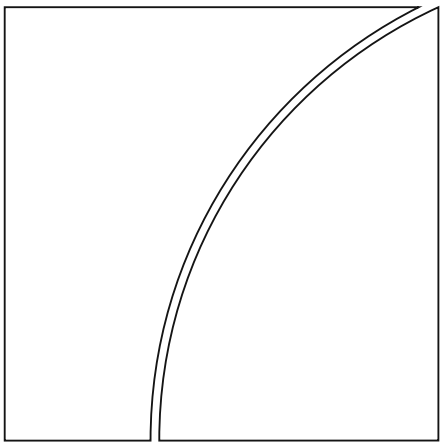
Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions



Implementation monitoring of PFMI: Level 3 assessment of FMIs' business continuity planning

July 2021

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 978-92-9259-473-2 (online)

Contents

Abbreviations

2hRTO	two-hour recovery time objective
BCP	business continuity plan
BIA	business impact analysis
CCP	central counterparty
CPMI	Committee on Payments and Market Infrastructures
CSD	central securities depository
CSP	critical service provider
FMI	financial market infrastructure
IMSG	Implementation Monitoring Standing Group
IOSCO	International Organization of Securities Commissions
IT	information technology
KC	Key Considerations
L1	Level 1
L2	Level 2
L3	Level 3
ORO	operational reliability objectives
PFMI	Principles for financial market infrastructures
PS	payment system
SLA	service-level agreement
SSS	securities settlement system
TR	trade repository

1. Executive summary

In April 2012, the 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 in the PFMI 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-assessments report 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 third L3 assessment of consistency in the outcomes of FMIs' implementation of the PFMI.[1] It focuses on business continuity planning and was carried out during 2019-20 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 recovery time objective and one issue of concern in the area of cyber risk. The IMSG has also noted some (other) observations.

1.1 Scope of the assessment

In this assessment, the IMSG has reviewed the business continuity planning practices at a sample of 38 FMIs from 29 jurisdictions. The sample comprised 14 PSs, 15 CSDs/SSSs, five CCPs and four TRs.

The FMIs participated voluntarily in the exercise, providing responses to a detailed survey and responding to follow-up questions from the IMSG. Since FMIs' operational risk management may involve sensitive information, survey responses were handled with due regard to confidentiality. The survey responses were anonymised by removing any identifiable information before being provided to the assessment team of experts nominated by CPMI and IOSCO member authorities. The IMSG would like to thank the participating FMIs – and their supervisors and overseers – for their cooperation during this exercise.

Importantly, L3 assessments are peer benchmarking exercises and not supervisory exercises. Accordingly, the report 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.

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

Furthermore, the findings in this report are based on the IMSG's review of the 38 FMIs alone and may not necessarily be representative of all FMIs.

1.2 Key findings of the assessment

The IMSG has identified one serious issue of concern and one issue of concern[2] which could be subject to future 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. Given that 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. However, the key findings of the exercise are summarised below.

1.2.1 Timely recovery in the event of a wide-scale or major disruption

The IMSG has identified one serious issue of concern, which is that the business continuity management of some, and potentially many, FMIs does not seem to "aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption", as expected by the Operational Risk Principle (Principle 17). Furthermore, based on the information provided by the participating FMIs, there are doubts about whether their business continuity plans are designed to "ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events" and "enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances" as expected by KC6. Given this is a serious area of concern, the CPMI and IOSCO expect the relevant FMIs and their supervisors to address this as a matter of the highest priority.

While almost all of the surveyed FMIs indicated that they have business continuity plans (BCPs) designed to meet this requirement, there is evidence that leads the IMSG to question this. In terms of specific evidence:

- A few of the surveyed FMIs do not explicitly aim for the 2hRTO, even for wide-scale physical (non-cyber) disruptions.
- One of the surveyed FMIs acknowledges that its secondary site does not have a distinct risk profile from that of its primary site.
- A small number of FMIs stated that they did not have alternative arrangements to allow for the processing of time-critical transactions. Of those that did have such arrangements, some relied solely on manual and paper-based alternative arrangements.
- A few FMIs indicated that they do not have specific plans to mitigate potential widespread staff unavailability. This suggests that these FMIs may have difficulty completing settlement if this were to occur.

Furthermore, since not all FMIs provided the same level of detail in response to the open-ended questions, there are gaps in the information provided by many of the FMIs, which leads the IMSG to question their ability to recover in a timely manner in the event of a wide-scale or major disruption affecting staff availability. In particular, there are gaps in information about certain FMIs' plans to recover in the event of a wide-scale or major disruption where:

[2] 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.

- The FMI's BCP relies on the availability of critical staff that support the primary site to operate the backup site, either remotely or after relocating to the backup site. This could mean that an event at the primary site may impede recovery at the backup site due to an insufficient number of staff members available to operate the backup site.
- The primary and backup sites are located within the same metropolitan area/region or within normal commuting range of each other. As a result, staff working at both sites could be affected by the same event, which may mean they are unavailable to facilitate recovery in a timely manner.

Many FMIs' responses suggested the presence of one or more of these possible impediments to timely recovery following a wide-scale or major disruption, but the information provided in the free text fields was not detailed enough to help understand whether or how their BCPs address this potentially serious issue of concern. Although it is possible that an FMI has mitigated the risk that the staff needed for the timely recovery and operation of the backup site are unavailable due to the same wide-scale or major disruption affecting the staff that support the primary site, significant gaps in the information provided by most FMIs lead the IMSG to question whether they have sufficiently mitigated this risk as expected by Principle 17.

1.2.2 Cyber risk

Principle 17 states that "[a]n 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…" The IMSG has identified one issue of concern, which is that a few FMIs in the sample did not provide specific BCP objectives with respect to cyber risk. Among the FMIs that have specific BCP objectives with respect to cyber risk, only a few explicitly acknowledged the breadth and depth of potential cyber attacks and the complexities of cyber risks that their BCPs may not be able to cover.

1.3 Covid-19 pandemic

In light of the Covid-19 pandemic, the IMSG has taken a closer look at the survey information on FMIs' plans to respond to a pandemic. The L3 business continuity planning survey contained one question specifically addressing contingency planning for pandemics (although responses were given prior to the onset of Covid-19). All FMIs indicated that their BCPs include a pandemic scenario (to address presumed pandemics prior to Covid-19), albeit some did not specify how they would react to such a scenario, and at least one noted that its plans for a pandemic scenario were not yet fully operational. Some FMIs' planned responses to a pandemic involved remote working, splitting staff between the primary and backup sites, or both.

For additional context, the IMSG has also prepared a high-level summary of FMIs' actual responses to Covid-19 in some IMSG member jurisdictions (including some of the FMIs surveyed for the L3 business continuity planning survey as well as other FMIs that were not part of that survey) based on information provided by IMSG authorities as of October 2020 (Box A). It is important to note that the information in Box A is not part of the assessment, but it has been included in the report to provide some additional context on this topic.

Box A

Businesss continuity measures in response to Covid-19

Based on high-level information provided by some authorities represented in the IMSG

In line with the PFMI, participating FMIs' BCPs had plans for responding to a pandemic scenario, including remote working and splitting staff between sites. However, the Covid-19 pandemic has been unprecedented in terms of both the breadth and the length of the required business continuity response. Therefore, it is possible that, in some cases, FMIs' responses to Covid-19 have gone beyond what was planned for in their BCPs.

While the information collected for the L3 business continuity planning assessment predates Covid-19, many FMI authorities have shared with the IMSG some high-level public information on general actions taken to address the business continuity challenges brought about by Covid-19. The summary below provides additional context for the themes presented in this report. Given that the assessment in the main body of the report was conducted prior to the start of the pandemic, this assessment does not take into account FMIs' actual Covid-19 responses in order to develop the findings and recommendations outlined in the report.

Overall, FMIs have not experienced service disruptions during the pandemic. In general, FMIs have reported that they activated their business continuity plans in order to maintain operations while minimising risks to staff in line with the measures taken by their respective governments or health authorities. FMIs have reported that they transitioned to a remote working environment (eg working from home) while maintaining operation of their critical functions. FMIs determined the minimum number of staff members necessary to conduct their critical functions and identified staff who can perform those functions. In most cases, the vast majority of staff have been working remotely, with only a few critical staff members remaining on-site. For the small number of staff members that remained on-site (for example, for hardware maintenance or to mitigate the risks arising out of remote work such as internet connectivity and latency issues), FMIs employed various safety measures such as social distancing practices and on-site/remote working rotational schedules. In other cases, FMIs operated completely remotely. FMIs have expanded their existing remote work capabilities to include more functions than initially planned for in their BCPs or to improve/strengthen existing functions. In some cases, this has included training staff to work in a fully remote working environment and the provision of additional IT support (including virtual private network (VPN) access) to staff working remotely. In other cases, this may also include taking a cautious approach in planning for a return-to-work scenario, in keeping with government/health authority guidance.

Although the Covid-19 pandemic did not cause service disruptions, it presented some operational challenges. For instance, some FMIs saw increases in the value and volume of the transactions they cleared and settled in March and April 2020 and were generally able to manage the operational challenges this presented. There were some cases in which operational challenges impacted clearing and settlement due to high levels of activity. Changes in the value or volume of transactions have not been homogeneous across FMI types during the pandemic. On the payments side, while some FMIs experienced peaks in transactions processed, others saw sharp and sudden decreases in transactions. For example, as the pandemic crisis deepened in April and May 2020, some payment systems settling wholesale transactions, as well as some settling foreign exchange transactions, experienced increased traffic due to the high volatility in financial markets, although the increased traffic did not give rise to capacity issues. In contrast, some retail payment systems processing card payments observed a considerable drop in transaction volumes as several business sectors came almost entirely to a halt (like the travel and aviation industries).

FMIs have observed that the Covid-19 pandemic has highlighted operational risks posed by third parties such as critical service providers. Overall, no major incidents involving third parties were reported during 2020. However, some issues with supply chains from third parties located in affected areas were noted in the first half of 2020. FMIs have assessed and updated their communications arrangements to ensure they can continue to effectively interact with internal and external stakeholders, including critical suppliers and participants, despite the move to remote working. In some cases, FMIs have conducted reviews of their third-party service providers. FMIs recognise that the threat landscape is evolving and are closely monitoring the trends and types of operational incidents, including those impacting critical service providers, as well as FMIs' ability to respond efficiently to severe incidents (eg default, disruption) either within their own operations or with a third party given ongoing remote working arrangements.

FMIs have also noted an increased threat of cyber risks, especially in remote working environments. In this context, FMIs are vigilant about cyber resilience controls of their remote devices. FMIs have also adopted enhanced cyber security monitoring, with extra vigilance regarding their internal VPN networks, and have trained their staff thoroughly on threats arising from remote access.

FMIs have maintained a dialogue with their relevant authorities in order to continue complying with regulatory requirements in the context of the pandemic. Some FMIs have prioritised business continuity and resilience testing exercises in order to obtain a sufficient level of assurance following the first wave of the pandemic. Other FMIs were able to conduct disaster recovery tests in 2020.

FMIs continue to be proactive in managing operational risks and have tightened existing controls, with some FMIs implementing additional controls targeting identified risk exposures, putting in place increased monitoring/reporting arrangements, and lowering incident escalation thresholds.

2. Introduction

2.1 Objective of the L3 assessment

The IMSG monitors the implementation of the PFMI.[3] This work is structured according to a monitoring framework that involves three phases:

(1) 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.

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

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

Assessing the consistency in outcomes (L3) involves a detailed consideration of how consistent each participating financial market infrastructure's implementation outcomes are with the Principles and an analysis of the range of implementation outcomes observed across FMIs. 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.
- Comparison of implementation outcomes across FMIs, with attention, where possible, to the drivers, degree and implications of observed variations.

Importantly, L3 reviews are peer benchmarking exercises and not supervisory exercises. Accordingly, these reviews focus on the consistency in outcomes of implementation of relevant Principles and 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.

2.2 Scope of this review

This assessment is the third L3 assessment carried out by the CPMI and IOSCO. The previous L3 assessments reviewed selected CCPs' financial risk management and recovery practices. The first reviewed practices at a sample of 10 derivatives CCPs.[4] The second reviewed the progress made by a broader set of CCPs in areas where the first assessment identified serious issues of concern.[5]

This Level 3 assessment focuses on Principle 17 (Operational risk), Key Considerations (KCs) 3, 6 and 7 (Table 1).

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

[4] Available at https://www.bis.org/cpmi/publ/d148.pdf and https://www.iosco.org/library/pubdocs/pdf/IOSCOPD538.pdf.

[5] Available at https://www.bis.org/cpmi/publ/d177.pdf and https://www.iosco.org/library/pubdocs/pdf/OSCOPD601.pdf.

KCs reviewed by this L3 assessment* Table 1

Principle (KC)	Topic	Text
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.*
17(3)	Operational reliability objectives	An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.
17(6)	Business continuity management	An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale 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.
17(7)	Interdependencies	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.**

* The IMSG also considered the Explanatory Notes in the PFMI, which provide guidance on one way of implementing the standards in the Principles and Key Considerations. ** No evidence was collected on the second point in the KC.

3. Process and methodology

This L3 assessment proceeded in three main stages over the course of [24] 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). Data collection and analysis was largely completed by late 2019, but work was paused in early 2020 in light of the Covid-19 pandemic, resuming in late 2020. Since FMIs' operational risk management may involve sensitive information, the data were anonymised with only a limited number of BIS 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

This L3 assessment covers all types of FMIs. FMIs from all of the 28 jurisdictions that are participating in the IMSG implementation monitoring programme were invited to participate in this L3. Participating FMIs were selected based on a number of criteria. These include:

- Balancing jurisdictional and FMI coverage on the one hand, and complexity and volume of work for the IMSG on the other hand.
- A large enough sample such that anonymisation is practical.
- Less weighting towards CCPs, as they have been the (sole) focus of previous L3 assessments.
- Covering both private and central bank-operated payment systems.
- Covering both small and large entities within each FMI category.
- Differences in the underlying population of the FMI candidates, eg there are relatively fewer TRs to draw from than PSs or CCPs.

Based on this, 38 FMIs from 29 jurisdictions[6] were selected to participate in this assessment. FMIs' participation in this exercise was voluntary.

3.2 Data collection and analysis

3.2.1 Data collection

The IMSG launched the L3 business continuity planning assessment on 12 June 2019 by sending the online survey questionnaire to participating FMIs. The survey included both open-ended and closed-form questions (Annex A). The survey was based on the questions in the PFMI Assessment Methodology,[7] but with more detailed and granular questions where necessary. Policy, procedural or methodological documents were not requested. It should be emphasised that the evidence base for this exercise was necessarily non-exhaustive.

3.2.2 Confidentiality and anonymity

Since FMIs' operational risk management may involve sensitive information, survey responses were handled with due regard to confidentiality. The survey responses were anonymised by removing any identifiable information before being provided to the assessment team of experts nominated by CPMI and IOSCO member authorities.[8] In this vein, it was agreed that a limited number of BIS staff members (previously identified by the CPMI and IOSCO secretariats) would anonymise the FMIs by assigning them a randomly generated alias. 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 secretariats made anonymised responses available to the assessment team for analysis. The IMSG was able to send follow-up questions to the responding FMIs through the relevant BIS staff. As needed, analysis of the FMIs' survey responses was combined with follow-up questions.

3.2.3 Format of the report

As stated above, this L3 assessment is a peer benchmarking exercise and not a supervisory exercise. Accordingly, the analysis is focused on the consistency in the outcomes of implementation of relevant KCs across the group of participating FMIs as a whole. As a result, this L3 review does not include formal ratings of observance.

The work proceeded in two stages:

- In the first stage, the IMSG focused on compiling the information based on each FMI's survey responses and reviewing how consistent each FMI's implementation outcomes were with the Principle and KCs.
- In the second stage, the IMSG reviewed the consistency of implementation outcomes across all selected FMIs in order to identify, by topic, areas in which differences in implementation could lead to material differences in specific aspects of FMIs' frameworks for managing operational risk and in their resilience.

[6] This includes the 28 jurisdictions that are participating in the IMSG implementation monitoring programme, plus one other jurisdiction which typically does not participate in implementation monitoring exercises.

[7] CPMI-IOSCO, *PFMI – Disclosure framework and Assessment methodology*, December 2012, available at www.bis.org/cpmi/publ/d106.pdf and www.iosco.org/library/pubdocs/pdf/IOSCOPD396.pdf.

[8] The experts supported the assessment by IMSG members (Annex B).

4. Analysis of results

This section presents the IMSG's review for each of the three KCs (3, 6 and 7) under Principle 17 (operational risk) that were analysed as part of this assessment exercise. As noted earlier, in considering these FMIs' implementation of the PFMI, the IMSG has not conducted a supervisory review or examination. Accordingly, this section focuses on the consistency in the outcomes of implementation of relevant 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". 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.

The remainder of the section is organised as follows. The first subsection on key findings summarises the serious issues of concern, issues of concern, observations and other observations. Subsequent subsections highlight the analysis for each of the three KCs reviewed. While the IMSG also analysed trends by FMI type, no significant differences were identified across FMI types. However, it should be noted that the FMI sample was not specifically designed to identify possible divergences across FMI types. Where appropriate, notable differences by FMI type are identified in the KC analysis.

4.1 Key findings

The IMSG has identified one serious issue of concern and one issue of concern, plus several observations, which are detailed in Sections 4.1.1 to 4.1.4 below. Beyond these issues, FMIs' responses suggest they believe that their practices are consistent in many aspects with the expectations regarding business continuity planning laid out in Principle 17 of the PFMI. All of the surveyed FMIs noted that they have operational reliability objectives (OROs), most of which focus on system availability and recovery time. Based on the information received, the IMSG considers FMIs' arrangements to be generally more developed with regard to managing "traditional" sources of operational risk (eg natural disasters) than cyber risks. All of the FMIs review their BCPs at least annually and test them regularly. Finally, FMIs generally state that they have identified the operational risks posed by key participants. However, responses to some of the more detailed questions suggest that there could be some gaps and inconsistencies in their practices.[9]

4.1.1 Serious issues of concern

Timely recovery in the event of a wide-scale or major disruption

The IMSG has identified one serious issue of concern, which is that the business continuity management of some, and potentially many, FMIs does not seem to "aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption" as expected by Principle 17. Furthermore, based on the information provided by participating FMIs, there are doubts about whether

[9] Given the nature of this assessment, the IMSG did not review the underlying policies and procedures designed to achieve those objectives.

their business continuity plans are designed to "ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events" and "enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances" as expected by KC6. Given this is a serious area of concern, the CPMI and IOSCO expect the relevant FMIs and their supervisors to address this as a matter of the highest priority.

While almost all of the surveyed FMIs indicated that they have BCPs designed to meet this requirement, there is evidence that leads the IMSG to question this. In terms of specific evidence:

- A few of the surveyed FMIs do not explicitly aim for the 2hRTO, even for wide-scale physical (non-cyber) disruptions. Instead they either have a three- or four-hour RTO, although at least one has plans to reduce its to two hours.
- At least one of the surveyed FMIs acknowledges that its secondary site does not have a distinct risk profile from that of its primary site. The FMI does have plans to move the secondary site to a location that has a distinct risk profile. However, in the meantime, it is difficult to see how this FMI can meet the two-hour recovery time objective (2hRTO) if an event affects both sites.
- A small number of FMIs stated that they did not have alternative arrangements to allow for the processing of time-critical transactions. Of those that did have such arrangements, some relied solely on manual, paper-based alternative arrangements.
- A few FMIs indicated that they do not have specific plans to mitigate potential widespread staff unavailability. This suggests that these FMIs may have difficulty completing settlement if this were to occur.

Furthermore, since not all FMIs provided the same level of detail in response to the open-ended questions, there are gaps in the information provided by many of the FMIs, which leads the IMSG to question their ability to recover in a timely manner in the event of a wide-scale or major disruption affecting staff availability. In particular, there are gaps in information about certain FMIs' plans to recover in the event of a wide-scale or major disruption where:

- The FMI's BCP relies on the availability and ability of critical staff that support the primary site to operate the backup site, either remotely or after relocating to the backup site. This could mean that an event at the primary site may impede recovery at the backup site due to an insufficient number of staff members available to operate the backup site.
- The primary and backup sites are located within the same metropolitan area/region or within normal commuting range of each other. As a result, staff working at both sites could be affected by the same event, which may mean they are unavailable to facilitate recovery in a timely manner.

Many FMIs' responses suggested the presence of one or more of these possible impediments to timely recovery following a wide-scale or major disruption, but the information provided in the free text fields was not detailed enough to help understand whether or how their BCPs address this potentially serious issue of concern. Although it is possible that an FMI has mitigated the risk that the staff needed for the timely recovery and operation of the backup site are unavailable due to the same wide-scale or major disruption affecting the staff that support the primary site, significant gaps in the information provided by most FMIs lead the IMSG to question whether they have sufficiently mitigated this risk as expected by Principle 17.

4.1.2 Issues of concern

Cyber risk

Principle 17 states that "[a]n 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…" The IMSG has identified one issue of concern, which is that a few FMIs did not provide specific BCP objectives with respect to cyber risk. This suggests that BCPs for cyber risk are works in progress.

Among the FMIs that have specific BCP objectives with respect to cyber risk, only a few explicitly acknowledged the breadth and depth of potential cyber attacks and the complexities of cyber risks that their BCPs may not be able to cover.

4.1.3 Observations

The IMSG identified a number of different implementation outcomes that could give rise to material differences in resilience across FMIs (ie they meet the criteria for "observations"). Specifically:

- *Board review of OROs:* In responding to the question on stakeholder review of OROs, some FMIs did not explicitly mention board review, despite the board being one of the examples of stakeholders given in response to the respective question. Paragraph 3.17.9 in the Explanatory Notes suggests that OROs should be reported regularly to (among others) relevant board committees. This could give rise to material differences in resilience across FMIs, although there is some evidence an alternative approach of boards reviewing IT services as a whole. More generally, the surveyed FMIs reported a variety of processes for governance and review of OROs.
- *Service-level agreement(s):* According to KC7, "[a]n FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations". It is difficult to identify how the FMIs whose responses indicate that they do not use service-level agreements (SLAs) or other contractual arrangements to manage their dependencies on critical service providers (CSPs) comply with this KC.
- *BCP testing:* The types and methods of BCP testing are highly diverse. For example, in order to monitor and manage the operational risk that CSPs can pose to an FMI, most FMIs using CSPs have involved them in BCP tests. However, there is scant evidence of industry-wide tests.

4.1.4 Other observations

The survey results show that the assessed FMIs adopt a variety of practices to implement KCs 3, 6 and 7. The IMSG found that such diverse practices do not have materially negative implications for resilience, and in fact some are likely to have a positive impact (ie they meet the criteria for "other observations"). These were:

- *The 2hRTO as an ORO*. While almost all of the FMIs stated that they meet the 2hRTO for a non-cyber wide-scale or major disruption, most FMIs have adopted a recovery time objective as an ORO (a few of them without explicitly referencing a two-hour maximum RTO).[10]
- *Third sites*. A small number of FMIs have established third sites, exceeding the minimum expectation in Principle 17.
- *Cross-system interdependencies*. The formality of the coordination between linked FMIs or cross-border systems varies. A significant majority of the FMIs indicated that they have cross-system interdependencies or that cross-border connections and communications arrangements are in place with the relevant parties at interlinked FMIs.
- *Outsourcing*. A few FMIs declared that they do not outsource any of their services. While this minimises external dependencies, it is unusual for an FMI to be able to eliminate such dependencies completely.

The various types of operational interdependencies that an FMI needs to manage were also interpreted differently. For example, at least one FMI responded that all participants are key participants, while at least one other FMI's answers suggest that it does not consider any of its participants to be key participants. In contrast, KC 7 implies that at least some participants will be key when it states that "[a]n FMI should identify, monitor, and manage the risks that key participants…" Some FMIs classified

[10] This suggests that at some FMIs there may be a distinction between OROs and business continuity planning.

custodians, exchanges/trading platforms, financial messaging providers, depositories or cash correspondents as "other FMIs". There were also varied responses regarding what constituted a CSP; for example, some FMIs that outsource provision of data services did not see these providers as CSPs. In addition, only a few FMIs identified water suppliers as critical utility providers and there was a difference in understanding of why water supply was critical.

The IMSG notes that the FMIs' responses indicate that the varying practices shown above may stem from different interpretations of terminology. For instance, FMIs have different ways of establishing BCPs because of their different understandings of terms used in the Principle, KCs and survey questionnaire such as "stakeholders", "second site", "material change", "test and review" of BCP arrangements, "key participants", "critical service providers" and "data-sharing agreements".

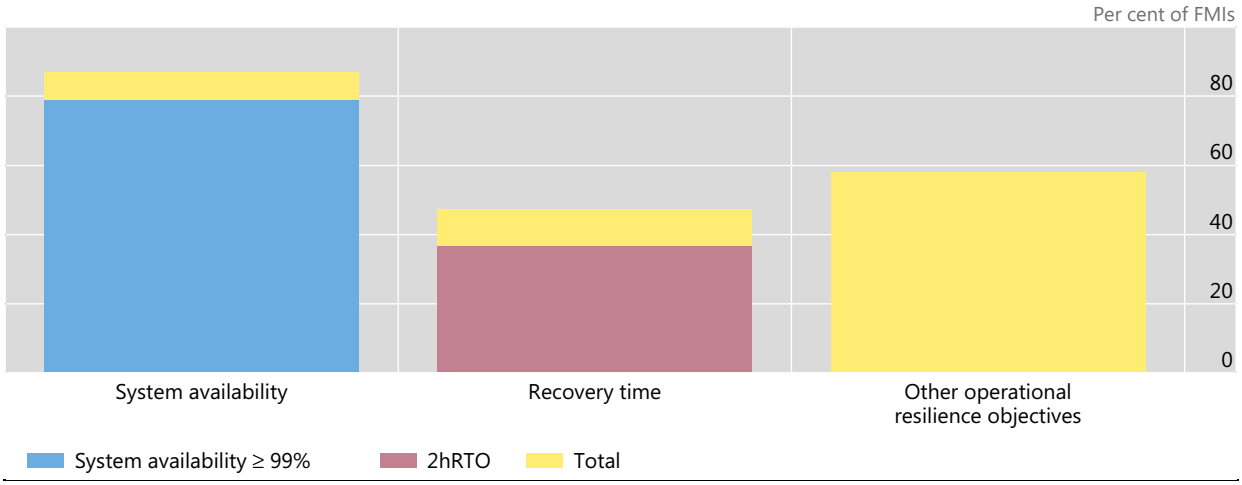
4.2 Key Consideration 3: Operational reliability objectives

Key Consideration 3 of Principle 17 provides that FMIs should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.

4.2.1 Operational reliability objectives

All of the surveyed FMIs identified OROs. Almost all of them have quantitative OROs, but a small number also have qualitative OROs. Almost all of the FMIs identified system availability as an ORO. Of these, a significant majority targeted availability of at least 99% of operating hours, while the rest of this subset of FMIs did not mention a specific target in their responses. Most FMIs identified recovery time as an ORO, with some identifying both system availability and 2hRTO as OROs. Some FMIs explicitly recognised the 2hRTO in their OROs. Most FMIs identified additional OROs, with specific objectives varying depending on the type and features of the FMI (Graph 1).

Operational resilience objectives — Graph 1



All FMIs regularly review their OROs at least annually. A small number of FMIs review their OROs quarterly and some responded that they do so monthly. A small number of FMIs stated that additional reviews can take place whenever a significant issue or material change occurs.

4.2.2 OROs monitoring process

Assessed FMIs indicate they have established policies, procedures and mechanisms designed to achieve their operational objectives. Survey responses refer to different aspects of their policies for meeting OROs, focusing on monitoring, business continuity planning and testing. FMIs' responses emphasised preventive measures to reduce the possibility of risk materialisation, as well as post-event risk mitigation and recovery.

Policies and procedures put in place to meet OROs tend to include a BCP, incident management, information security, cyber security and a detailed operation manual for each business segment. When describing their operational risk policies, some FMIs mentioned international, national, and industry-level standards, such as ISO 20000 Operation and Maintenance Service Management System, ISO 27001 Information Security Management System, national information security protection requirements and change management policy. This is consistent with the Explanatory Note in 3.17.5, which states that "an FMI should seek to comply with relevant commercial standards in a manner commensurate with the FMI's importance and level of interconnectedness".

Most of the FMIs referred to on-going monitoring and control mechanisms that allow for compliance with OROs and ensure that issues are detected in a timely manner. Some FMIs described using automated tools that check the operation of components at short intervals and automatically generate alerts to relevant staff members if any issues are detected in order to prevent system failures. For example, a few FMIs monitor deviations from previously agreed-upon service levels and key performance indicator thresholds and then prompt escalation, including effective escalation paths to address critical shortfalls.

The responses of a small number of FMIs suggested that their policies on OROs also focus on post-event mitigation and recovery. Crisis management procedures warrant timely and responsive actions to meet OROs and ensure the continuity of FMIs' critical processes. At least one FMI indicated that it conducts business continuity management awareness training on an annual basis.

To help ensure that business continuity arrangements, including contingency procedures, are up to date and effective, some FMIs explicitly stated in their responses that they perform regular reviews and testing. The testing covers various contingency scenarios relating to component failure at a site; total system failure at the active site with failover to the alternate site; remote access to a site's systems; external infrastructure outages; and a total site outage (staff and systems). While some FMIs may not specifically review and test OROs, all FMIs indicated that they perform various reviews and testing of their BCP at least annually (4.3.6).

Almost all of the FMIs stated that they involve stakeholders in ORO reviews. However, some did not mention their board as a stakeholder, despite the suggestion in paragraph 3.17.9 of the Explanatory Note that the system's performance relative to its established objectives and service-level targets should be reported regularly to (among others) relevant board committees. Some FMIs indicated that senior management are involved in ORO reviews. A small number of FMIs indicated that they only report the results to internal committees such as the Risk Committee, Technology Committee and Security Committee, with the board reviewing IT services as a whole. There are also situations in which the board, or another governance body internal to the FMI, specifically reviews OROs separately from an overall review of IT services. A few FMIs refer to external parties such as third-party participants and regulators as stakeholders.

The scope of these reviews is not always clear. Some FMIs made explicit reference to the fact that the objective is to assess the appropriate incorporation of new technological and business developments into OROs.

4.2.3 Incident management procedure

All of the surveyed FMIs have in place incident management procedures to ensure that incidents are met with a coordinated and prompt response, roles and responsibilities are clear, and communication is appropriate. According to the FMIs' responses, incident management procedures cover incident detection and recording, classification and initial support, investigation and root cause analysis, resolution, closure, ownership, monitoring, tracking and communication, and post-incident review.

The responses of at least one of the FMIs indicated they have set up comprehensive incident management processes. These FMIs stated that, if needed, they would make investments to improve procedures and infrastructure performance (enhancement) based on regular review and incident/root

cause analysis review. A few FMIs referred to training in the context of an incident review in order to enhance the skills and capabilities of the staff involved if the incident is caused by human error.

4.3 Key Consideration 6: Business continuity management

Key Consideration 6 of Principle 17 provides that FMIs should have a BCP that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical 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.

4.3.1 Business continuity plan

Regarding non-cyber-related disruptions, all of the surveyed FMIs indicated that they have a BCP designed to address events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The surveyed FMIs indicated that they review and test their BCPs at least annually. When discussing their BCPs, almost all of the surveyed FMIs mentioned that they meet the PFMI requirement of having a 2hRTO for the rapid recovery and timely resumption of critical operations following a non-cyber wide-scale or major disruption.

BCPs regarding cyber-related disruptions appear less developed than those for traditional operational risks. Almost all of the FMIs surveyed indicated that their BCPs address cyber risk. At least one FMI stated that it has a stand-alone cyber risk framework independent of its BCP. The extent to which cyber risk is addressed by the BCPs varies. For example, a few FMIs are in the process of updating their BCPs to include cyber risks, and at least one FMI is in the process of updating parts of its BCP regarding cyber risks as a result of its ISO 27001 assessments. A few of the FMIs addressed cyber risk more generally by referring to their day-to-day IT operations, data centres and backup routines, but did not specifically include or distinguish cyber risk objectives within their BCPs. Only a few FMIs explicitly acknowledged the breadth and depth of potential cyber attacks and the complexities of cyber risks that their BCPs may not be able to cover.

4.3.2 Secondary site

All of the surveyed FMIs stated that they have a secondary site, which can take over and resume operations following a disruption. A small number of FMIs stated that they have three data centres, and one FMI indicated that it has four data centres.

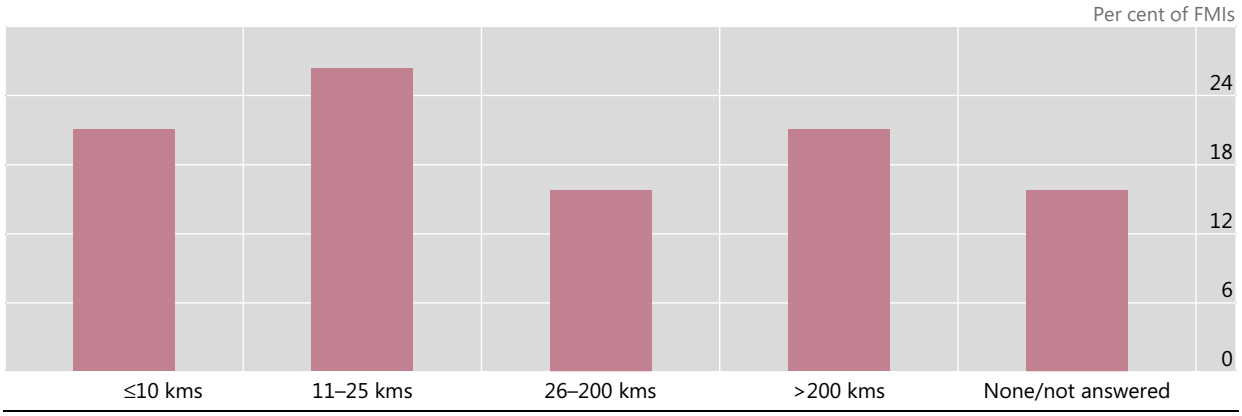
Although all FMIs stated that they have a secondary site, they identified secondary sites using various terminologies, including, without limitation, "data centres", "environment", "split-site model", "backup facilities", "offsite backup data centres", "contingency data centres", "standalone tertiary solution" and "enhanced dual sites". Because the majority of the FMIs did not explain their terms, there is a lack of clarity regarding the resources, capabilities, functionalities, and staffing arrangements of secondary sites compared with those of primary sites.

Many FMIs' responses suggested the presence of one or more possible risks to timely recovery via a secondary site following a wide-scale or major disruption, but the information provided in the free text fields was not detailed enough to help understand whether or how their BCPs mitigate these risks. Nevertheless, only one FMI acknowledges that its secondary site does not have a distinct risk profile. However, this FMI plans to move its secondary site to a location with a distinct risk profile, thus solving this issue.

When deciding on the location of their secondary sites, the FMIs considered the following factors in order to distinguish the new sites from their primary sites:

- *Distance:* There was a wide range of distances between primary and secondary sites, ranging between 300 metres to over 500 kilometres (Graph 2). For most of the FMIs, the distance between their primary and secondary sites is less than or equal to 25 kilometres. At least one FMI explained that a short distance between the sites allows staff to travel between them within two hours to meet the 2hRTO. However, reliance on staff movement between sites suggests that the sites may not have a distinct risk profile due to co-dependency on staff availability. While the PFMI do not specify a minimum distance, the distances reported by some FMIs call into question whether geographical diversity has been adequately considered. In some cases, the information available suggests that staff working at both sites may live in the same metropolitan area/region and could therefore be impacted by the same wide-scale or major event, but there was not enough information in the FMIs' responses for the IMSG to understand how this risk is mitigated. Overall, this raises a potential serious issue of concern about FMIs' ability to recover within two hours or settle by the end of the day in the event of a wide-scale or major disruption that affects the staff that support the primary site.

Distance between primary and secondary sites — Graph 2



- *Transportation disruption:* In almost all cases, the FMIs chose their secondary sites with multiple modes of transportation in mind. A small number of FMIs explicitly mentioned capacity for remote work as a means of mitigating a transportation disruption. Only a few FMIs explicitly stated that the secondary site is located at enough of a geographical distance from the primary site such that a disruption of regional transportation networks to the primary site would not also affect the secondary site.
- *Weather and natural disasters:* Almost all of the FMIs stated that their secondary sites are located in areas with limited risk of natural disasters. A small number of the FMIs stated that a geographical distance from the primary site explains why the secondary site would not be affected by the weather and natural disasters that may affect the primary site.
- *Telecommunications connectivity disruption:* Almost all of the FMIs indicated that they employ duplicative and separate lines and different telecommunications providers for their secondary site from the ones used by their primary site. Again, the FMIs cited a geographical distance from the primary site as an explanation of how a telecommunications connectivity disruption to the primary site would not affect the secondary site.
- *Power supply disruption:* Almost all of the FMIs stated that they have adopted various measures to mitigate this risk. The FMIs cited geographical distance from the primary site, as well as having a redundant power supply: a diesel secondary power generator: or an uninterruptible power supply (UPS), as countermeasures.
- *Act of terrorism:* Almost all of the FMIs stated that this risk is addressed by allowing staff to work remotely, distance from the primary site, and neutral characteristics that do not attract attention.

At least one FMI described a detailed and itemised plan for addressing various scenarios such as bomb threats and suspicious packages.

- *Water supply disruption:* A significant majority of the FMIs considered this risk and stated that the geographical distance between primary and secondary sites ensures different water sources for each site. However, there was a divergence in understanding of water usage: for fire protection, as a drinking source, or no use.

4.3.3 Two-hour RTO

Almost all of the surveyed FMIs indicated that they have BCPs designed to enable critical IT systems to resume operations within two hours. A few FMIs have either a three- or four-hour RTO and have no plans to move towards a 2hRTO. At least one FMI currently has a three-hour RTO and plans to reduce this to two hours.

A significant majority of the FMIs mentioned that they perform a business impact analysis (BIA) to identify the resources, capabilities, functionalities, and appropriate staffing arrangements that would be needed to resume critical operations within two hours and to complete settlement by the end of the day of the disruption. They also indicated that the output of the BIA is then validated and integrated into the BCP. According to these FMIs, the BIA is generally reviewed annually.

In order to meet their respective RTOs, all of the surveyed FMIs indicated that they have designed processes for failover to their secondary sites following a major disruption. Since all of the FMIs cited their secondary sites as a primary method of resuming operations, they also stated that the risks[11] that are considered and mitigated in establishing these sites (ie a transportation disruption, weather and natural disasters, a telecommunications connectivity disruption, a power supply disruption, an act of terrorism, a water supply disruption) are also considered mitigated in achieving their RTOs.

Non-cyber events

Software failure: All of the surveyed FMIs noted that they consider the risk of software failure and take a number of measures to mitigate this risk. In most cases, however, FMIs depended on having a secondary site with similar arrangements or backup measures in order to mitigate this risk. Such measures include the presence of software developers on-site, arrangements with external vendors and experts, access to software source codes, or alternative or different software applications at the secondary site. A small number of FMIs described that they maintain different software arrangements by using alternative software or previous versions of the same software at their secondary sites in order to achieve the 2hRTO. A few FMIs noted that they have different hardware at the secondary sites. A few also stated that they have alternative tools for manually recovering critical processes, although it was noted that this capability was limited depending on the volume of transactions or type of processes that were impacted.

Staff unavailability: As indicated previously, gaps in information provided by many FMIs lead the IMSG to question their ability to recover in a timely manner in the event of a wide-scale or major disruption that affects staff availability. Nevertheless, almost all of the surveyed FMIs indicated that they have plans to mitigate potential staff unavailability in a number of important scenarios. Some of the FMIs have split staff arrangements and service-level agreements with vendors which allow for there to be enough critical staff members present at each of the primary and secondary sites to continue operations if the staff at one site is unavailable. Some FMIs indicated that they have established capabilities for critical staff members to connect to both the primary and secondary sites remotely. A few FMIs divide their staff into multiple pools to ensure that the secondary site has 24/7 on-site staff presence. At least one of the FMIs also focuses on training and maintaining high-quality documentation, such as detailed checklists, to facilitate the recovery of critical processes.

[11] See Section 4.3.2.

To some extent, FMIs' plans for staff unavailability vary depending on the cause, although only a few of the surveyed FMIs provided customised responses to the questions about unavailability due to a pandemic compared with other events such as industrial action. In describing their planned response to a pandemic, some FMIs mentioned either working remotely or splitting staff between sites, and others mentioned plans involving both. A few of the FMIs stated that they have mitigation strategies for managing the risk of staff unavailability due to events such as industrial action (ie staff members are unwilling to work) using a combination of junior, managerial, and external support to ensure the maintenance and continuity of critical systems and processes.

Cyber Events

Cyber incident response: Although almost all of the surveyed FMIs indicated that their BCPs address cyber risk, a significant majority indicated that they have incorporated either a cyber incident response plan or a list of steps to take during a cyber event. A small number of FMIs indicated that their first action is to isolate the affected components and activate responsible management teams or governance committees. At least one FMI stated that their BCP does not include cyber event plans but they are planning to include them in the future, and a few FMIs responded affirmatively to the survey questions around cyber incident response planning but did not provide specific cyber-related actions.

Data copy and restoration: Almost all of the FMIs indicated that their BCPs include procedures for re-establishing the integrity and availability of data and operations. Some of those that answered positively look for a valid point in time from which data will be reconstructed (eg using incremental backups and/or reconciliations with FMI participants).

All of the FMIs confirmed that their BCPs include procedures for addressing data loss related to a cyber event, including the use of data backups or copies and re-submitted trade data. Almost all of the FMIs responded that they kept a copy of received data as a part of their BCPs. A significant majority of the FMIs indicated that they have synchronous data replication between their primary and secondary sites.

Transaction replay: A significant majority of the FMIs indicated that their BCPs include a transaction replay capability. Among those with this capability, a couple FMIs indicated that the transaction replay capability requires manual intervention and at least one FMI indicated that they rely on members to resubmit instructions along with transaction replay capabilities.

Data-sharing agreement: Although most of the FMIs confirmed that their BCPs include data sharing agreements with third parties, the responses to the survey question regarding these agreements were highly varied. For example, while some FMIs understood that data-sharing agreements are between FMIs and their respective service providers, other FMIs understood them to be between FMIs and their respective data submitters/participants. In addition, while some FMIs saw data-sharing agreements as written agreements, other FMIs believed standard industry practices qualified as data-sharing agreements.

Independent reconciliation: A significant majority of the FMIs indicated that they have procedures for producing data in order to allow participants to reconcile their positions in the event of an extreme but plausible cyber disruption. Of the FMIs that responded that they do not have reconciliation procedures, at least one is conducting an evaluation of their reconciliation of participant positions, while a few FMIs believe that reconciliation is unnecessary due to the nature of their businesses.

Status of transactions: Almost all of the FMIs confirmed the ability to identify the status of transactions. Of those that did not respond in the affirmative, at least one FMI reconciles liquidated transactions, but not those transactions pending settlement; while at least one other FMI noted that it has improvement plans ongoing.

Technically different systems: Some FMIs noted that they do not have the ability to replicate critical operations in a system that is technically different from the primary system in order to complete settlement in a non-standardised way during a cyber event. At least one FMI stated that it is planning to develop this element. A small number of FMIs indicated that they rely on alternative options, tools, or backup procedures and arrangements in order to complete settlement in a non-standardised way.

Recovery point objectives (RPO) to support data integrity: Almost all of the FMIs noted that their BCPs include RPOs that are consistent with the 2hRTO for critical operations. Some of these FMIs noted that the RPO is 2 minutes or less due to data replication capabilities that are in place. However, a few FMIs addressed concerns regarding their ability to meet both RPO and RTO targets depending on the severity and nature of the cyber event (eg time and capacity to identify and address compromised systems). Specifically, at least one FMI noted that, although recovery points are understood, it is not feasible to complete comprehensive reconciliation processes within a two-hour window and answered that the RTO may be challenged depending on the scale of the attack.

4.3.4 Crisis management

Crisis management procedures: All FMIs responded that their crisis management procedures address the need for a multi-skilled crisis and event management team that can be rapidly deployed. Crisis management procedures include decision points on the activation of the plan, escalation paths, critical staff designations, roles and responsibilities of staff and senior management, internal communications, and external communications with participants and relevant stakeholders. The responses suggested that typical crisis management teams include subject matter representatives from business operational areas, risk control, legal, IT experts and senior management.

All of the FMIs indicated that they have some escalation procedures and have defined thresholds for their crisis management activation. However, some FMIs' responses suggested that paths of escalation are not clearly outlined and defined. For example, only a few FMIs responded that their plans identify incident thresholds or have predefined priority or impact levels at which they deploy crisis management actions, while at least one FMI indicated that the same crisis management procedure is used for incidents large and small alike. At least one other FMI stated that its crisis management plan can be recommended for activation by any member of its staff.

Cross-system crisis management: Most of the FMIs indicated that they have cross-system interdependencies or cross-border connections and communications arrangements with the relevant parties at interlinked FMIs. The responses suggest that the formality of the coordination network for cross-FMI or cross-border systems varies: at least one FMI has formal coordination across interdependent FMIs at the domestic level; a few FMIs stated that they conduct communications coordination efforts as required by their regulators; and at least one FMI stated that it has exercised key elements of international cooperation at a strategic level despite a lack of formal arrangements.

4.3.5 Alternative arrangements

The survey responses show that a significant majority of the FMIs have alternative arrangements in their BCPs to allow for the processing of time-critical transactions in extreme circumstances. Of those that do not, a few plan to develop a system or manual processing procedure in the near future. In order to obtain accurate data while using alternative arrangements, most of the FMIs stated that they have procedures for validating data either via reconciliation with participants or by using internal tools, while others did not provide information on this issue. Most of the FMIs have considered cyber-related failures in their alternative arrangements; others did not provide information about this. At least one FMI considered the 2hRTO in its alternative arrangements.

Among the FMIs that have alternative arrangements, only a few plan to use them for all transactions, while the rest plan to apply such arrangements only for their time-critical transactions, such as high value fund settlement, settlements from other FMIs, margin calls, treasury operations, and new issue operations. The methods used to identify time-critical transactions range from determination by participants, determination by seasoned managers, business impact analysis and lessons learned from past incidents.

Technically different arrangements: Most FMIs indicated that they have technically different alternative arrangements. These ranged from PC-based solutions to batch processing to alternative systems. Some examples include:

- A system for all transactions of receiving transactions from participants via DVD, processing them in batches, settling them once per day, and distributing the results back to participants via DVD.
- A process in which the system reverts to net deferred settlement of interbank obligations in the next day's settlement batch.
- A fallback arrangement which involves multilateral netting and settlement of transactions.
- Procedures for the use of another system as a contingency in the FMI's operational business continuity plans.
- Working with paying agents to arrange for alternate methods of payment (wire instead of cheque) in extreme incidents.
- Alternative communication links for when a participant fails to submit their transactions.
- Alternative access channels for when participants cannot submit their transactions.
- Alternative arrangements for processing all transactions using semi-automated tools.
- Tools with the necessary contingency functions for settlement and systems linked to the central bank and the CSD.

4.3.6 Review and testing

Review: All FMIs review their BCPs at least annually and when there is a triggering event. The most common triggering event for reviewing a BCP is the identification of weaknesses in tests, exercises or drills. A few FMIs use the review process to identify the need for new or updated BCPs using other companies' scenarios and cases, to identify new risks to be added to existing BCPs, or to determine if training and the exercise of existing BCPs are enough.

Testing: The FMIs' responses indicate that FMI types, functionalities, interconnectedness and dependencies significantly affect the type, size and complexity of the tests conducted for their BCPs. Therefore, there is a high amount of variability across FMIs. A significant majority of FMIs noted that they conduct full switchover tests. Participants, third parties and linked FMIs are included in these switchover tests, which are usually performed at least annually. Out of these FMIs, a few stated that they also perform live operations from their secondary sites up to four times a year. Some FMIs noted that they have comprehensive testing programmes relating to the workplace, disaster sites, remote access, data recovery and reconciliation, tabletop and walkthrough exercises, crisis management, and cyber issues, most of which are conducted at least semiannually or annually. A few FMIs stated they have testing programmes for their alternative arrangements and conduct tests at least once a year, usually internally and organisation-wide, but in some cases in collaboration with linked FMIs and participants as well.

The responses include many other test types. The most common tests are a full switchover (used by a significant majority of the FMIs). In almost all of the tests, FMIs noted that they involve all related parties (participants, third parties, linked FMIs, internal staff, etc). In addition, a few FMIs perform industry-wide tests by including all related parties (third party providers, linked FMIs, participants, etc.) in the sector, usually annually or every two years. At least one of these also participates in a number of desktop exercises performed internationally, including those arranged by financial authorities.

4.4 Key Consideration 7: Interdependencies

Key Consideration 7 of Principle 17 provides that 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,

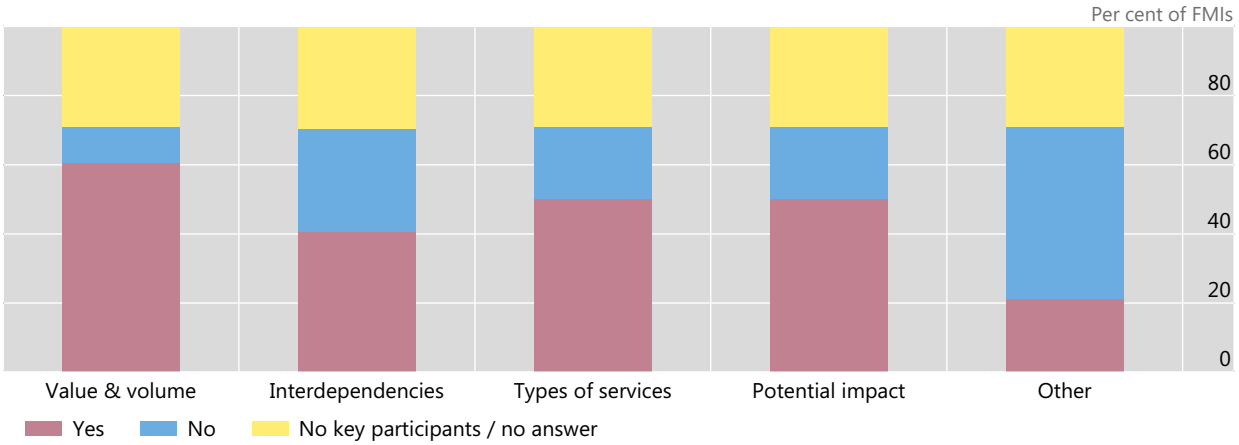
FMIs should identify, monitor, and manage the risks its operations might pose to other FMIs. This section discusses the findings with respect to each category of stakeholder, including key participants, other FMIs, and service and utility providers. The survey did not include any questions on the second part of the key consideration, ie that an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs, so there are no findings with respect to this.

4.4.1 Key participants

Almost all of the FMIs stated that they have identified the operational risks posed by key participants; at least one FMI responded that all participants are key participants. The answers from at least one FMI suggest that it does not consider any of its participants to be key participants. This FMI identified the risks posed by its settlement banks, payment systems and linked FMIs.

Most FMIs use volume and value criteria to identify which participants are key participants (Graph 3). Types of services and potential impact on the system are also common considerations. Some FMIs also consider interdependencies when identifying key participants. Other criteria mentioned were physical location, the extent to which they act as agents for indirect participants and regulatory status.

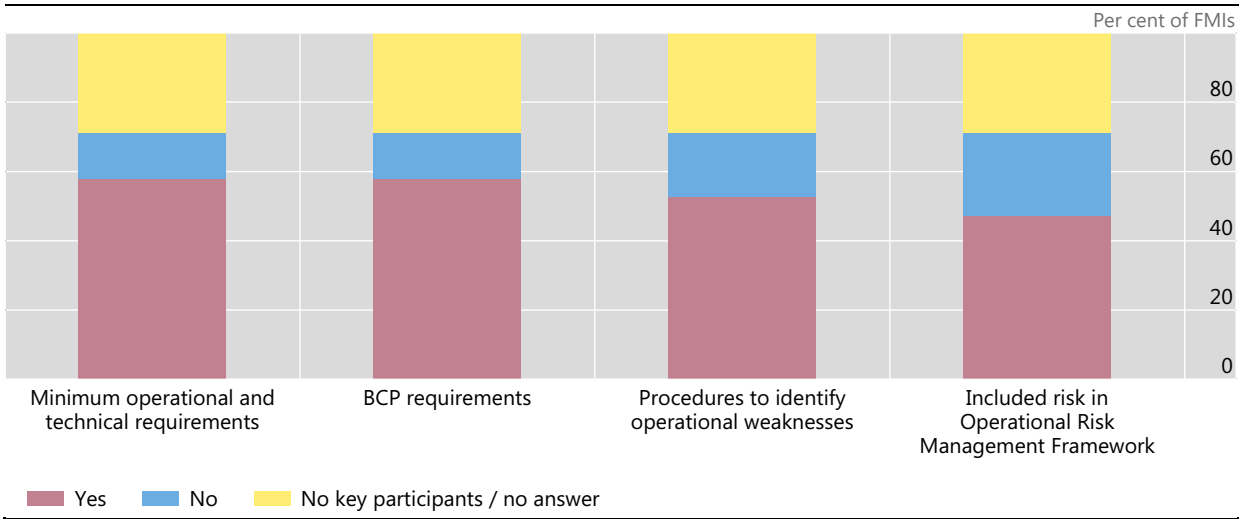
Criteria used to identify key participants — Graph 3



The responses from the FMIs indicated that they use a range of methods to manage the risks posed by key participants (Graph 4). Most FMIs indicated that they manage the risks posed by key participants by establishing minimum operational and technical requirements. Most stated that they establish business continuity requirements while others implement procedures to identify key participants' operational weaknesses. Most of the FMIs that identify key participants include associated risks in their own operational risk management frameworks.

Limited information was provided on how FMIs monitor the risks posed by key participants. From the information that was provided, this process included continuously monitoring a participant's activity, investigating incidents, requiring participants to self-certify compliance with operational risk requirements, requiring periodic audits to verify this compliance, and periodic review meetings with key participants.

Management of operational risk posed by key participants Graph 4



4.4.2 Other FMIs

Almost all of the FMIs stated that they have identified operational risks posed by other FMIs. At least one FMI stated that it is not affected by an outage at another FMI. Generally these risks come from payment systems and CSDs/SSSs, with a small number of FMIs also identifying risks from CCPs and at least one FMI identified risks posed by other TRs. A subset of the FMIs included non-FMIs in response to this question (eg custodians, exchanges/trading platforms, financial messaging providers, depositories and cash correspondents), suggesting that there are some misunderstandings about what constitutes an FMI.

Many FMIs' responses suggest that they manage this risk similarly to how they manage the risks posed by key participants, ie by setting minimum operational and technical requirements; establishing business continuity requirements; implementing procedures to identify weaknesses and including this risk in their Operational Risk Management Framework. A small number of FMIs mentioned that they have contingency arrangements (eg alternative communications arrangements) in place to manage the impact of an operational problem at another FMI.

4.4.3 Service providers

A significant majority of the FMIs stated that they have identified operational risks posed by service providers. Of the small number that did not, a few explained that they do not outsource critical services. FMIs identified a variety of types of outsourced services (Graph 5).[12] The most common type of service provider identified was a financial messaging provider. Some FMIs use outsourced data centres, although not all FMIs that use such services view them as critical. The other main type of outsourced service was application/software development and support; however, these services were not viewed as critical.

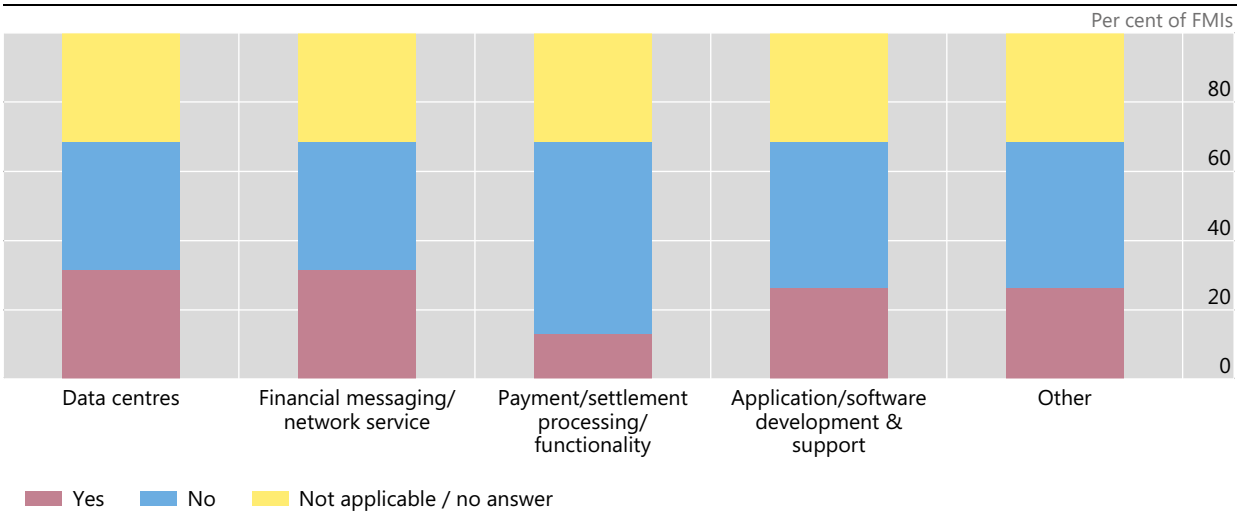
When asked about how CSPs are held to the same requirements, most FMIs mentioned contractual/service-level agreements. At least one FMI described contractual/service-level agreements that provide for audits and assessments to be shared with the FMI, allow for service meetings and on-site inspections, and include penalties for breaches. A few FMIs mentioned assessing CSPs against Annex F.

[12] The definition of a critical service provider in the PFMI is that they are a service provider that is critical to an FMI's operations (Annex F). The explanatory notes (paragraphs 3.17.20 and 3.17.21) give data processing, information systems management and financial messaging service providers as examples in the context of operational risk. In other parts of the PFMI, matching and portfolio compression service providers are given as another example (paragraph 3.3.1). In Annex F, the examples given are IT and messaging providers.

The responses from most of the FMIs indicate that at least a subset of CSPs are involved in some of the FMIs' business continuity tests and a small number of FMIs participated in the CSPs' BCP testing. Those that conducted BCP tests involving their CSPs generally did so on an annual basis. Tests conducted by the surveyed FMIs include failover, data or disaster recovery, and incident management (including communication procedures) as well as switchovers (eg to a second site). The involvement of providers depended on the nature of the tests being conducted.

Outsourced services

Graph 5



4.4.4 Utility providers

Almost all of the FMIs identified risks posed by utility providers; the remaining FMIs did not provide any explanation of why they did not face operational risks from utility providers. Power and telecommunications were the main types of utility providers identified. Interestingly, only a small number of FMIs identified water suppliers as critical utility providers.

To manage the risks posed by utility providers, most of the FMIs have contractual arrangements in place to ensure that the smooth provision of services is not affected. Most FMIs have informed their regulator about this dependency. Most also noted that they have established redundant sources of the service and/or have backup arrangements (eg uninterrupted power supply systems) in order to mitigate risk.

4.4.5 Cyber risks

A significant majority of the FMIs stated that they frequently review the cyber risks posed by third parties. Most FMIs noted that the review occurs annually, with a few FMIs stating they review these risks more frequently, the highest frequency being monthly.

Annex A: Survey questions

Principle 17, KC 3

"An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives."

Q1a. Please complete the following table on the operational reliability objectives in place at your FMI. *[Rows can be added to the table as required.]*

	Name/list of operational reliability objective(s) ("ORO") incl. units of measurement (eg "Transactions on Service Y processed in Z time"; "system A should be available xx per cent of the time")	**Is the ORO:** **(i) quantitative and/or** **(ii) qualitative in nature?** [Drop down menu: Quantitative or Qualitative]
1		
2		

b. Please indicate how frequently your FMI assesses/reviews each ORO and to whom the results of such review are communicated.

Q2. Please describe the policies, procedures, processes and mechanisms that you have in place at your FMI that are designed to meet each ORO outlined in Q1?

Q3. Do stakeholders (eg the board, board committees, senior management, other relevant decision-making bodies) review the OROs to gain comfort that new technological and business developments have been adequately incorporated? If so, how often do these stakeholders conduct such reviews?

Q4. Do your FMI's incident management procedures cover (*Select all that apply*):

i. Detection and recording of incidents
ii. Classification and initial support
iii. Investigation and root cause analysis of incidents
iv. Resolution of incidents
v. Incident closure
vi. Incident ownership, monitoring, tracking and communication
vii. Post-incident review
viii. Near misses
ix. Others (Please explain)

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 wide-scale 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."

Q5. How does the FMI's business continuity plan reflect objectives, policies and procedures that allow for the rapid recovery and timely resumption of critical operations following a wide-scale or major disruption? In particular:

a. Please describe the objectives of the FMI's business continuity plan with respect to wide-scale or major disruptions other than cyber events (eg, physical events).

b. Please describe the objectives of the FMI's business continuity plan with respect to cyber risk. Please include, among other scenarios, the case of a successful cyber-attack that compromise the integrity or availability of an FMI's data.

c. Please provide any other relevant information (eg How are the business continuity plan objectives set?)

Q6. *Secondary site*

a. Is there a secondary site (for both business operations and data centre) that has a distinct risk profile and can take over, recover and resume operations within two hours following a wide-scale or major physical disruptions? (Yes/No; please provide an explanation as appropriate.)

b. What factors has the FMI considered in determining the appropriateness of the location of the secondary site such that it has a distinct risk profile to the primary site? In particular:

	Event	**Yes/No**	**Explanation** (If "Y", please explain why the risk profile of the secondary site is considered sufficiently distinct from the primary site with respect to this potential disruption. If "N", please explain why not and indicate if plans are in place to address this.)
i.	A disruption of regional transportation networks (eg trains, roads, etc) that could potentially lead to the unavailability of many – and potentially all – staff within normal commuting range of the primary site.		
ii.	Weather/natural disasters (eg hurricane, earthquake,		

	snowstorm, wildfire, flooding, etc) that could potentially lead to the evacuation or unavailability of many – and potentially all – staff within normal commuting range of the primary site and/or to the inaccessibility of the primary site.		
iii.	A potential disruption of telecommunications connectivity at the primary site or a disruption to the regional telecommunications grid.		
iv.	A potential disruption of power supply at the primary site or a disruption to the regional power grids (eg electricity, gas, etc).		
v.	A potential disruption of the regional water supply across the entire metropolitan or other relevant geographic area in which the primary site is located.		
vi.	An act of terrorism (eg physical, biological, etc) that could potentially lead to the evacuation or unavailability of many – and potentially all – staff within normal commuting range of the primary site.		
vii.	Other.		Please explain.

c. How has the FMI identified all resources, capabilities, functionalities and appropriate staffing arrangements that would be needed to recover and resume critical operations (including all support, physical sites and related functions that are integral to performing the FMI's critical activities) within two hours and to complete settlement by end of day of the disruption?

d. Please provide any other relevant information.

Q7.

a. How and to what extent is the FMI's business continuity plan designed to enable critical IT systems to resume operations within two hours following disruptive events, and to enable the FMI to complete settlement by the end of the day even in extreme circumstances? In particular:

	Event		**Explanation** Please explain how the BCP is designed to enable the FMI to resume operations within two hours following each event. If the BCP is not currently designed to enable the FMI to resume operations within two hours following each event, please explain why not, the expected challenges that may impede the FMI to meet the 2-hr RTO, and indicate if plans are in place to address
i.	A disruption of regional transportation networks (eg trains, roads, etc) that could potentially lead to the unavailability of many – and potentially all – staff within normal commuting range of the primary site.		
ii.	Weather/natural disasters (eg hurricane, earthquake, snowstorm, wildfire, flooding, etc) that could potentially lead to the evacuation or unavailability of many – and potentially all – staff within normal commuting range of the primary site and/or to the inaccessibility of the primary site.		
iii.	A potential disruption of telecommunications connectivity at the primary site or a disruption to the regional telecommunications grid.		
iv.	A potential disruption of power supply at the primary site or a disruption to the regional power grids (eg electricity, gas, etc).		
v.	A potential disruption of the regional water supply across the entire metropolitan or other relevant geographic area in which the primary site is located.		
vi.	An act of terrorism (eg physical, biological, etc) that could potentially lead to the evacuation or unavailability of many – and potentially all – staff within normal commuting range of the primary site.		

vii.	Software failure not involving a cyber attack.		
viii.	A pandemic leading to the unavailability of all or a large proportion of staff.		
ix.	Other events resulting in widespread staff unavailability (eg industrial action).		
x.	Other.		Please explain.

b. If there is a possibility of data loss (eg due to potential gaps associated with asynchronous mirroring of data between the primary and backup site), what are the procedures to deal with such loss, including any procedures with participants or third parties?

c. Please provide any other relevant information, including on plans to resume operations and complete settlement if failing over to a secondary site is ineffective.

Q8. Please describe how the plan is designed to achieve a two-hour RTO and to complete settlement by the end of the day following a disruption involving an extreme but plausible cyber event, including following a disruption as a result of a cyber attack that compromises the integrity or availability of both primary and secondary systems or data of an FMI. In particular:

a.

	Potential element	**Yes/No**	**Explanation** Please indicate which, if any, of the following potential elements are included in the plan. If an element is included in the plan, please describe in more detail. If it is not included in the plan, please explain if you expect to include in the plan and what are the challenges faced to do so.
i.	Immediate actions upon detection of a cyber event to contain the situation, to prevent further damage, and to commence recovery efforts to restore operations.	(Y/N)	
ii.	Processes and procedures to protect and, if necessary, re-establish integrity and availability of the FMI's data and operations, and the confidentiality of its information assets.	(Y/N)	
iii.	Keeping a copy of all received and processed data (including the	(Y/N)	

	original intent of instructions being sent to the FMI for processing).		
iv.	Data-sharing agreements with relevant third parties or participants in advance in order to enable such uncorrupted data to be received in a timely manner once a successful cyber attack has been identified.		
v.	Maintaining transaction replay capability.	(Y/N)	
vi.	Conducting frequent periodic independent reconciliation of participants' positions.	(Y/N)	
vii.	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.	(Y/N)	
viii.	Recovery point objectives to support data integrity efforts that are consistent with the FMI's resumption time objective for critical operations.	(Y/N)	

b. How is the contingency plan designed to ensure that the status of all transactions can be identified in a timely manner, at the time of the disruption?

c. If there is a possibility of data loss, what are the procedures to deal with such loss?

d. Please provide any other relevant information (eg how do your FMI's policies and procedures define "an extreme but plausible" cyber event).

Q9. How do the FMI's crisis management procedures address the need for effective communications internally and with key external stakeholders and authorities? In particular:

a. Please describe how and to what extent your FMI's crisis management procedures include ex ante identification of crisis management staff and key decision makers (including roles and responsibilities).

b. What is the composition of your FMI's crisis management team?

c. What are your FMI's criteria and processes for crisis management activation?

d. Does the FMI have global importance or critical interlinkages with one or more interdependent FMIs? (Yes/No.)

e. If yes, is there a cross-system or cross-border crisis management arrangement and, if so, please describe this arrangement.

f. With whom does your FMI's BCP contain procedures to communicate? (*Please select all that apply.*)

i. Internal personnel and functions.
ii. The FMI's participants.
iii. Interdependent FMIs.
iv. Your FMI's service providers.
v. Relevant authorities.
vi. Others. (Please explain.)
vii. The business continuity plan does not contain such communication procedures. (Please elaborate.)

g. Please provide any other relevant information.

Q10. Has your FMI considered alternative arrangements (such as manual, paper-based procedures or alternatives) to allow the processing of time-critical transactions in extreme circumstances (in the event of a major physical-related or cyber-related outage)*? (Yes/No.)*

a. If "Yes", has the FMI made provisions for any such alternative arrangements in policies and procedures? If so, please describe the type of transactions considered "time-critical transaction" and the alternative arrangements to support processing of these transactions.

b. If "No", please explain if the FMI plans to consider this in the future.

Q11. How are the FMI's business continuity and contingency arrangements reviewed and tested? In particular:

a. Reviews

		Response[13]
i.	What might trigger a review of the BCP (identification of new threats, serious incident, testing identified weaknesses, etc)?	
ii.	Scope of reviews (partial (eg updated or new element, select processes, including the recovery/reconciliation of potentially lost or corrupt data) or full BCP).	
iii.	Frequency of such reviews.	

[13] Where applicable, please describe the extent to which testing covers all of the identified resources, capabilities, functionalities and appropriate staffing arrangements that would be needed to recover and resume critical operations (including all support and related functions that are integral to performing the FMI's critical activities).

b. Tests (*rows can be added if necessary*)

Description of the types of tests conducted (eg full/partial site switchover, recovery/reconciliation of potentially lost or corrupt data, desktop exercises, crisis management exercises)	**Frequency of testing** (eg annual, quarterly etc)	**Parties involved in the testing** (eg FMI participants, critical service providers, linked FMIs)

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."

Q12. What risks has the FMI identified to its operations arising from its key participants, other FMIs and service utility providers?[14] How and to what extent does the FMI monitor and manage these risks? Please provide your response in the table below:

	Has the FMI identified operational risks from these stakeholders? (Y/N)	**Type of entity**	**Explanation** (If you have answered "Y" for column 2, please describe how and to what extent the FMI monitors and manages these risks. If "N", please explain.)
Key participants		Eg banks, payment service providers, dealers, etc.	
Other FMIs		Eg payment system, CSD, etc.	
Service providers[15]		Eg financial messaging provider, etc.	
Utility providers		Eg power and telecommunications companies.	

Q13. Does the FMI rely upon externally provided services critical to its operations (including outsourced services)? (Yes/No.) If "Yes":

a. What types of critical services are outsourced,[16] offshored or otherwise externally sourced?

[14] Further details are provided in the PFMI, paragraph 3.17.21. An example of a "critical service provider" is a financial messaging provider or an information technology provider (PFMI, Annex F: Oversight expectations applicable to critical service providers). Power and telecommunications companies would be examples of "utility providers".

[15] Other than utility providers.

[16] Including intragroup outsourcing.

b. If the FMI has outsourced services critical to its operations, how and to what extent does the FMI ensure that the operations of a critical service provider meet the same reliability and contingency requirements they would need to meet if they were provided internally?

c. How does the FMI involve critical service providers in the testing of its BCP?

Q14. How frequently does your FMI review the cyber risks that it bears from its third-party service providers?

Any other useful information for the purposes of this survey

Q15. Please provide any other information or additional explanation that you deem appropriate to get a better understanding on how your FMI observes or applies Principle 17, Key Considerations 3, 6 and 7.

Annex B: Members of the IMSG and assessment team

IMSG co-chairs	
Bank of France	Valérie Fasquelle
Securities and Exchange Commission, United States	Christian Sabella
IMSG and assessment team members	
Reserve Bank of Australia	Matthew Gibson Ninad Chitnis**
National Bank of Belgium	Vincent Olécrano**
Bank of Canada	Wade McMahon Yusu Guo**
Bank of France	Thomas Carré* (assessment team member from Feb 2020) Clay Youale** (until Jan 2020)
Bundesanstalt für Finanzdienstleistungsaufsicht, Germany	Edip Acat (until May 2020)
European Central Bank	Tom Kokkola Patrick Papsdorf**
European Securities and Markets Authority	Maud Timon
Hong Kong Monetary Authority	Stephen Pang* (until Jan 2020) Osbert Lam* (from Jan 2020)
Securities and Futures Commission, Hong Kong SAR	Thomas Wong**
Securities and Exchange Board of India	Sanjay Purao (until Dec 2019) Amit Tandon (Dec 2019 to Dec 2020) Sudeep Mishra (from Dec 2020)
Bank of Italy	Veronica Fucile Anna Maria Germano**
Bank of Japan	Takashi Hamano
Financial Services Agency, Japan	Kazunari Mochizuki
Bank of Korea	Hyung Koo Lee (until Apr 2020) Myeong-Jin Han (Apr 2020 to Feb 2021) Sanghyun Song (from Feb 2021)
Central Bank of the Russian Federation	Ekaterina Seredkina
Monetary Authority of Singapore	Tze Hon Lau Joey Ho
Bank of Spain	Carlos Conesa**#
Comisión Nacional del Mercado de Valores, Spain	Vicente García Rubert**
Sveriges Riksbank	Loredana Sinko
Capital Markets Board of Turkey	Nalan Sahin Urkan Cemil Ulu**

Bank of England	Harpal Singh Hungin* (until Oct 2020) James Pople Hoskins (from Oct 2020)
Board of Governors of the Federal Reserve System	Jessica Dwyer (until Jan 2021) Kathy Wang (from Jan 2021)
Federal Reserve Bank of New York	John Rutigliano Jenny McMahan**
Commodity Futures Trading Commission, United States	Andrée Goldsmith (until Mar 2020) Alicia Lewis (from Mar 2020 to Feb 2021) Andrea Musalem (from Feb 2021) Frank J Sensenbrenner**
Securities and Exchange Commission, United States	Stephanie Kim Park Sharon Park**[#]
IOSCO Assessment Committee	Raluca Tircoci-Craciun
IOSCO Secretariat	Tajinder Singh Josafat De Luna Martínez
CPMI Secretariat	Umar Faruqui Jenny Hancock Dalton Appolis (until Dec 2019)

* IMSG and assessment team member.
** Assessment team member only.
[#] Assessment team lead.

The IMSG would like to extend its thanks to Carlos Conesa (Bank of Spain) and Sharon Park (Securities and Exchange Commission, United States), the team co-leads for this assessment, and the experts that made up the assessment team. In addition, the IMSG thanks Codruta Boar (Bank for International Settlements), Sofía Galmés (Bank of Spain), Luis López (Bank for International Settlements), José Luis Romero (Bank of Spain) and Jara Quintanero (Bank of Spain) for their assistance in the assessment process.