JAN 2020

EBA Guidelines on outsourcing

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

Introduction

European and UK supervisory authorities have made their intent to increase their focus on operational resilience and outsourcing risk clear. With UK supervisory authorities stating that the operational resilience of firms is no less important than financial resilience.

Financial institutions increasingly adopt third-party technology solutions in order to access technology talent and tap into cutting-edge technology, at an economically viable rate. This has changed the risk profile of financial services, with greater risk now sitting with unregulated third-parties. As a result, regulators globally are issuing additional guidance and implementing new rules. This briefing note outlines the EBA (European Banking Authority) guidance which the UK and EU authorities have adopted. The UK FCA has indicated that they will expand on the EBA guidelines, "*We want to have a consistent analytical capability on the amount and type of outsourcing that firms are undertaking*".

The Scope

EBA Guidelines on Outsourcing were published in Feb 2019. The Guidelines set out a new harmonised governance framework for outsourcings, including cloud outsourcings in one document.

The harmonised framework applies to all financial institutions that are:

- Within the scope of the EBA's mandate, including credit institutions
- Investment firms subject to (Capital Requirements Directive)
- Payment institutions
- Electronic money institutions

In summary: all banks, building societies, designated investment firms (authorised persons) and IFPRU investment firms (collective portfolio management firms).

The Guidelines take into account and harmonise requirements under:

- Capital Requirement Directive (2013/36/EU)
- MiFID II (Markets in Financial Instruments Directive 2014/65/EU)
- PSD2 Revised Payment Service Directive
- Outsourcing to cloud service providers (Dec 2017)
- Electronic Money Directive; EMD
- Bank Recovery and Resolution Directive

The Guidelines replace - Committee of European Banking Supervisors (CEBS) guidelines on outsourcing (2006).

Key Dates

- The Guidelines came into force on **30 September 2019**
- Outsourcings entered into, reviewed, or amended after 30 September 2019 must comply with the Guidelines
- Existing outsourcing arrangements, other than for outsourcing arrangements to cloud service providers, should be updated following the first renewal date of each existing outsourcing arrangement, but by no later than **31 December 2021**

Focus

- There is effective day-to-day management and oversight by the management team.
- There is a sound outsourcing policy and there are sound outsourcing processes.
- Institutions and payment institutions have an effective and efficient internal control framework, including with regard to their outsourced functions.
- All the risks associated with the outsourcing of critical or important functions are identified, assessed, monitored, managed, reported and, as appropriate, mitigated.
- There are appropriate plans for the exit from outsourcing arrangements of critical or important functions, e.g. by migrating to another service provider or by reintegrating the critical or important outsourced functions; and
- Competent authorities remain able to effectively supervise institutions and payment institutions, including the functions that have been outsourced.

Definitions

Outsourcing: "Outsourcing means an arrangement of any form between an institution, a payment institution or an electronic money institution and a service provider by which that service provider performs a process, a service or an activity that would otherwise be undertaken by the institution, the payment institution or the electronic money institution itself."

Critical or Important Functions: Based on the wording within MiFID II. "An operational function shall be regarded as critical or important where a defect or failure in its performance would materially impair the continuing compliance of an investment firm with the conditions and obligations of its authorisation or its other obligations under Directive 2014/65/EU, or its financial performance, or the soundness or the continuity of its investment services and activities'."

Key points

- Guidance is risk weighted, that is, services deemed critical or important require greater oversight.
- A written outsourcing policy is required to cover the principles, responsibilities and processes applicable to all phases of the outsourcing.
- An outsourcing register needs to be maintained.
- Pre-contract due diligence and risk assessments must be undertaken.
- Vendor contracts should grant firms and regulators full access and unrestricted audit rights.
- Institutions should have in place, maintain and periodically test appropriate BCP plans with regard to outsourced critical or important functions.
- Due diligence should be undertaken to ensure that the service provider has the business reputation, appropriate and sufficient abilities, the expertise, the capacity, the resources (e.g. human, IT, financial), the organisational structure and, if applicable, the required regulatory authorisations/registrations to perform the critical or important function in a reliable and professional manner to meet its obligations.
- The monitoring and governance framework for engagement between the firm and service provider needs to be clear and reflected in the outsourcing agreement.
- Requirement to document cost, benefit and risk analysis including:
    - Concentration risk
    - Over-reliance on outsourcing of critical or important functions
    - Step-in risk
    - Chain outsourcing
- Intra-group outsourcings are subject to the same risk assessments.
- The guidance outlines a list of grounds for termination that should be included in all outsourcing agreements.
- For critical or important functions firms also need to have documented the exit strategy. The overarching requirement to ensure that firms are able to exit without undue disruption/impact on continuity of service to clients.

Queries and Follow Ups

Adoptech provides products and consultancy services that support firms in their adoption of technology, reduction of outsourcing risk and compliance with regulations.

Contact one of our Third-Party Risk Management specialists:
Email: TPRM@adoptech.co.uk

JAN 2020