July 2020

ESMA Draft Guidelines on Outsourcing to Cloud Service Providers

NOTE: This briefing note is intended as general guidance and no action should be taken in reliance on it without specific legal advice.

Introduction

A significant level of guidance on outsourcing is being published by National and International regulatory authorities as concern increases around the management of outsourcing risk.

The International Organization for Securities Commissions (IOSCO) launched a Consultation on Outsourcing Principles to ensure operational resilience in May. The UK FCA is conducting a Consultation on Operational Resilience.

At a European level, the EBA (European Banking Authority) published Guidelines on Outsourcing Arrangements that came into force in September 2019. EIOPA (European Insurance and Occupational Pension Authority) recently published Guidelines on Outsourcing to Cloud Service Providers and as outlined within this briefing paper, on June 3rd ESMA published a consultation paper on outsourcing to cloud service providers.

Whilst drafting the guidelines, ESMA has considered the existing EBA and EIOPA guidelines. There are commonalities across the guidelines, however, there are material differences that will create a challenge for dual-regulated firms.

ESMA's draft guidelines are intended to help FS firms identify, address, and monitor the risks that may arise from their cloud outsourcing arrangements; from making the decision to outsource, selecting a cloud service provider, monitoring outsourced activities to providing for exit strategies.

Steven Maijoor, ESMA Chair, said:

"Cloud outsourcing can bring benefits to firms and their customers, for example, reduced costs and enhanced operational efficiency and flexibility. It also raises important challenges and risks that need to be properly addressed, particularly in relation to data protection and information security.

Financial markets participants should be careful that they do not become overly reliant on their cloud services providers. They need to closely monitor the performance and the security measures of their cloud service provider and make sure that they are able to exit the cloud outsourcing arrangement as and when necessary." Today's proposals will help firms understand and mitigate the risks that they are exposed to when outsourcing to cloud service providers."

The Scope

The guidelines apply to:

- Investment Firms and Credit Institutions
- Alternative Investment Fund Managers (AIFMs) and depositaries of AIFs
- UCITS and depositaries of UCITS
- Central Counterparties (CCPs), including Tier 2 third-country CCPs
- Trade Repositories (TRs) and Data Reporting Services Providers (DRSPs)
- Trading Venues and Central Securities Depositories (CSDs)
- Credit Rating Agencies (CRAs)
- Securitisation Repositories (SRs)
- Administrators of Benchmarks

ESMA has taken into account the principle of proportionality when drafting these guidelines. For example, the guidelines differentiate between critical or important functions and noncritical functions as outlined in the EBA Guidelines to take into account the risk underlying the outsourcing of those functions.

Key Dates

- **Consultation responses due 1st September 2020**
- These guidelines will apply from **30 June 2021** to all cloud outsourcing arrangements entered into, renewed, or amended on or after this date.
- Firms should review and amend existing cloud outsourcing arrangements with a view to ensuring that they take into account these guidelines by **31 December 2022**.
- Where the review of cloud outsourcing arrangements of critical or important functions is not finalised by 31 December 2022, firms will be expected to inform their competent authority of this fact, including the measures planned to complete the review or the possible exit strategy.

Definitions

Critical or Important Functions: means any function whose defect or failure in its performance would materially impair:
a) a firm's compliance with its obligations under the applicable legislation;

b) a firm's financial performance; or
c) the soundness or the continuity of a firm's main services and activities;

cloud services mean services provided using cloud computing;

cloud deployment model means the way in which cloud may be organised based on the control and sharing of physical or virtual resources. Cloud deployment models include community, hybrid, private and public clouds.

Focus

ESMA acknowledges that cloud outsourcing can bring certain benefits, including enhanced flexibility, operational efficiency, and cost-effectiveness, with potential positive outcomes for firms and investors. Yet, cloud outsourcing comes with risks that need to be properly identified, monitored and mitigated, as outlined below. It is the firm's responsibility to identify and implement effective ways to manage risks in relation to the use of cloud services

The proposed guidelines set out:

Strategy, governance and oversight
Responsibility for the governance and ongoing oversight of Cloud Service Providers (CSPs) outsourcing arrangements need to be clearly assigned and documented.

This includes the need to maintain a register of all cloud outsourcing arrangements distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements. For critical or important functions, the guidelines outline the minimum set of information that should be maintained. This includes details of 4th party (sub-outsourcer) details.

Due diligence and risk assessment
Before entering into any cloud outsourcing arrangement a proportionate level of due diligence should be undertaken taking into account operational, legal, compliance, and regulatory risk.

Contractual Arrangements
For critical and important functions the guidelines set out terms that should be included within a contract. These include the right for the FS firm to monitor the CSPs performance on a regular basis and for its competent authority to audit the CSP.

Information security and disaster recovery risk
The CSP's adherence with agreed Information security policies and procedures should be monitored on an ongoing basis.

Exit Strategies
A firm should ensure that it is able to exit cloud outsourcing arrangements without undue disruption to its business activities and services to its clients. For critical and important functions, an exit plan needs to be maintained and tested, based on scenarios such as the CSP failing.

Access and Audit Right
A firm should ensure that the cloud outsourcing written agreement does not limit the firm's effective exercise of the access and audit rights as well as its oversight options on the CSP.

Sub-outsourcing
For critical or important functions, firms need to be aware of all sub-outsourcing (fourth party) arrangements in place and have the right to object to any proposed changes.

Written notification to competent authorities
The guidelines set out that firms are required to notify their competent authorities in a timely manner with details of all critical or important cloud outsourcing arrangements.

Queries and Follow-Ups

The full consultation paper can be found here:
https://www.esma.europa.eu/sites/default/files/library/esma50-164-3342_cp_cloud_outsourcing_guidelines.pdf

For questions on the consultation or our service please contact one of the team
Email: contact@adoptech.co.uk

About Adoptech

Adoptech was founded to break down the barriers to technology adoption

Consumers gain the confidence to accelerate their adoption of innovative technologies and benefit from more efficient third-party risk management. Technology vendors benefit from shorter sales cycles, efficient assessments, and access to our vendor toolset that supports the adoption of best practices, reducing risk and increasing sales.