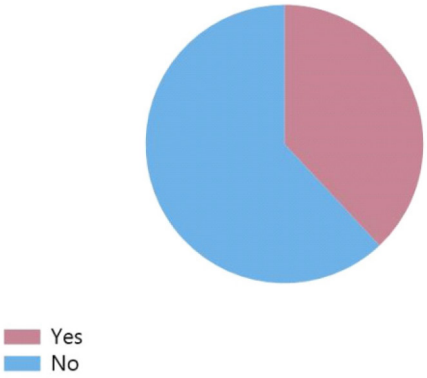
PFMI – Principle 17 KC7

An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs.

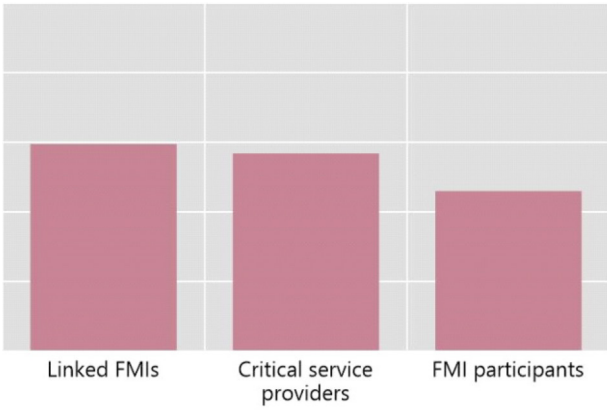
[16] A significant majority of the FMIs that perform red team testing retest and/or validate their test results.

Testing with external parties Graph 7

FMIs that exclude external parties from cyber resilience testing



FMIs that exclude external parties in cyber resilience testing by type



Source: CPMI-IOSCO survey on cyber resilience of FMIs, 2021.

Although industry-wide testing is also considered useful for achieving the timely market-wide recovery of operations and is advised in the Cyber Guidance, some FMIs' industries and a small number of FMIs' relevant authorities had not conducted industry-wide tests or organised market-wide exercises in the last three years.[17] Consideration may be given to whether authorities and the industry should be encouraged to conduct industry-wide tests or organise market-wide exercises, as appropriate.

4.4 Learning and evolving

Observations

- While all FMIs confirmed participation in broader forums to exchange information on lessons learnt, some FMIs indicated that they were not required to share cyber information with a centralised agency, although they may still do so on a voluntary basis.
- Among the small number of FMIs that do not use cyber tests or other lessons learnt to improve their operational resilience objectives, there are FMIs that are considering using their cyber tests to meet this goal.

4.4.1 Reviewing the resilience posture

All FMIs reported that their resilience posture is reviewed at least annually, and a significant majority indicated that this review is done at every level. The scope and depth of the reviews conducted were observed to vary significantly. For example, some FMIs indicated that they rely on the results of the resilience tests to perform the review, whereas others asserted that risk assessments performed by operational units are reviewed by risk management and information security and then endorsed by a dedicated board at enterprise level.

[17] Some FMIs selected, "The FMI's industry did not conduct industry-wide tests in the last three years." At least one FMI selected, "The FMI's industry did not conduct industry-wide tests in the last three years, but is in the process of implementing a test that will take place within the next year." A small number of FMIs selected, "The FMI's relevant authority/authorities did not conduct exercises in the last three years."

4.4.2 Defining the attack surface

A few FMIs indicated that they did not define their attack surfaces. A significant majority of FMIs provided a range of parameters that they used to describe their attack surfaces. These parameters include business operations, IT systems and infrastructure (software and hardware), and people. Overall, there seemed to be a general tendency among most FMIs just to test their IT environment against known vulnerabilities, but this alone would not be sufficient to enable them to define and explore their entire attack surfaces.

As stated in paragraph 7.2.2-d of the Cyber Guidance, FMIs are encouraged to conduct red team testing, and use it as a means to test beyond the known vulnerabilities and explore the attack surfaces to identify other possible cyber security weaknesses in their environment. This is important as attackers will often think out of the box and could go beyond exploiting known vulnerabilities to attack their targets.

Cyber Guidance

7.2.2d. 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.

4.4.3 Lessons from cyber events

All FMIs indicated that they had capabilities in place to distil key lessons from common vulnerabilities, cyber threats, events and incidents occurring within their environment. A significant majority of FMIs indicated that they were also able to do so for incidents occurring outside the FMI, through information obtained from information-sharing for groups, authorities and regulars, external cyber security experts, as well as public sources from the internet.

All FMIs confirmed participation in broad forums to exchange information on lessons learnt. FMIs highlighted that they had benefited from access to information on potential and actual threats, as well as best practices on security measures, to shape their CRF. A significant majority of FMIs stated that they were required to share cyber information with a centralised agency, such as a national regulator (some FMIs), national cyber/information security agency (a small number of FMIs) and law enforcement agencies (a few FMIs). Some FMIs indicated that they were not required to share cyber information with a centralised agency, although the FMIs may still do so on a voluntary basis.

4.4.4 Acquiring new knowledge and capabilities

Almost all FMIs monitor technological developments and new cyber risk management measures to actively counter existing or new cyber threats. FMIs listed industry forums, regulators and public agencies, as well as industry experts and online publications and bulletins, as the sources of information that they monitor. A key area mentioned was the acquisition and use of external (both open source and commercial) threat intelligence to understand and achieve awareness of the evolving cyber threat landscape. At least one FMI also mentioned monitoring technical developments in the area of cloud and virtualisation technologies (eg container and Kubernetes).

A significant majority of FMIs have made progress in developing capabilities to help pre-empt and address future cyber risks. Apart from cyber threat intelligence and information-sharing, FMIs made references to acquiring new solutions in machine learning, user and entity behavioural analytics, multi-factor authentication, endpoint detection and response, threat hunting and red teaming exercises.

The rest of the FMIs are in the process of reassessing and monitoring their cyber defence capabilities. Some FMIs also highlighted that they use third parties to perform industry benchmarking to help them in identifying gaps in their cyber resilience framework.

4.4.5 Cyber resilience benchmarking

A significant majority of FMIs indicated that they are using metrics to identify gaps in their cyber resilience frameworks. These FMIs also use audit results, security operation centre metrics and key risk indicators to improve their cyber resilience, despite the fact that three quarters of these FMIs operate in jurisdictions that did not require the use of any cyber-related metrics or benchmarks. The FMIs that are not using metrics are either considering the use of metrics in the future or are using other ways to identify gaps in their framework.

A small number of FMIs currently do not use a maturity model to assess their cyber resilience, although three of these FMIs are evaluating the inclusion of a cyber resilience model in their cyber resilience processes. Those that do use a maturity model to assess their cyber resilience often cite industry standards, such as the National Institute of Standards and Technology (NIST) *Cybersecurity framework* and the ECB's *Cyber resilience oversight expectations for financial market infrastructures*. A few FMIs also mentioned *Process assessment model*, *Control objectives for information and related technology* (COBIT) and *Security incident management and capability maturity model integration*. Some FMIs use only one maturity model while others may use two or more at the same time.

A significant majority of FMIs use cyber tests (eg red teaming, penetration testing, compromise assessments, disaster recovery and BCP testing etc) and lessons learnt through past incidents, audit reports and third-party analyses to improve their operational resilience objectives. Many FMIs said that the frequency of the tests depends on the type of test. Among the small number of FMIs that do not use cyber tests or other lessons learnt to improve their operational resilience objectives, there are FMIs that are considering using their cyber tests to meet this goal, and other FMIs felt that their operational resilience objectives were adequate, and they had not changed or improved from the cyber tests conducted. In these cases, it was not clear whether the cyber tests had been challenging enough to stress-test the FMIs.

Annex A – Survey questions

FMI type

Please select one option:

- Payment system
- Central securities depository/securities settlements system
- Central counterparty
- Trade repository

Any overall comments/contextual information about your survey responses:

[Text box to complement response]

General questions

A. Is the FMI aware of and familiar with the *Guidance on cyber resilience for financial market infrastructures* ("Cyber Guidance")?
   a. Yes
   b. No

   If yes, has the FMI used or made reference to it to design its cyber resilience framework? If the FMI has not used the cyber guidance, please explain how the FMI has designed its cyber resilience framework.
   [Text box to complement response]

B. Has the FMI used or made reference to any other guidance, frameworks or standards to design its cyber resilience framework:
   a. No
   b. Yes, from public authorities
   c. Yes, from industry bodies or private sector
   d. Yes, from both public authorities and industry/private

   If yes, please indicate which one(s):
   [Text box to complement response]

C. Has the FMI developed concrete (ie documented) cyber response and recovery plans to meet the two-hour recovery time objective (2hrRTO)? Please select the appropriate option and provide details in the space below.
   a. Yes (please indicate if these plans have already been provided to the FMI's primary supervisory authority(ies) and/or overseer(s))
   b. No

   [Text box to complement response]

D. Does the FMI have plans in place to address cyber scenarios which, if materialised, would lead to the FMI not meeting its intended recovery time objectives?
   a. Yes
   b. No

E. Do the FMI's crisis communications plans address extreme but plausible cyber disruption scenarios?
   a. Yes
   b. No

F. Does the FMI have policies and procedures to enable the disclosure of potential vulnerabilities and/or incidents?
   a. Yes
   b. No

G. Does the Covid-19 pandemic situation (and in particular, the work from home (WFH) and split team arrangements at the FMI, FMI participants and third-party service providers) affect the ability of the FMI to prevent, detect, respond to or recover from cyber incidents?
   a. Yes (please provide details)
   b. No (please provide details)

[Text box to complement response]

Governance

According to the Cyber Guidance, cyber governance refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks. The purpose of this section is: (i) to gather information on FMIs' cyber governance arrangements; (ii) to understand whether the governance methodologies and practices of the FMIs as a group (including by FMI type) achieve outcomes consistent with the PFMI; and (iii) to understand whether FMIs' cyber resilience governance programmes have been informed by the Cyber Guidance.

The questions below are informed by the relevant KCs of **Principle 2**.

Cyber resilience objectives and governance arrangements

1. Does the FMI's cyber resilience programme include cyber resilience objectives?
   a. Yes (please provide details)
   b. No

   [Text box to complement response]

2. How does cyber risk management (CRM) fit into the FMI's broader risk management objectives? (Please check the applicable box)

a.	CRM is part of the enterprise risk management process	Please provide further detail. [Text box to complement response]
b.	Not part of the enterprise risk management process, but the general principles are aligned	Please provide further detail. [Text box to complement response]
c.	Not part of the enterprise risk management process, and the general principles are not aligned at all	Please explain. [Text box to complement response]

3. How does the FMI assess its performance in meeting its cyber resilience objectives? Please check one or more options from the list below that apply:
   a. Through identified metrics
   b. Through periodic assessments
   c. Through monitoring activities
   d. Other (please specify and explain, particularly regarding changes, if any, to the way the FMI assesses its performance in meeting its cyber resilience objections, as a result of the Covid-19 pandemic):

      [Text box to complement response]

4. What activities does the FMI's board (or the equivalent management body) participate in to support the organisation's management of cyber risks and ensure the cyber resilience of the FMI?
   [Text box to complement response]

Cyber resilience framework

5. Does the FMI have a documented cyber resilience framework (CRF)?
   a. Yes (please list and explain at a high level the CRF's main components (ie specific policy provisions, specific roles and responsibilities, procedures for cyber incidents, performance indicators etc))
   b. No (please explain why)

   [Text box to complement response]

6. Does the CRF address the FMI's risk tolerance policy?
   a. Yes (please describe below)
   b. No

   [Text box to complement response]

7. Does the CRF define roles and responsibilities, including accountability for decision-making, in both "business as usual" conditions and crisis/emergencies for cyber-related matters/situations?
   a. Yes
   b. No

8. Does the CRF include requirements for timely communication and coordination arrangements to enable the FMI to collaborate with the relevant stakeholders to effectively respond and recover from cyber attacks?
   a. Yes (please provide further details on the requirement(s) and list any additional component)
   b. No

   [Text box to complement response]

9. Regarding the risk acceptance level required, please specify the following:

a.	How are "acceptable risk levels" defined in the CRF?	[Text box to complement response]
b.	Who is responsible for approving a risk level as "acceptable"?	[Text box to complement response]
c.	Are roles and responsibilities for defining and adhering to risk levels defined within the overall cyber risk framework (eg has a senior individual been appointed as accountable for this role/responsibility)? Please provide descriptions of the roles and responsibilities.	[Text box to complement response]

10. With regards to cyber risk management, were any changes made, planned and/or are under consideration to the aforementioned factors in Q9 as a result of the Covid-19 pandemic?
    a. Yes (if changes were made, planned or under consideration, please specify the changes and the reasons for those changes)
    b. No (please explain why not)

    [Text box to complement response]

11. How is the adequacy and effectiveness of the FMI's CRF being assessed? Please select all that apply:
    a. Independent internal audits
    b. Compliance assessments
    c. Information security risk assessments (includes information security reviews, penetration tests) performed by internal teams
    d. Information security risk assessments performed by third party
    e. Other risk assessments than (c) or (d); please specify
    [Text box to complement response]
    f. Other measures (please specify)
    [Text box to complement response]

12. What leading industry cyber security framework, standards and guidelines are being used (eg NIST-CSF, COBIT, ISO/IEC 27000 etc)?
    Please list the standards/guidelines and elaborate on how these relevant standards and frameworks are adopted and contextualised within the FMI.
    [Text box to complement response]

13. Does the FMI periodically review and update its CRF to ensure it remains relevant?

Yes	a. Please specify the frequency of the review and updates. [Text box to complement response] b. Please describe the methodology followed for reviewing and updating and the subjects/business functions involved in the process. [Text box to complement response] c. Please explain whether changes (and if so, what changes) were made to the frequency of review and/or updates as a result of the Covid-19 pandemic. Please include both changes already implemented and those that are planned or under consideration for the near to medium term, but not yet implemented. [Text box to complement response]
No	Please explain why, including if/when the FMI intends to review and update its CRF. [Text box to complement response]

Cyber resilience strategy (CRS)

14. Please describe the FMI's CRS.
    [Text box to complement response]

15. Regarding CRS please provide the following information.

Question	Yes	No
a. Does the FMI have a documented CRS in place?	Does the strategy covers the following key components: • mission, vision, goals & objectives; • roles and responsibilities; • main internal and external stakeholders; • governance model;	Please explain why not. [Text box to complement response]

	• cyber maturity targets and roadmap; and • capabilities relating to people, processes and technology. [Text box to complement response]	
b. Has the CRS been approved by the FMI board (or the equivalent management body)?	[Text box to complement response]	Please explain why not. [Text box to complement response]
c. Is the CRS subject to regular review?	[Text box to complement response]	Please explain why not. [Text box to complement response]
d. Is the CRS aligned with the overall corporate strategy, the business strategy and other relevant strategies (eg the IT strategy and the business continuity strategy)?	Please explain how by providing specific examples. [Text box to complement response]	Please explain why not. [Text box to complement response]
e. Has the CRS been developed by involving relevant business units (eg business, finance, risk management, internal audit, operations, cyber security, information technology, communications, legal and human resources) and aligned with the overall response and recovery priorities of the FMI?	Please provide a brief description of the business units involved. [Text box to complement response]	If no, please explain why certain business units have not been involved in the development [Text box to complement response]
f. Have changes been made or planned to the CRS as a result of the Covid-19 pandemic? Please include both changes already implemented and those that are planned or under consideration for the near to medium term.	Please explain what changes have been made, planned or are under consideration. [Text box to complement response]	If no, please explain how the current CRS works in the pandemic situation. [Text box to complement response]

16. Has the FMI enhanced its CRS through coordination with the relevant stakeholders on the design of resilience solutions?
    a. Yes
    b. No

17. Has the FMI had to manage trade-offs between security and the continuity of its operations as a result of the Covid-19 pandemic?
    a. Yes (please provide details of how the trade-off influenced the decision)

b. Under consideration (please explain when and how the FMI would make a decision)
c. No (please explain why the FMI has decided not to make an adjustment)

[Text box to complement response]

18. Has the FMI adjusted its controls and measures in light of the Covid-19 pandemic situation to address the risks that third-party service providers pose to the FMI's organisation and its operations?
    a. Yes (please provide additional details of how the governance arrangements of the FMI towards third party service providers have been adjusted)
    b. Under consideration (please explain when and how the FMI would make a decision)
    c. No (please explain why the FMI has decided not to make an adjustment including additional details of the FMI's considerations and decision-making)

    [Text box to complement response]

19. Has the FMI implemented any policy changes in order to support remote working arrangements? If so, how has the FMI ensured the workforce is able to continue operating in a safe and secure manner from a cyber resilience perspective?
    a. Yes (please provide details)
    b. Under consideration (please explain when and how the FMI would make a decision)
    c. No (please explain why the FMI has decided not to make an adjustment, and please also explain how the existing arrangements facilitated the major shift of the disrupted workforce)

    [Text box to complement response]

Roles and responsibilities of the FMI board (or the equivalent management body) and senior management for cyber resilience

20. Are the cyber resilience roles and responsibilities of the FMI board (or the equivalent management body) specified?[18]

Yes	a. In what type of document(s)? [Text box to complement response]
	b. Please describe the roles and responsibilities. [Text box to complement response]
	c. Are these roles and responsibilities clearly identified to the relevant individuals? i. Yes ii. No
	d. Has the FMI board (or the equivalent management body) formally approved the CRS? i. Yes ii. No
No	Please explain why not, including if/when the FMI board (or the equivalent management body) intends to provide a formally approved CRS in the future. [Text box to complement response]

[18] Special considerations for central bank-owned FMIs apply, see CPMI-IOSCO, *Application of the Principles for financial market infrastructures to central bank FMIs*, August 2015. Where an FMI is operated as an internal function of the central bank, Principle 2, Key Considerations 3 and 4 on governance are not intended to constrain the composition of the central bank's governing body or that body's roles and responsibilities.

21. Describe how the management engages with the FMI board (or the equivalent management body) on cyber resilience and describe the board's role in related oversight.
    [Text box to complement response]

22. How does the FMI determine whether its board (or the equivalent management body) members and the senior management[19] have the appropriate level of skills, knowledge and awareness to understand and manage cyber risks? Please also describe the process or metrics through which the FMI assesses the level of cyber risk-related skills, knowledge and awareness of its board (or the equivalent management body) members and senior management.
    [Text box to complement response]

23. Describe how the FMI's senior management oversees the FMI's implementation of its cyber resilience framework, policies and controls.
    [Text box to complement response]

24. Is there a senior executive responsible and accountable for the cyber resilience strategy and framework of the FMI?

Yes	a. Please explain how it is ensured that the senior executive has sufficient seniority, authority, independence, resources and access to the FMI board (or the equivalent management body). [Text box to complement response]
	b. Please explain how human resources and budgets are allocated within the FMI to secure sufficient resources for cyber resilience. [Text box to complement response]
	c. Please explain the modality and frequency of reporting by the senior executive to the FMI board (or the equivalent management body) on cyber resilience strategy-related matters and/or cyber resilience framework-related matters. [Text box to complement response]
No	Please explain why not, including if/when the FMI intends to establish a senior executive responsible and accountable for the cyber resilience strategy and framework in the future. [Text box to complement response]

Testing[20]

Testing is the means by which an FMI validates that it has identified, and implemented effective measures to address risks to its systems, and thus testing is an integral component of any cyber resilience framework. 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.

The purpose of this section is: (i) to gather information on FMIs' cyber-resilience testing programmes implemented to address cyber risk; (ii) to understand whether the testing methodologies and practices of the surveyed FMIs as a group (including by FMI type) achieve (in the context of cyber risk) outcomes consistent

[19] "Senior management" refers to persons who exercise executive functions within the FMI and who are responsible and accountable to the FMI board or the equivalent management body for the day-to-day management of that FMI.

[20] Relevant Principles and Key Considerations: P17, KC 1, 2, 5, and 7; P3, KC 1 and 3.

with Principle 3 and Principle 17 of the PFMI and their relevant underlying Key Considerations; and (iii) to understand whether an FMI's cyber resilience testing programme has been informed by the Cyber Guidance.

The questions below are informed by the relevant Key Considerations of Principle 3 and 17 of the PFMI as well as Section 7 of the Cyber Guidance. The survey questions are focused on the methodologies and practices mentioned in Section 7 of the Cyber Guidance – vulnerability assessments, scenario-based testing, penetration testing, and red team tests – for definitions, please see the Glossary in the Guidance on cyber resilience for financial market infrastructures, the FSB cyber lexicon and the glossary at the end of the survey (Annex 1). While these methodologies and practices may partly overlap or be combined, each should be considered individually for the purposes of this survey. The survey questions seek to gather information about the nature, scope and frequency of such tests, the range of systems tested, as well as how the results of such testing are used, among others. To the extent that the FMI is not conducting these types of test, the CPMI and IOSCO are interested in learning about the FMI's methodologies and practices employed to achieve cyber resilience as well as the FMI's coordination of its cyber testing programme with relevant stakeholders in its ecosystem.

General questions on FMI's cyber testing programme

25. How does testing fit within the FMI's overall strategy for cyber resilience?
    [Text box to complement response]

26. How frequently is the FMI's cyber testing programme reviewed (ie scope, objectives, nature of threats considered etc)? Please select all that apply. Where an explanation is required, please use the comment box below:
    a. Annually
    b. After significant changes (please explain)
    c. Other (please explain)

    [Text box to complement response]

27. A. How does the management of the FMI communicate the objectives, scope and results of cyber testing to its board (or the equivalent management body) (eg regular updates at the board (or the equivalent management body) meeting, ad hoc documentation provided occasionally etc)?
    [Text box to complement response]

    B. How does the FMI board (or the equivalent management body) oversee the FMI's cyber testing programme (eg approval of the framework for testing, discussion of the results of testing etc)?
    [Text box to complement response]

28. How often is the integrity of backup data tested? Please select all that apply. Where an explanation is required, please use the comment box below.
    a. Annually
    b. Quarterly
    c. Monthly
    d. After significant changes (please explain)
    e. Other frequency (please explain)
    f. Never (please explain)

    [Text box to complement response]

29. Does the FMI use leading international, national and industry-level standards, guidelines, frameworks or recommendations reflecting current industry best practices in developing its cyber testing programme?
    a. Yes (if yes, please note which standards, guidelines, frameworks or recommendations are used or followed)
    b. No (if no, please explain why)

    [Text box to complement response]

Vulnerability assessments

30. Does the FMI perform vulnerability assessments as part of its cyber testing programme?
    a. Yes
    b. No (if not, please explain and then proceed to Scenario-based testing)

    [INSERT TEXT BOX]

31. What is the frequency of vulnerability assessments? Please select all that apply. Where an explanation is required, please use the comment box below.
    a. Annually
    b. Quarterly
    c. Monthly
    d. After significant changes (please explain)
    e. Other frequency (please explain)
    f. Never (please explain)

    [Text box to complement response]

32. Is a subset of external-facing and/or internal-facing systems ever excluded from vulnerability assessments?
    a. Yes (if yes, please describe which systems (ie external- and/or internal-facing) are excluded and explain why)
    b. No (if no, please explain why)

    [INSERT TEXT BOX]

33. Does the FMI perform authenticated or unauthenticated vulnerability scans as part of its vulnerability assessments? Please select one.
    a. Authenticated vulnerability scans
    b. Unauthenticated vulnerability scans
    c. Both
    d. Neither

34. How does the FMI review, analyse and use the results of the vulnerability assessment? Specifically:
    a. When analysing the test results, how does the FMI delineate between significant vulnerabilities and false positives (eg "noise")?

       [Text box to complement response]
    b. In reviewing significant vulnerabilities, how does the FMI prioritise the vulnerabilities or threats for remediation?

       [Text box to complement response]
    c. What steps does the FMI take to ensure that any significant vulnerability/threat is remediated or that remediation is complete?

       [Text box to complement response]

Scenario-based testing

35. Does the FMI perform scenario-based testing or exercises as part of its cyber testing programme?
    a. Yes
    b. No (if not, please explain and then proceed to Penetration testing)

    [Text box to complement response]

36. What is the frequency of such testing? Please select all that apply. Where an explanation is required, please use the comment box below.
    a. Annually
    b. Quarterly
    c. Monthly
    d. After significant changes (please explain)
    e. Other frequency (please explain)
    f. Never (please explain)

    [Text box to complement response]

37. How does the FMI identify the scenarios that should be used in its cyber testing programme?

    [Text box to complement response]

38. Is a subset of external-facing and/or internal-facing systems ever excluded from scenario-based tests?
    a. Yes (if yes, please describe which systems (ie external- and/or internal-facing) are excluded and explain why)

       [Text box to complement response]
    b. No

39. Do any of the scenarios capture the following? Please select all that apply and provide a brief description.
    a. Data destruction

       [Text box to complement response]
    b. Data integrity corruption

       [Text box to complement response]
    c. Data leakage

       [Text box to complement response]
    d. System/data unavailability

       [Text box to complement response]

40. Do the scenarios test the following? Please select all that apply and provide a brief description.
    a. Incident detection

       [Text box to complement response]
    b. Incident response plans and communication protocols

       [Text box to complement response]
    c. System recovery plans

       [Text box to complement response]
    d. Governance arrangements

       [Text box to complement response]

41. Does the FMI utilise cyber threat intelligence and perform cyber threat modelling?
    a. Cyber threat intelligence?
        i. Yes

ii. No

If yes, please explain how the FMI uses this intelligence and from what types of source the FMI gathers this intelligence (eg governmental, open source, private, public).
[Text box to complement response]

b. Cyber threat modelling?
   i. Yes
   ii. No

If yes, please explain how the FMI uses cyber threat modelling and to what extent it imitates the unique characteristics of cyber threats.
[Text box to complement response]

If no, what information does the FMI use to build custom scenarios applicable to the FMI's specific threat and operating environment?
[Text box to complement response]

42. How does the FMI test resilience to unfamiliar scenarios?[21]
[Text box to complement response]

43. How does the FMI review, analyse and use the results of scenario-based testing? Specifically:
    a. How does the FMI prioritise the significant vulnerabilities/threats identified through the scenario-based testing for remediation?
    [Text box to complement response]

    b. What steps does the FMI take to ensure that any significant vulnerability/threat is remediated or that remediation is complete?
    [Text box to complement response]

Penetration testing

44. Does the FMI perform penetration testing as part of its cyber testing programme?
    a. Yes
    b. No (if not, please explain and then proceed to Red team tests.)
    [Text box to complement response]

45. What is the frequency of such testing? Please select all that apply. Where an explanation is required, please use the comment box below.
    a. Annually
    b. Quarterly
    c. Monthly
    d. After significant changes (please explain)
    e. Other frequency (please explain)
    f. Never (please explain)
[Text box to complement response]

46. Is a subset of external-facing and/or internal-facing systems ever excluded from penetration tests?
    a. Yes (If yes, please describe which systems (ie external and/or internal-facing) are excluded and explain why)
    [Text box to complement response]

[21] See Para 7.2.2, bullet point "b" for context and the Glossary of this survey for definition.

b. No

47. Does the penetration testing include the following? Please select all that apply and provide a brief description.
    a. Phishing
       [Text box to complement response]
    b. Social engineering/physical penetration
       [Text box to complement response]

48. Is threat intelligence used to design the FMI's penetration tests applicable to the FMI's specific threat and operating environment? (If yes is selected, please provide a brief description.)
    a. Yes
       [Text box to complement response]
    b. No

49. Are penetration tests performed by internal staff or third-party entities?
    a. Internal staff:
        i. Yes
        ii. No
    b. Third party:
        i. Yes
        ii. No

    Please provide a brief description.
    [Text box to complement response]

50. Do the FMI's penetration tests include internal and external stakeholders?
    a. Operational units (including business lines)?
        i. Yes
        ii. No

    b. Incident and crisis response teams?
        i. Internal:
            i. Yes
            ii. No
        ii. External:
            i. Yes
            ii. No
        iii. Both:
            i. Yes
            ii. No

    c. Third-party service providers?
        i. Yes
        ii. No

    d. Participants?
        i. Yes
        ii. No

    Please provide a brief description of your responses.

[Text box to complement response]

51. How does the FMI review, analyse and use the results of penetration testing? Specifically:
    a. How does the FMI prioritise the significant vulnerabilities/threats identified through penetration testing for remediation?
    [Text box to complement response]

    b. What steps does the FMI take to ensure that any significant vulnerability/threat is remediated or that remediation is complete?
    [Text box to complement response]

Red team tests

52. Does the FMI perform red team tests as part of its cyber testing programme?
    a. Yes
    b. No (if not, please explain and then proceed on to Coordination.)
    [Text box to complement response]

53. What is the frequency of such testing? Please select all that apply. Where an explanation is required, please use the comment box below.
    a. Annually
    b. Quarterly
    c. Monthly
    d. After significant changes (please explain)
    e. Other frequency (please explain)
    f. Never (please explain)

    [Text box to complement response]

54. Does the FMI's red team consist of the following?
    a. The FMI's own employees?
        i. Yes
        ii. No

    b. Outside experts?
        i. Yes
        ii. No

    Please provide a brief description.
    [Text box to complement response]

55. How does the FMI review, analyse and use the results of red team testing? Specifically:
    a. How does the FMI prioritise the significant vulnerabilities/threats identified through red team testing for remediation?
    [Text box to complement response]
    b. What steps does the FMI take to ensure that any significant vulnerability/threat is remediated or that remediation is complete?
    [Text box to complement response]

Other testing practices or methodologies

56. Are there tests other than those identified above (ie vulnerability assessments, scenario-based, penetration and red team) that the FMI conducts to address potential vulnerabilities, threats and cyber risks? If so, please explain.
    [Text box to complement response]

57. In the light of the FMI's cyber testing programme, do the categories of tests described in the Cyber Guidance (ie vulnerability assessments, scenario-based, penetration and red team) accurately capture the FMI's practices?
    a. Yes
    b. No (if not, please explain how the FMI's practices differ and how the categories of tests in the Cyber Guidance should evolve.)
       [Text box to complement response]

Coordination

58. In how many cyber testing exercises organised by FMI's relevant authority/authorities has the FMI participated within the last three years?
    a. The FMI's relevant authority/authorities did not conduct exercises in the last three years.
    b. The FMI's relevant authority/authorities did not conduct exercises in the last three years, but is in the process of implementing an exercise that will take place within the next year.
    c. The FMI's relevant authority/authorities conducted exercises in the last three years, but the FMI has not participated.
    d. One exercise
    e. Two exercises
    f. Three exercises
    g. More than three exercises

59. If the FMI's industry conducts industry-wide cyber tests, in how many industry-wide tests has the FMI participated within the last three years?
    a. The FMI's industry did not conduct industry-wide tests in the last three years.
    b. The FMI's industry did not conduct industry-wide tests in the last three years, but is in the process of implementing a test that will take place within the next year.
    c. The FMI's industry conducted industry-wide tests in the last three years, but the FMI has not participated.
    d. One exercise
    e. Two exercises
    f. Three exercises
    g. More than three exercises

60. With respect to cyber incidents, has the FMI tested its response, resumption and recovery plans and processes with any of the following?
    a. FMI participants
        i. Yes
        ii. No
    b. Critical service providers
        i. Yes
        ii. No
    c. Linked FMIs

i. Yes
ii. No

If yes is selected, please provide a brief description, including the frequency of the respective tests.

[Text box to complement response]

61. For each of the answers to Q58, Q59 or Q60 above that are affirmative (ie "yes"), please describe the nature and scope of these tests, if applicable, and any findings/lessons learnt from these exercises.

[Text box to complement response]

Learning and evolving

An FMI's cyber resilience framework and measures need to be constantly updated amid a continually developing technology landscape and evolving threat environment. The purpose of this section is: (i) to gather information on FMIs' cyber learning and evolving programme; (ii) to understand whether the learning and evolving methodologies and practices of the FMIs as a group (including by FMI type) achieve outcomes consistent with the PFMI; and (iii) to understand whether FMIs' cyber resilience learning and evolving programme has been informed by the Cyber Guidance.

The questions below are informed by the relevant KCs of Principle 17 and 20 of the PFMI.[22]

General questions on learning and evolving

62. Does the FMI re-evaluate its resilience posture at least annually?
    a. Yes (please describe the process)
    b. No (please explain why and if/when the FMI intends to perform such re-evaluation)

[Text box to complement response]

63. When the FMI re-evaluates its resilience posture, is this done at every level?
    a. Yes (please describe the process)
    b. No (please describe at which levels the re-evaluation is performed)

[Text box to complement response]

64. Does the FMI define and understand its attack surface[23] in both the user space and the technology space?
    a. Yes
    b. No

In either case, please comment on the basis for definition and understanding.

[Text box to complement response]

Ongoing learning: lessons from cyber events

65. Does the FMI have capabilities in place to distil key lessons from common vulnerabilities, cyber threats, events and incidents occurring within the FMI?
    a. Yes
    b. No

66. Does the FMI have capabilities in place to systematically identify and distil key lessons from cyber events that have occurred outside the FMI?

[22] Some of the Principles/Key Considerations may not apply to all FMI types.

[23] See CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, June 2016, for a definition of "attack surface".

a. Yes
b. No

If the answer is yes to one or both of Q65 and Q66, please describe how the FMI's cyber resilience framework has been impacted based on the lessons learnt. If the answer is no to one or both of Q65 and Q66, please explain why and if the FMI intends to develop such capabilities.
[Text box to complement response]

67. Does the FMI participate in broader forums (for example industry associations, regulatory/supervisory authorities or governmental organisations) to exchange information on lessons learnt?
    a. Yes (please explain how the participation in these forums have contributed to the evolvement of the resilience framework for the FMI)
    b. No (please explain why and if/when the FMI intends to participate in such forums)

    [Text box to complement response]

68. Is the FMI required to share cyber information on vulnerabilities, threats, events and incidents gathered with a centralised (eg industry, supervisory or enforcement) agency?
    a. Yes (please explain further, referencing any regulatory/supervisory requirements in the relevant jurisdictions, type of agency (eg industry, supervisory or enforcement) with whom the information is shared and the frequency of sharing)
    b. No

    [Text box to complement response]

Acquiring new knowledge and capabilities

69. Does the FMI monitor, on an ongoing basis, technological developments and new cyber risk management processes that can actively counter existing and newly developed cyber attacks (in addition to those motivated by lessons learned in the above questions)?
    a. Yes (please provide details)
    b. No (please explain why and if/when the FMI intends to monitor such developments)

    [Text box to complement response]

70. Did the FMI experience or observe an increasing number of cyber attacks (whether failed or successful) on FMI or FMI participants during the Covid-19 period?
    a. Yes (please provide details)
    b. No (please provide details)

    [Text box to complement response]

Predictive capacity

71. Has the FMI progressed in developing other forward-looking capabilities that could help pre-empt future cyber risks?
    a. Yes (please describe)
    b. No (please explain why and if/when the FMI intends to develop such capabilities)

    [Text box to complement response]

Cyber resilience benchmarking: metrics

72. Does the FMI use metrics to help identify gaps in its cyber resilience framework for remediation?
    a. Yes

b. No

In either case, please provide further details, including if the FMI is subject to cyber-related metrics in its jurisdiction.
[Text box to complement response]

73. Does the FMI use maturity models to allow it to assess its cyber resilience maturity against a set of predefined criteria, including its operational resilience objectives?
    a. Yes
    b. No

    In either case, please provide further details and indicate the maturity model used, if based on an existing industry standard.
    [Text box to complement response]

74. Has the FMI used cyber tests and other lessons learnt to improve its operational resilience objectives, including its response and recovery time objectives?
    a. Yes
    b. No

    In either case, please provide further details.
    [Text box to complement response]

75. Is the FMI subject to cyber-related metrics and benchmarks in its jurisdiction?
    a. Yes
    b. No

    If yes, please explain what these metrics are (< 200 words).
    [Text box to complement response]

Other

76. The Covid-19 pandemic situation highlighted the need for closer coordination and information-sharing between FMIs and other financial institutions and partners in their ecosystem to maintain cyber and operational resilience. Has the FMI incorporated any lessons learnt, in particular with respect to the structures for coordination and information-sharing with the relevant parties (eg participants, related parties, critical service providers etc)?
    a. Yes (please elaborate)
    b. Under consideration (please explain when and how the FMI would make a decision)
    c. No (please explain how the existing practices and structures for coordination are able to address the increased needs for coordination with the relevant parties)

    [Text box to complement response]

77. Has the FMI explicitly adjusted its cyber resilience posture and/or developed/implemented additional good practices that arose during the Covid-19 pandemic situation?
    a. Yes (please elaborate)
    b. Under consideration (please explain when and how the FMI would make a decision)
    c. No (please explain what existing practices were in place to deal with the unique circumstances that the pandemic situation brought to the FMI and its related ecosystem)

    [Text box to complement response]

78. Is there any other information or explanation that has not been covered in the previous three sections or any other information that is deemed relevant for the Assessment Team to consider for the purposes of this exercise?
    a. Yes (please provide details)
       [Text box to complement response]
    b. No

Annex to questionnaire: Glossary

For general definition of terms used in the survey, please see the *Glossary in the guidance on cyber resilience for financial market infrastructures* and the *FSB cyber lexicon*. Terms not covered in these referenced compilations are described below.[24]

Communication protocol: procedure to inform the FMI's participants and, as appropriate, the public on the occurrence of an incident and when the FMI has resolved the incident.

External stakeholders: entities outside the FMI who are affected by its decisions, actions and performance (eg end users, customers).

External-facing systems: systems that allow or enable connections from outside the network (eg website, portals, emails, firewalls etc).

False positive: an error in the reported result that incorrectly indicates presence of a condition, incident or attribute that is actually not present.

Governance arrangements: decision-making processes and procedures to inform the management bodies and to apply their decisions.

Incident detection: process used to identify whether an incident has occurred.

Internal stakeholders: persons and entities within the FMI (eg employees, managers, the board of directors, investors).

Internal-facing systems: systems other than external-facing systems.

Penetration testing: a test methodology in which assessors, subject to specific constraints set by the targeted entity, attempt to circumvent the security features of an information system.

Phishing: a technique for attempting to acquire sensitive data or information through a solicitation by email, on a website or by some other electronic means, in which the perpetrator masquerades as a legitimate business or reputable person.

Recovery plans: procedure set up to restore all systems after any potential incident as defined from pre-identified emergency scenarios. They should aim at re-establishing integrity and availability of the operations, and the confidentiality of the information assets.

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

[24] These additional terms are for specific use in this survey only.

focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.

Resumption plans: procedure set up to restore business after any potential incident defined by pre-identified emergency scenarios. It is distinct from the business contingency plan that deals with running the business while an emergency is occurring.

Scenario-based testing or exercises: a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. In an exercise, personnel with roles and responsibilities in a particular IT plan meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that does not involve using the actual operational environment. Exercises are scenario-driven, eg a power failure in one of the organisation's data centres or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise.

Unfamiliar scenarios: novel, unknown or unconventional sequences of events.

Vulnerability assessments: 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.

Vulnerability scans: program that identifies vulnerabilities in a network, application, system, etc. An authenticated scan is performed by a logged-in user, while an unauthenticated scan is performed by an outside party.

Annex B – Members of the IMSG and Assessment Team

IMSG co-chairs

US Securities and Exchange Commission	Elizabeth L Fitzgerald (since December 2021) Christian Sabella (until Jun 2021)
European Central Bank	Fiona van Echelpoel (since Mar 2022)
Bank of France	Valérie Fasquelle (until Jul 2021)

IMSG and Assessment Team members

Reserve Bank of Australia	Matthew Gibson Konrad Szylar**
National Bank of Belgium**	Vincent Olécrano**
Bank of Canada	Nikil Chande (since Aug 2021) Wade McMahon (until Aug 2021) Steven Lavergne**
European Central Bank	Beata Wrobel (since Oct 2021) Tom Kokkola (until Oct 2021) Constantinos Christoforides**
European Securities and Markets Authority	Maud Timon
Bank of France	Katia Pascarella (since Aug 2021) Thomas Carre* (until Jul 2021) Marc Andries**# (until Oct 2021) Christophe Mace** (since Jul 2021)
Bundesanstalt für Finanzdienstleistungsaufsicht, Germany	Edip Acat (until May 2020) Stephan Moegelin** Johannes Reinschmidt**
Hong Kong Monetary Authority	Osbert Lam
Securities and Futures Commission, Hong Kong SAR**	Hokinson Ho**
Securities and Exchange Board of India	Sudeep Mishra (since Jan 2020) Sanjay Purao (until Dec 2019)
Bank of Italy	Alessio Abbate Enrico Silvaggi**
Bank of Japan	Takashi Hamano
Financial Services Agency, Japan	Megumi Ota (since Jan 2022) Fumikazu Nishio
Bank of Korea	Young Seok Kin (since Jan 2022) Hyung Koo Lee (until Dec 2021) Sungwoo Choo**
Netherlands Bank**	Raymond Kleijmeer** (until June 2022)
Central Bank of the Russian Federation***	Ekaterina Peregudova (until Feb 2022) Savva Morozov** (until Feb 2022)
Monetary Authority of Singapore (MAS)	Tze Hon Lau Edward Oei (since Nov 2021) Joey Ho (until Nov 2021) Tong Lee Lim**#
Sveriges Riksbank	Loredana Sinko

Capital Markets Board, Turkey	Nalan Sahin Urkan
Bank of England	James Pople Hoskins (until March 2022) Francesco Fici (since March 2022)
Board of Governors of the Federal Reserve System	Dibora Spiegler (since Oct 2021) Kathy Wang (until Oct 2021)
Federal Reserve Bank of Chicago**	Wei Zhang**
Federal Reserve Bank of New York	Emilie Walgenbach (since May 2021) John Rutigliano (until May 2021) Jenny McMahan**# (AT lead from Nov 2021) Seaira Christian-Daniels (until Feb 2021) Jack Janson**
US Commodity Futures Trading Commission	Andrea Musalem (from Feb 2021) Alicia Lewis (until Feb 2021)
US Securities and Exchange Commission	Stephanie Kim Park
World Bank**	Dorothee Delort** Fredesvinda Fatima Montes**
IOSCO Assessment Committee	Raluca Tircoci-Craciun
IOSCO Secretariat	Tajinder Singh Josafat De Luna Martínez
BIS CPMI Secretariat	Jenny Hancock Carlos Sosa (from Sep 2021) Umar Faruqui (until Jun 2021) Codruta Boar (until Feb 2021)

\# Assessment team lead.
* IMSG and Assessment Team member.
** Assessment Team member only.
*** The access of the Central Bank of the Russian Federation to all BIS services, meetings and other BIS activities has been suspended.

The IMSG would like to extend its thanks to Tong Lee Lim (MAS), Jenny McMahan (FRBNY) and Marc Andries (Bank of France), the team co-leads for this assessment, and the experts that made up the Assessment Team.