Principles on Outsourcing. IOSCO Final Report. International Bulletin, March 2022.

IOSCO has published a report analysing recent developments in outsourcing by participants in the securities markets and to update the existing IOSCO Principles on Outsourcing to address these developments. Committee 2 on Secondary Markets (C2), Committee 3 on the Regulation of Financial Intermediaries (C3), Committee 6 on Credit Rating Agencies (C6), and Committee 7 on Derivatives (C7) participated in the preparation of this document.
The IOSCO Report proposes seven outsourcing principles, which are based on the earlier 2005 Outsourcing Principles for Market Intermediaries and the 2009 Outsourcing Principles for Markets, but their application is expanded to trading venues, market intermediaries, market participants acting on a proprietary basis and credit rating agencies. It is also suggested that their application be considered by financial market infrastructures.

These revised outsourcing principles are encompassed in a specific framework, the elements of which are set out below:

Scope of application

The Outsourcing Principles apply to regulated entities that fall within the purview of IOSCO Committees 2, 3, 6 and 7, i.e. trading venues, market intermediaries, market participants acting on a proprietary basis and regulated credit rating agencies.

The Principles do not address financial market infrastructures, which are already covered by the CPMI-IOSCO Principles for Financial Market Infrastructures. However, it is suggested that financial market infrastructures consider applying some or all of the principles set out in this Report to themselves or to those parts of their infrastructure that are not formally covered by the CPMI-IOSCO Principles, in particular with respect to areas that are recent developments or not otherwise covered by existing material.

Definition of Outsourcing

The Report defines outsourcing as a business practice in which a regulated entity uses a service provider to perform tasks, functions, processes, services or activities that would otherwise be undertaken by the regulated entity itself.

Legal responsibility

The regulated entity retains full responsibility, legal liability and accountability to the regulator for all tasks that it may outsource to a service provider to the same extent as if the service were provided in-house. Moreover, outsourcing must not be permitted to impair the regulator’s ability to perform its functions, including the proper supervision and examination of the regulated entity.

Possible risks deriving from outsourcing processes

The Report mentions several risks related to outsourcing processes, such as the risk of loss of control, increased exposure to cyberattacks and operational risks, the risk of concentration or reduced competition among companies that provide the outsourced services, and the increased risks to adequate supervision by market regulators.

Materiality or criticality of outsourced services

The Principles proposed in the Report must be applied according to the degree of materiality or criticality of the outsourced task. To this end, the regulated entity must develop processes that enable it to determine the materiality or criticality of the tasks it is seeking to outsource.

Group companies

The Outsourcing Principles apply whether the outsourced tasks are performed by a member company of the regulated entity's group or by an entity that is external to the corporate group.

Cross-border outsourcing

The Outsourcing Principles apply to the tasks that a regulated entity outsources both within its jurisdiction and on a cross-border basis.

Sub-outsourcing

Companies that offer outsourcing services may in turn subcontract these services to other providers, providing this practice does not negatively affect the quality of the service provided or cause a material increase in risks.

Concentration of outsourcing tasks

When a large number of regulated entities use the same service provider, operational risks become concentrated and may increase to the point that they present a systemic risk.

In the context of the concepts set forth above, the seven Principles proposed in the Report establish the expectations for regulated entities that outsource tasks, as well as providing useful information for their practical application.

The Principles proposed by IOSCO in this Report in relation to service outsourcing processes are as follows:

Principle 1: A regulated entity should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.

It is important for regulated entities to exercise due care and diligence in selecting their service providers. In this regard, they must ensure that the suppliers have sufficient capacity to perform the outsourced task effectively at all times.

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

A legally binding contract is the critical element that underpins relations between the regulated entity and the service provider. Contractual provisions can reduce the risks of non-compliance and facilitate the resolution of possible disagreements about the scope, nature and quality of the services to be provided. The existence of a written contract also facilitates the supervision of the outsourced tasks by the entity and the regulators.

Principle 3: A regulated entity should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.

The security, effectiveness and resilience of the IT systems of regulated entities are essential for financial markets. Connections to suppliers that do not have sufficient security measures in their systems can cause significant risks, which could jeopardise the privacy of investors and the confidentiality of information as well as seriously damage the reputation of regulated entities and cause a loss of market confidence in them.

Principle 4: A regulated entity should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients from intentional or inadvertent unauthorised disclosure to third parties.

Unauthorised disclosure of confidential information of regulated entities or their clients could have serious consequences, including harm to clients and investors, damage to the reputation of the regulated entity, potential financial loss or unwanted disclosure of trade secrets.

Principle 5: A regulated entity should be aware of the risks posed and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.

Concentration risks arise when a regulated entity relies heavily on a single service provider, or when a large

number of regulated entities rely on a single provider or a small number of service providers. When several regulated entities use a common service provider, operational risks are concentrated and can pose a threat of systemic risk in the markets.

Principle 6: A regulated entity should take appropriate steps to ensure that its regulator, its auditors and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.

Regulated entities must provide regulators with quick and complete access to this information, so that they can carry out the inspections, investigations and supervision tasks they deem appropriate. The scope of supervision should not be affected by a regulated entity's decision to engage a service provider. Besides, regulated entities retain full accountability to the regulator for outsourced tasks, to the same extent as they would if the service had been provided in-house.

Principle 7: A regulated entity should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.

When a task is outsourced, the risk of continuity increases, since there are certain elements related to it, such as daily control, information management or employee training, for which the uninterrupted performance of the activity largely depends on the service provider's continuing in that role and performing that task. This risk must be addressed through an agreement between the regulated entity and the service provider, in which it is clearly determined when and how the contract can be terminated and the effects of its termination, while identifying measures that allow efficient management of the transfer of the task to the regulated entity itself or to a new service provider.

Finally, it is worth mentioning that the Report briefly addresses the impact of COVID-19 on outsourcing processes and the operational capacity of regulated entities, in addition to including an annex specifically focused on outsourcing processes in credit rating agencies.

Link of interest:

Principles on Outsourcing. IOSCO Final Report.