OVERVIEW

No. RADAR
4237

Responsible level
International

Competent authority
IOSCO – International Organization of Securities Commissions

Standard designation
Principles on Outsourcing

Title of Standard
Principles on Outsourcing

Abbreviation (standard)

Short Title

Abbreviation (standard)
FRI07/2021

Abbreviation
FRI07/2021

Implementation status of the standard
published

Industry relevance
Banking industry

category
02. Capital Markets Law

Document type
Miscellaneous

Management Summary
Increasing transaction speed and growing competition are leading to greater complexity in markets and businesses, accompanied by increasing automation of trading. At the same time, this creates incentives to reduce costs and increase efficiency, which are being achieved, among other things, through the outsourcing of activities to service providers. IOSCO observes that some market participants and infrastructures are outsourcing on a significant scale, resulting in dependencies on service providers.

Against this background, IOSCO has updated the existing principles on outsourcing (Outsourcing Principles for Market Intermediaries (2005) and Outsourcing Principles for Markets (2009)) and summarized them in this report. In addition to intermediaries and trading venues, the user group explicitly includes principals, financial market infrastructures, and credit rating agencies. IOSCO formulates fundamental principles and seven principles for outsourcing. The fundamental principles include the definition of outsourcing, details on the assessment of materiality and criticality, related entities, subcontracting, and cross-border outsourcing. The seven principles set out IOSCO's expectations of supervised entities that outsource functions and formulate guidelines for implementation.

Management Summary

The increasing speed of transactions and growing competition are leading to greater complexity of markets and transactions, accompanied by increasing automation of trading. This creates incentives to reduce costs and increase efficiency, eg by outsourcing activities to service providers. IOSCO observes that market participants and infrastructures sometimes outsource activities on a significant extent that is leading to a certain dependency on service providers in this respect.

Against this background, IOSCO has updated the existing principles on outsourcing (Outsourcing Principles for Market Intermediaries (2005) and Outsourcing Principles for Markets (2009)) and summarized them in this report. In addition to intermediaries and trading venues, the application group explicitly includes proprietary traders, financial market infrastructures and credit rating agencies. IOSCO sets out fundamental precepts and seven principles on outsourcing. These precepts include the definition of outsourcing, the assessment of materiality and criticality, related parties, subcontracting and cross-border outsourcing. The seven principles set out IOSCO's expectations for regulated entities that outsource tasks and provide guidance for implementation.

CONTENTS

Main content

B. Essential content

I. Basic Principles (Chapter 4)

Section A explains the scope of users in more detail and specifies which companies fall under the terms trading venues, intermediaries and market participants, credit rating agencies and financial market infrastructures within the meaning of these principles (see source for details).
The scope of outsourcing covered by these principles is specified in Section B. It is clarified that both sub-outsourcing and intra-group outsourcing are covered by the requirements (see source for details).
Sections C to D provide clarifications on the responsibility of the outsourcing company and the risks and challenges associated with outsourcing.
Section E explains the proportionality aspect to be considered in connection with these principles. For the assessment of materiality and

A non-exhaustive list of relevant indicators is provided to assess the criticality of an outsourcing arrangement. These include, among other things, potential impacts on pricing, potential risks to clearing and settlement systems, service quality, and data integrity (see source for details).
Sections F to H contain information on outsourcing within a group, cross-border outsourcing and further outsourcing (see source for details).
According to the explanations in Section I, concentration risks caused by outsourcing are also considered relevant when a large number of companies access the same service provider (see source for details).

II. Principles of outsourcing (Chapter 5)

1. Due diligence in the selection and monitoring of a service provider and its performance

a) Principle 1: A supervised entity should apply appropriate due diligence procedures in selecting a suitable service provider and monitoring its ongoing performance.
Companies should ensure that the service provider has the capabilities and capacity to perform the outsourced functions on an ongoing basis. When determining appropriate monitoring measures, the materiality and criticality of the outsourced functions with respect to ongoing business operations and regulatory obligations should be considered.

b) Implementation

The implementation of the requirements according to Principle 1 can be achieved, for example, by the following steps (see source for details):

- documented procedures for evaluating the service provider (including technical, financial and human resources);
- appropriate measures to ensure that the selection, evaluation and monitoring of the service provider is carried out by appropriately competent staff (e.g. by involving various internal departments);
- Processes and procedures for identifying potential or actual conflicts of interest (including at Group level) and procedures for dealing with them;
- Review of the service provider’s market position to avoid concentration risks;
- Processes and procedures for monitoring service provision and compliance with legal framework conditions, including measures in the event of non-compliance;
- documented procedures for re-evaluating existing outsourcing agreements.

In addition, the company must maintain a minimum level of operational and management capacity appropriate to its business model, size, and nature of the activity. Key functions such as management and control functions (e.g., risk management, compliance) should generally remain with the supervised entity. The company should periodically review whether excessive outsourcing of activities is occurring, whether controls are adequate to monitor the outsourced functions, and whether activities should be brought back in-house. Outsourcing management can be assigned to a dedicated function (see source for details).

2. The contract with a service provider

a) Principle 2: A supervised entity should enter into a legally binding written contract with each service provider, the nature and details of which should be appropriate to the materiality or criticality of the outsourced function to the regulated entity's business.

The level of detail of contractual agreements must be adapted to the circumstances of the outsourcing company, taking into account proportionality aspects and any regulatory requirements (see source for details).
b) Implementation
Regarding the assessment of the materiality and criticality of the outsourced tasks for appropriate consideration in the contract design, reference is made to Section F of the fundamental principles (see Section I). Possible elements for the contract design include, for example, the scope of responsibility and liability, monitoring and intervention options by the outsourcing company, confidentiality in data processing, provisions regarding the emergency plan, and the handling upon termination of the outsourcing (see source for details).

3. Information security, resilience, continuity and disaster recovery
(a) Principle 3: A supervised entity should take appropriate measures to ensure that both the supervised entity and each service provider establish procedures and controls to protect the supervised entity's own and client information and software and to ensure continuity of service to the supervised entity, including a disaster recovery plan with regular testing of the safeguards.

Service providers should have adequate IT security, cybercrime resilience, and contingency plans in place. Additional measures may be required if outsourcing is conducted at a cross-border level.
b) Implementation
Appropriate measures and standards should be included in the contract with the service provider and include, among other things, the following steps (see source for details):

- Specification of security requirements for automated systems, including data protection measures and, in particular, customer privacy protection in accordance with legal provisions (particularly relevant when outsourcing to cloud technology providers);

- comprehensive cybersecurity security measures taken by the service provider and their regular testing;

- Disclosure of security breaches by the service provider that lead to unauthorized access and preparation of a corresponding report;

- measures to be taken upon termination of outsourcing;

- Ensuring comprehensive cybersecurity and resilience programs at the service provider (taking into account relevant standards).

4. Questions of confidentiality
(a) Principle 4: A supervised entity should take appropriate measures to ensure that service providers protect confidential information and data relating to the supervised entity and its clients from intentional or accidental unauthorised disclosure to third parties.

b) Implementation
Appropriate measures to secure confidential data and protect it from misuse should be included in the contract and could include the following conditions (see source for details):

- a prohibition on the use and/or disclosure of confidential data of the supervised entity or its customers;

- Consideration of both physical and electronic information;

- Regulation for subcontractors;

- Obligation of the service provider to securely dispose of data and information after termination of the contractual relationship, taking into account the retention periods.

If necessary, customers should be informed about the transfer of data to a service provider. If necessary, additional precautions (e.g., enhanced data encryption) should be implemented (see source for details).

5. Concentration of outsourcing agreements

(a) Principle 5: A supervised entity should be aware of and effectively manage the risks of being dependent on a single service provider for essential or critical outsourced functions or knowing that a service provider provides essential or critical outsourcing services to several supervised entities, including itself.
With regard to potential concentration risks, both the individual dependence of the company and the overall market share of the service provider must be considered. In this context, IOSCO recognizes that, despite best efforts, companies may not have sufficient information about the provider's business scope. Subshoring can also make it difficult to effectively identify concentration risks, particularly when the companies in the subshoring chain are spread across different physical and geographical locations.

b) Implementation
Regulated companies should consider the following measures to reduce concentration risks (see source for details):

- appropriate screening of the provider before outsourcing;

- shorter contract terms;

- Business continuity and insourcing plans;

- Distribution of outsourcing across multiple providers;

- Designation of secondary providers as replacements in case of interruptions.

In addition, procedures should be in place to regularly review the service provider's capabilities, its own business continuity, and emergency recovery measures (see source for details).

6. Access to data, premises and personnel and related control rights

a) Principle 6: A supervised entity should take appropriate measures to ensure that its supervisor, its auditors, and the supervised entity are able to obtain, upon request, promptly information about outsourced functions relevant to contractual compliance and/or regulatory oversight. Where necessary, access to data, IT systems, premises, and personnel of service providers related to the outsourced functions must also be possible.

The supervised entity retains full responsibility, legal liability, and accountability to the supervisory authority for all outsourced functions. Accordingly, the outsourcing agreements should stipulate immediate access by the supervisory authorities to relevant premises and responsible personnel of the service provider. The supervisory authority's expectations regarding the form and language of information provision must be met (see source for details).

b) Implementation
The following measures may be relevant (see source for details):

- Contractual provisions governing electronic or physical access to the service provider's data, premises, systems, software, algorithms and procedures;
- joint audits or assurances regarding compliance with regulatory requirements;
- Obligation of the service provider to provide the supervisory authority with accounting documents and other information relating to the outsourced task;
- Ensuring access by the supervisory authority even after the outsourcing has ended;
- Contractual agreement prohibiting the deletion, destruction or prevention of the availability of the data by the service provider.

7. Termination of outsourcing agreements
a) Principle 7: A regulated entity should include written provisions on the termination of outsourced functions in its contracts with service providers and ensure that it implements appropriate exit strategies.
This should include the grounds for contract termination and procedures for transferring the activity to the outsourcing company or third parties (e.g., the service provider's ownership or retention rights). Supervised entities should be aware that implementing an exit plan can be complex and time-consuming, and exercising termination agreements can be difficult. Furthermore, the termination of external and internal group processes can vary, so exit strategies should take this into account (see source for details).
b) Implementation
The following contractual conditions could be considered (see source for details):

- Termination rights, e.g. in the event of insolvency, liquidation, change of ownership or breach of contract;
- Notice periods for orderly (data) transfer;
- clear definition of who is entitled to the intellectual property after the contract ends;
- Support for the transfer by the service provider.

III. Appendix
In Annex A of these Principles, IOSCO explains the outsourcing practices of credit rating agencies and their use of cloud computing (see source for details).

CATEGORIZATION

Keywords
Retention obligation, record-keeping obligation, supervisory authority, outsourcing, outsourcing management, exit strategy, supervised company, cloud computing, cloud technology, cybersecurity, data retransmission, data security, data availability, data protection, service provider, service, service provider, disaster recovery, due diligence, exit strategy, intellectual property, IT system,

Information security, continuity, concentration risk, criticality, data misuse, business continuity plan, recovery, outsourcing, outsourcing agreement, rating agency, key function, monitoring measure, confidential information, confidentiality, essential outsourcing, sub-outsourcing, materiality, resilience, critical outsourcing, access

Legal and information bases

- Outsourcing Principles for Market Intermediaries (2005)
- Outsourcing Principles for Markets (2009)

Related Standards

- Outsourcing Principles for Market Intermediaries (2005)
- Outsourcing Principles for Markets (2009)

Target group – credit institutions
Yes

Target group – financial services institutions
Yes

Target group – Other companies in the financial sector
Yes

Target group – payment institutions
No

Target group – insurance companies
No

Target group – supplement

Comments

Statement by (date)

Implementation status Explanation
Final report

Status – Further Details
Final report

Date of entry into force/publication
October 27, 2021

Entry into force estimated?
No

Date of first application

October 27, 2021

Application appreciated?

No

Date Standard repealed

Remark (Entry into force/Publication)

Comments

Sources

The sources are not shown in this working paper.