CENTRE DE DROIT
BANCAIRE ET FINANCIER

IOSCO

Best practices in outsourcing

Par Yannick Caballero Cuevas le 15 November 2021

The International Organization of Securities Commissions (IOSCO) recently published an update of the principles on outsourcing established in 2005 for market intermediaries and in 2009 for stock exchanges. This update is due to new technological developments and recent developments in the field of outsourcing.

Firstly, the personal scope of these principles has been broadened. They apply not only to the aforementioned entities, but also to trading platforms (in particular multilateral trading facilities), participants in the financial markets acting on their own account and rating agencies (hereinafter : regulated entities). The report also contains an in-depth analysis of the use of outsourcing and cloud computing by rating agencies.

The report then highlights the various risks of outsourcing for regulated entities. These include loss of control in the execution of outsourced tasks, increased risk of cyber incidents and data leakage, and risks to the operational resilience of regulated entities.

Seven main principles regarding outsourcing are proposed. These can be grouped into three categories, namely the principles regarding the selection of the service provider, the principles regarding the control and supervision of the provider and finally the principles applying to the termination of contractual relationships.

For the selection of service providers, the report recommends conducting an audit. This makes it possible, in particular, to identify potential conflicts of interest, to assess the service provider’s skills, to identify the tasks to be outsourced and to determine the cross-border risks associated with outsourcing. This audit will also facilitate the drafting of the contract, which will have to address the critical and material risks of the outsourced tasks, while providing for conflict rules regarding applicable law and legal jurisdiction.

With regard to the control and supervision of the service provider, the report recommends that regulated entities and their service providers take appropriate measures to protect customer data against any leakage and ensure the resilience of the system used. The proposed measures include the implementation of periodic backups, regular testing of the IT system to assess the effectiveness of cybersecurity measures, and the establishment of emergency procedures for the service provider or disaster recovery plans. These measures should take into account the various applicable laws, especially in the case of cross-border outsourcing.

Another principle that aids supervision is access on request to the data, computer systems, premises and personnel of the service provider. This access makes it possible to check that the outsourced task is being carried out properly with regard to the contract and the applicable regulations. Auditors and supervisory authorities of regulated entities should also have a right of access. It is therefore suggested that a contractual clause granting a right of inspection be included. It is foreseeable that the drafting of this clause will be the subject of tough negotiations, since the regulated entity will want to have the broadest right of inspection, while the service provider will limit it to what is strictly necessary in order to protect its business secrets. This issue could arise in relation to whether or not to access in-house algorithms used by the service provider to perform outsourced tasks.

Finally, the report recommends including contractual clauses that determine when termination can be effected, under what conditions and when the termination takes effect. These clauses make it possible to establish a transitional period before the end of the contractual relationship. The parties will also have to provide for procedures for the transfer of data to the regulated entity as well as their deletion.

In conclusion, these principles are nothing revolutionary, but they clarify the good practices to be adopted when a task is outsourced to a service provider. Moreover, it is clear that major principles in the field of information security are becoming essential, such as the resilience of systems in the face of cyber-incidents. These principles can therefore inspire more than one institution when outsourcing its tasks.
