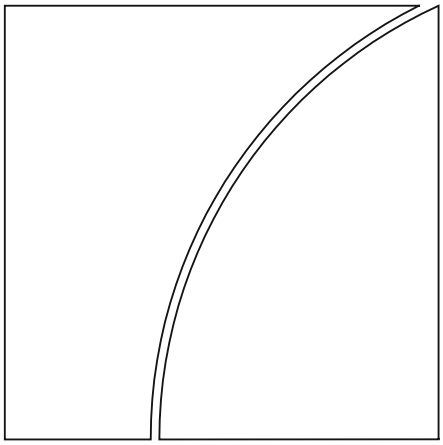
Committee on Payments and Market Infrastructures

Board of the International Organization of Securities Commissions



Principles for financial market infrastructures:

Assessment methodology for the oversight expectations applicable to critical service providers

December 2014

BANK FOR INTERNATIONAL SETTLEMENTS

OICV-IOSCO

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

Statement by IOSCO: *Certain authorities may consider rule proposals or standards that relate to the substance of this report. These authorities provided information to IOSCO or otherwise participated in the preparation of this report, but their participation should not be viewed as an expression of a judgment by these authorities regarding their current or future regulatory proposals or of their rulemaking or standards implementation work. This report thus does not reflect a judgment by, or limit the choices of, these authorities with regard to their proposed or final versions of their rules or standards.*

ISBN 978-92-9197-025-4 (online)

Introduction

Annex F of the *Principles for financial market infrastructures* outlines five oversight expectations for critical service providers in order to support a financial market infrastructure's (FMI) overall safety and efficiency.[1] Although the FMI remains ultimately responsible for its operations, the regulator, supervisor or overseer of the FMI may use Annex F to establish expectations specifically targeted at critical service providers. In those cases where an authority does so, adherence to these expectations can be achieved in one of two ways, at the discretion of the authority: (i) the authority monitors adherence to the expectations itself in a direct relationship with the critical service provider;[2] or (ii) the authority communicates the standards to the FMI, which obtains assurances from its critical service providers that they comply with the expectations. These expectations may also be relevant to an FMI as it reviews its contracts with critical service providers.

Where permitted under the applicable legal framework, a regulator, supervisor or overseer of an FMI may choose to assess an FMI's critical service provider against these expectations to promote robust payment systems that are systemically important, central securities depositories, securities settlement systems, central counterparties and trade repositories. Such assessments are intended to provide an assurance of quality of service that FMIs would seek from their critical service providers as part of their compliance with the broader principles of the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO).

Critical service providers

As noted in Annex F, the operational reliability of an FMI may be dependent on the continuous and adequate functioning of third-party service providers that are critical to an FMI's operations, such as information technology and messaging providers. An FMI may have a contractual arrangement with a third-party service provider that performs, on a continuing basis, activities essential to the operations of the FMI. The continuous, secure and efficient delivery of these services by the third-party service provider may be critical to the operations of the FMI or, in some cases, multiple FMIs.

Where a third-party service provider operates other lines of business or provides other services that are not essential or important to the operation of an FMI, these activities are out of the scope of the assessment against the oversight expectations of Annex F.

Unless otherwise indicated by the relevant authorities, activities not directly related to essential operations of the FMI and utilities (such as basic telecommunication services, water, electricity and gas) are out of scope when identifying critical service providers.

Oversight expectations of authorities

Where they have the authority to do so, authorities may choose to establish expectations for critical service providers of FMIs in order to support their responsibilities in regulating, supervising and overseeing FMIs. Annex F outlines five oversight expectations that help ensure that the operations of a critical service provider are held to the same standards as the FMI would be if it provided the same

[1] See CPSS-IOSCO, *Principles for financial market infrastructures*, April 2012. Before 1 September 2014, the Committee on Payments and Market Infrastructures (CPMI) was known as the Committee on Payment and Settlement Systems (CPSS). Please note that references to reports published before that date cite the Committee's old name.

[2] Such direct relationship between the authority and the critical service provider does not exempt the FMI from the requirement that "A contractual relationship should be in place between the FMI and the critical service provider allowing the FMI [and relevant authorities] to have full access to necessary information", as specified in the *Principles for financial market infrastructures,* 3.17.20.

service. These expectations are specifically targeted at ensuring strong risk identification and management, robust information security management, reliability and resilience of systems, effective technology planning and strong communications with users.[3] These expectations are written at a broad level, allowing critical service providers flexibility in demonstrating that they meet the expectations.

Assessment methodology

This document establishes an assessment methodology and provides guidance for regulators, supervisors and overseers in assessing an FMI's critical service providers against the oversight expectations in Annex F. This assessment methodology mirrors the approach used in the CPSS-IOSCO *Principles for financial market infrastructures: disclosure framework and assessment methodology* report.[4] Typically, this assessment would be conducted (or commanded) by the critical service provider itself, which would then make the (self-)assessment available to the FMI and the latter's regulatory authority. The assessment methodology relies on key questions for each oversight expectation, which address the critical service provider's approach or framework for managing risks. These questions are not intended to serve purely as a checklist or to be exhaustive. Regulators, supervisors and overseers of FMIs could, at their discretion, pose additional questions as needed to address the particulars of the FMI, its critical service providers or other relevant issues.

This assessment methodology also provides guidance to critical service providers in complying with the oversight expectations in Annex F. The assessment methodology builds upon the existing explanatory text in Annex F and provides more detailed guidance on risk management practices and additional issues of consideration. The key questions seek answers as to whether the critical service provider's policies and procedures in the identified areas are clear and comprehensive, and how these are documented, reviewed and updated. A critical service provider may find it beneficial to disclose its answers to the key questions in the assessment methodology in order to help authorities, FMIs and, where relevant, their participants enhance their understanding of the risks involved in using the critical service provider's services.

Under this assessment methodology for Annex F, a rating for each oversight expectation can be assigned according to the same framework developed for the CPSS-IOSCO *Principles for financial market infrastructures: disclosure framework and assessment methodology*. The rating framework is built on the gravity and urgency of the need to remedy identified issues of concern.

This assessment focuses only on the critical services provided by a third-party service provider to an FMI.

Cooperation among authorities

If a critical service provider provides critical services to multiple FMIs, authorities of the respective FMIs could cooperate with each other in assessing the critical service provider against these expectations. Where such cooperation is set up, authorities should observe the guidance provided in Responsibility E of the CPSS-IOSCO *Principles for financial market infrastructures*, the CPSS *Central bank oversight of payment and settlement systems* and the IOSCO *Principles regarding cross-border supervisory cooperation*, as appropriate.[5]

[3] Users are the customers of the critical service provider, and include (an) FMI(s) and its/their participants, as relevant.

[4] CPSS-IOSCO, *Principles for financial market infrastructures: disclosure framework and assessment methodology*, December 2012.

[5] See CPSS, *Central bank oversight of payment and settlement systems*, May 2005, and IOSCO, *Principles regarding cross-border supervisory cooperation*, May 2010.

The authority of an FMI might have limited direct access to a critical service provider of that FMI when the critical service provider resides in another country. In such case, the authority can either convey its requirements through the above-mentioned cross-border supervisory cooperation, or communicate its requirements via the FMI over which it has authority.

Oversight expectations applicable to critical service providers and key questions

OE 1. Risk identification and management

A critical service provider is expected to identify and manage relevant operational and financial risks to its critical services and ensure that its risk-management processes are effective.

A critical service provider should have effective processes and systems for identifying and documenting risks, implementing controls to manage risks, and making decisions to accept certain risks. A critical service provider may face risks related to information security, reliability and resilience, and technology planning, as well as legal and regulatory requirements pertaining to its corporate organisation and conduct, relationships with customers, strategic decisions that affect its ability to operate as a going concern, and dependencies on third parties. A critical service provider should reassess its risks, as well as the adequacy of its risk-management framework in addressing the identified risks, on an ongoing basis.

The identification and management of risks should be overseen by the critical service provider's board of directors (board) and assessed by an independent, internal audit function that can communicate clearly its assessments to relevant board members. The board is expected to ensure an independent and professional internal audit function. The internal audit function should be reviewed to ensure it adheres to the principles of a professional organisation that governs audit practice and behaviour (such as the Institute of Internal Auditors) and is able to independently assess inherent risks as well as the design and effectiveness of risk-management processes and internal controls. The internal audit function should also ensure that its assessments are communicated clearly to relevant board members.

Key questions

Enterprise-wide risk management framework

Q 1.1: What are the critical service provider's processes and systems to identify and document its risks, including relevant operational, financial and human resources risks? What risks did the critical service provider identify and document through its processes and systems?

Q 1.2: What are the critical service provider's processes and systems to manage these risks? How does the critical service provider decide on accepting residual risks?

Q 1.3: How does the critical service provider reassess its risks and the adequacy of its risk-management framework in addressing the identified risks? How frequently is this reassessment conducted?

Q 1.4: How does the critical service provider address any legal or regulatory requirements or changes in requirements?

Q 1.5: How does the critical service provider assess risks relating to its relationships with users?

Q 1.6: How does the critical service provider incorporate risk management into its strategic decision-making process, including assessments of general business risk and financial condition?

Dependencies on third parties

Q 1.7: How does the critical service provider identify and monitor the risks that dependencies on third-party providers might pose to its operations?

Q 1.8: How does the critical service provider assess that the security, reliability and resilience of its operations are not reduced by dependencies on third parties?

Q 1.9: How does the critical service provider manage/address any unaccepted reduction in the security, reliability and resilience of its operations caused by its dependencies on third parties?

Governance of the enterprise-wide risk management framework

Q 1.10: What are the critical service provider's governance arrangements for the identification and management of risks? What are the lines of responsibility and accountability within the critical service provider as they relate to risk management? How frequently is the effectiveness of the internal audit function reviewed?

Q 1.11: How does the critical service provider's board explicitly review and endorse the enterprise-wide risk management framework?

Internal audit function

Q 1.12: How does the critical service provider ensure an independent and professional audit function? To which of the internationally accepted practices that govern the audit profession does the internal audit function adhere?

Q 1.13: What are the reporting mechanisms for the internal audit function to communicate its findings to the board and, where appropriate, its regulator or overseer?

OE 2. Information security

A critical service provider is expected to implement and maintain appropriate policies and procedures, and devote sufficient resources to ensure the confidentiality and integrity of information and the availability of its critical services in order to fulfil the terms of its relationship with an FMI.

A critical service provider should have a robust information security framework that appropriately manages its information security risks. The framework should include sound policies and procedures to protect information from unauthorised disclosure, ensure data integrity, and guarantee the availability of its services. In addition, a critical service provider should have policies and procedures for monitoring its compliance with its information security framework. This framework should also include capacity planning policies and change-management practices. For example, a critical service provider that plans to change its operations should assess the implications of such a change on its information security arrangements.

Key questions

Information security framework

Q 2.1: What is the critical service provider's enterprise-wide information security framework for providing general, overarching guidance on the solutions and practices for addressing physical and cyber security risks? How does this framework encompass policies and procedures for:

a) categorising assets (systems and services) along the dimensions of confidentiality, integrity and availability;

b) identifying internal and external threats on an ongoing basis;

c) selecting, implementing and documenting security controls to mitigate identified risks and vulnerabilities; and

d) adequate governance of all security risk-management activities?

Q 2.2: How does the critical service provider incorporate relevant international, national and industry standards into its policies and procedures?

Q 2.3: What sources of information security risks has the critical service provider identified relating to its critical services? How has the critical service provider addressed these risks?

Q 2.4: What is the critical service provider's board involvement in the critical service provider's information security framework? Does the board explicitly review and endorse the framework? How frequently does the board review the framework?

Q 2.5: How has the critical service provider's board endorsed senior management's key roles and responsibilities for information security?

Information security policies and procedures

Q 2.6: What policies and procedures are used to prevent unauthorised access and unauthorised disclosure of information?

In particular, what are policies and procedures for:

a) granting authorisations to and removing authorisations from users, including both logical and physical access;

b) periodic recertification of user privileges;

c) granting, using and controlling administrator (or highly privileged) accounts;

d) avoiding data confidentiality breaches;

e) protecting the integrity of systems against logical or physical attacks; and

f) embedding controls in applications provided to the FMI, to prevent errors, loss, unauthorised modification or misuse of information?

Q 2.7: How does the critical service provider ensure that all employees and relevant external parties are made aware of their responsibilities and liabilities, and of security threats, as defined in the information security framework?

Q 2.8: What policies and procedures are used to ensure the confidentiality, integrity and non-repudiation of data, including while in transit on networks and while stored at the critical service provider?

Q 2.9: What policies and procedures are used to detect, react to and recover from information security incidents?

Security compliance monitoring

Q 2.10: How does the critical service provider verify compliance with its information security framework and monitor the effectiveness of the security controls in place? Specifically, do these policies and procedures include vulnerability scanning and penetration testing at both infrastructure and application level?

Q 2.11: To what extent is the critical service provider's information security framework subject to internal and external audit?

Q 2.12: How and with what frequency is the critical service provider's board updated on the main findings of the security compliance monitoring activities?

Capacity planning

Q 2.13: What are the critical service provider's policies on capacity planning? How does the critical service provider monitor and adjust the use of resources to meet the needs of the FMI and, where appropriate, its participants, even in stressed market conditions? How does the critical service provider address situations where the FMI's or participants' needs exceed operational capacity?

Q 2.14: How does the critical service provider review, audit, and test the scalability and adequacy of its capacity to handle, at the minimum, projected stress volumes identified by one FMI, and, where applicable, concurrent projected stress volumes when serving several FMIs? How frequently does the critical service provider conduct these reviews, audits and tests?

Change management

Q 2.15: How do the critical service provider's change management and project management policies and procedures mitigate the risks that changes inadvertently affect the security and reliability of the critical service provider's operations?

Q 2.16: How do the critical service provider's change management policies define formal management responsibilities and procedures for the planning and testing of changes, including regression, performance and security testing?

Q 2.17: To what extent are changes impacting users subject to consultation with the FMI and tested with the participation of the FMI and, where appropriate, of its participants?

OE 3. Reliability and resilience

A critical service provider is expected to implement appropriate policies and procedures, and devote sufficient resources to ensure that its critical services are available, reliable, and resilient. Its business continuity management and disaster recovery plans should therefore support the timely resumption of its critical services in the event of an outage so that the service provided fulfils the terms of its agreement with an FMI.

A critical service provider should ensure that it provides reliable and resilient operations to users, whether these operations are provided to an FMI directly or to both an FMI and its participants. A critical service provider should have robust operations that meet or exceed the needs of the FMI. Any operational incidents should be recorded and reported to the FMI and the FMI's regulator, supervisor, or overseer. Incidents should be analysed promptly by the critical service provider in order to prevent recurrences that could have greater implications. In addition, a critical service provider should have robust business continuity and disaster recovery objectives and plans. These plans should include routine business continuity testing and a review of these test results to assess the risk of a major operational disruption.

Key questions

Available, reliable and resilient operations

Q 3.1: What are the critical service provider's operational availability, reliability and resilience objectives and how are these documented? How do these objectives meet or exceed the needs of the FMI and, where appropriate, of its participants?

Q 3.2: How do the critical service provider's policies and procedures support its availability, reliability and resilience objectives?

Q 3.3: How does the critical service provider ensure that it provides reliable and resilient operations to the FMI and, where relevant, its participants? In particular, how does the critical service provider ensure that its different operating sites have sufficiently different risk profiles? How does the critical service provider ensure that its operating sites are adequately protected against natural disasters, power failures and adverse human actions? How does the critical service provider ensure that its backup sites have sufficient capacity to handle the critical services for a sustained period of time?

Operations monitoring and incident management

Q 3.4: How does the critical service provider monitor its operations? How does the critical service provider monitor whether it meets the reliability and resilience objectives of the FMI? How is this process documented and maintained?

Q 3.5: How does the critical service provider identify, record, categorise, analyse and manage operational incidents? How are these incidents reported to senior management? How does the critical service provider keep the FMI and, where appropriate, relevant authorities, informed about such incidents? What is the process for escalating an incident into a crisis?

Q 3.6: What is the process for performing a post-mortem analysis of incidents, and how is this process designed to ensure identification of the root cause of incidents and to avoid recurrence in the future? What is the FMI's involvement in such a post-mortem analysis?

Business continuity

Q 3.7: What are the critical service provider's business continuity and disaster recovery objectives? How are these objectives set by the board and senior management? How frequently are these objectives reviewed by the board and senior management?

Q 3.8: How do the critical service provider's business continuity and disaster recovery plans ensure the timely resumption of its critical services in the event of a service disruption, including in case of a wide-scale disruption? How do these plans address potential data loss resulting from a service disruption?

Q 3.9: How does the critical service provider identify scenarios on potential service disruption and how is the FMI involved in this process?

Q 3.10: How does the critical service provider's business continuity and disaster recovery plans address cyber attacks? How do these plans ensure that the critical service provider will have the ability to identify and manage the impact of a cyber attack, including the recovery of systems after a compromise?

Q 3.11: What is the critical service provider's crisis communication plan to handle service disruptions? In particular, how does the plan address communications and information exchange with the FMI and relevant authorities?

Q 3.12: How are the business continuity and disaster recovery plans tested and with which frequency? Which scenarios are tested and do they include cyber attacks? How are the results of these tests assessed and audited? How are the FMI and, where relevant, its participants, involved in business continuity simulation tests?

Q 3.13: How are the business continuity and disaster recovery plans of the critical service provider regularly assessed with the FMI expectations?

OE 4. Technology planning

The critical service provider is expected to have in place robust methods to plan for the entire lifecycle of the use of technologies and the selection of technological standards.

A critical service provider should have effective technology planning that minimises overall operational risk and enhances operational performance. Planning entails a comprehensive information technology strategy that considers the entire lifecycle for the use of technologies and a process for selecting standards when deploying and managing a service. Proposed changes to a critical service provider's technology should entail a thorough and comprehensive consultation with the FMI and, where relevant, its participants. A critical service provider should regularly review its technology plans, including assessments of its technologies and the processes it uses for implementing change.

Key questions

Policies, procedures and governance arrangements for technology planning

Q 4.1: What are the critical service provider's policies, procedures and governance arrangements for technology planning? How do these policies, procedures and governance arrangements address the lifecycle for the use of technologies and the selection of new technological standards?

Q 4.2: How frequently does the critical service provider assess its technology risks? How do such assessments take into account reliability and resilience, obsolescence risks and information security risks related to the use of its technology? How do these assessments take into account technology risks potentially affecting the FMI and, where appropriate, its participants?

Policies, procedures and governance arrangements for managing technological changes

Q 4.3: What are the critical service provider's policies, procedures and governance arrangements for implementing changes to the technologies used? How do these policies and procedures address release management, the consistent use of technology and maintaining the security and stability of technology?

Q 4.4: How do these policies, procedures and governance arrangements ensure that risks related to technology changes are identified and adequately mitigated, in order to avoid such changes potentially impacting the reliability and resilience of the provider's critical services? How and with what frequency does the critical service provider assess and test the processes used for implementing technological changes?

Q 4.5: How does the critical service provider consult with the FMI and, where relevant, its participants, in any proposed important changes to its technology that may materially affect the FMI?

Q 4.6: How does the critical service involve the FMI, where appropriate, when implementing a technology change? For example, is the FMI involved in the testing of technology changes as appropriate?

OE 5. Communication with users

A critical service provider is expected to be transparent to its users and provide them sufficient information to enable users to understand clearly their roles and responsibilities in managing risks related to their use of a critical service provider.

A critical service provider should have effective customer communication procedures and processes. In particular, a critical service provider should provide the FMI and, where appropriate, its participants with sufficient information so that users clearly understand their roles and responsibilities, enabling them to manage adequately their risks related to their use of the services provided. Useful information for users typically includes, but is not limited to, information concerning the critical service provider's management processes, controls, and independent reviews of the effectiveness of these processes and controls. As a part of its communication procedures and processes, a critical service provider should have mechanisms to consult with users and the broader market on any technical changes to its operations that may affect its risk profile, including incidences of absent or non-performing risk controls of services. In addition, a critical service provider should have a crisis communication plan to handle operational disruptions to its services.

Key questions

General communication

Q 5.1: What are the critical service provider's procedures and processes for communicating with users?

Q.5.2: What information does the critical service provider provide to the FMI and, where appropriate, its participants so that they understand their roles and responsibilities, enabling them to manage the risks related to their use of the critical service provider? With what frequency is this information reviewed?

Q.5.3: How does the critical service provider communicate to users on important changes to its operations? (See also Q.2.17, Q.4.5 and Q.4.6.)

Q 5.4: How does the critical service provider communicate to its users its risk analysis, including relevant operational, financial and human resources risks?

Consultation mechanisms

Q 5.5: What mechanisms are used by the critical service provider to consult with users and the broader market when needed (for example, on any technical changes to its operations that may materially affect the FMI)? (See also Q.4.5.)

Communications on incidents and in crisis situations

Q 5.6: How does the critical service provider inform users, where appropriate, about incidents? (See also Q.3.5.)

Q 5.7: What is the critical service provider's crisis communication plan for handling service disruptions? Does this plan involve all users and relevant stakeholders? (See also Q.3.11.)