EBA CP on draft Guidelines on outsourcing
Public hearing 4 September 2018

European Banking Authority

EBA CP on Guidelines on Outsourcing

Consultation paper published 22 June 2018

Consultation runs until 24 September 2018, comments to be submitted via the EBA's website

- Guidelines update the 2006 CEBS Guidelines on Outsourcing (applicable to credit institutions only) and integrate the 2017 Recommendation on outsourcing to cloud service providers, which will both be repealed when EBA GL on Outsourcing enter into force

Definition

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, or parts thereof that would **otherwise be undertaken by the institution**, the payment institutions or the electronic money institution itself.

Scope of outsourcing

- In line with MiFID and Commission delegated Regulation (EU) 2017/565 and PSD the Guidelines deal with the **outsourcing of operational functions** (i.e. excluding the final responsibility)
- Guidelines differentiate requirements for the outsourcing of:
  - Critical or important operational functions
  - Other operational functions (with a less strict requirements)
- GL aim at avoiding “empty shells” _ e.g. resulting from back to back business models
- The acquisition of services (e.g. advice of an architect regarding the premises, servicing of company cars), goods (e.g. purchase of office supplies, company cars or furniture) or facilities (e.g. electricity, water, gas, telephone line) that are not normally performed by institutions themselves are **not considered outsourcing**.

Outsourcing of authorised services

Outsourcing of activities to an extent that requires authorisation itself (outsourcing of parts of operational processes not covered)

- It always must be possible for the home competent authority to conduct effective supervision of the institution, including their outsourced processes, services or activities.
- Regarding outsourcing of banking and payment services to third countries additional safeguards are introduced (investment services regulated via COM delegated Regulation)
  - The service provider is authorised and subject to supervision
  - The existence of a cooperation requirement in the form of a memorandum of understanding that ensures effective supervision
  - In any case the institution must ensure access and audit rights

Governance requirements

All institutions must have robust governance arrangements

- Institutions should retain an appropriate internal organisation at the head office to oversee and manage the relationship with service providers
- Where operational task of internal control functions are outsourced (e.g. in the case of intragroup outsourcing or outsourcing within institutional protection schemes), the institution should exercise appropriate oversight and be able to manage the risks that are created by such outsourcing and not unduly rely on controls performed by the service providers.

Internal audit function

Outsourced operational functions stay within the audit universe of the internal audit function

- The audit plan should include also the operational functions that have been outsourced, including the appropriateness of data protection measures, controls, risk management and business continuity measures implemented by the service provider.

The internal audit function should audit the institutions framework for outsourcing and the implementation of the outsourcing policy,

- including the outsourcing process,
- the risk assessment for outsourcing arrangements and that the risks stay within the risk appetite,
- the appropriate monitoring and management of outsourcing arrangements.

Access and audit rights

Outsourcing contracts must ensure access and audit rights at the service provider for the outsourcing institution and competent authorities and parties appointed by either of them, including:

- complete access to all its relevant business premises (head offices and operations centers), including the full range of devices, systems, networks, information and data used for providing the outsourced service, financial information, personnel and the service provider's external auditors ('access rights'); and
- unrestricted rights of inspection and auditing related to the outsourced services ('audit rights').

Critical or important outsourcing (replaces term material OS)

In line with Regulation (EU) 2017/565 institutions should always consider an operational function as critical or important where a defect or failure in its performance would materially impair:

- their continuing compliance with the conditions of their authorisation or regulatory obligations under CRD/CRR and/or PSD ;
- their financial performance; or
- soundness or continuity of their banking, investment and payments services and activities.

Outsourcing arrangements should always be considered critical or important, if they:

- concerns the operational functions of internal control functions;
- carries a high degree of operational risk individually or collectively when assessed together with other outsourcing arrangements with the same service provider and outsourcing arrangements regarding the same business area.

Risk assessment

Institutions to assess all risks before outsourcing and as part of their monitoring, the guidelines have a focus on operational and reputational risks

- Institutions should assess the impact of the outsourcing based on scenario analysis (considering loss data where available)
- Assess the risk related to data (GDPR and accessibility, integrity, security)
- Identifying concentration risks (multiple outsourcings in one area or to one provider)
- Institutions to consider the risk that may result from sub-outsourcing

Documentation requirements

The institution should maintain a register of all outsourcing arrangements and be able to submit it in a common data base format (frequency 1 – 3 years in line with SREP)

- Register should distinguish outsourcing of critical or important operational functions and other outsourcing arrangements; extent of documentation differs, but all outsourcings are to be documented
- Separate timely information of the competent authority required for new critical or important outsourcing
    - New planned outsourcing of critical or important functions
    - Existing outsourcing that became critical or important
    - Material events or changes that could have a material impact on the continuing provision of the business activities

Questions and comments

EUROPEAN BANKING AUTHORITY

Floor 46, One Canada Square, London E14 5AA

Tel: +44 207 382 1776
Fax: +44 207 382 1771

E-mail: info@eba.europa.eu
http://www.eba.europa.eu