Time to re-examine outsourcing

30 September 2019

The revised European Banking Authority (EBA) outsourcing Guidelines take effect today. They apply to credit institutions and investment firms subject to the Capital Requirements Directive (CRD) as well as payment and electronic money institutions; they are also indirectly relevant to service providers for those firms.

The Guidelines harmonise the framework for outsourcings by those categories of financial services firm. They apply to arrangements "entered into, reviewed, or amended" on or after 30 September 2019. They replace those from 2006 published by the EBA's predecessor, the Committee of European Banking Supervisors (CEBS), although those only applied to credit institutions. They also replace and incorporate the EBA's final recommendations on outsourcing to cloud service providers. So, relevant financial services firms now need only consult one set of guidelines for cloud and non-cloud outsourcings.

Main themes

There are already regulatory expectations around the management of third party operational relationships in financial services, including outsourcings. In the UK, the FCA Handbook and PRA Rulebook has contained requirements and guidance on this topic for many years. The content of the Guidelines will therefore be familiar to most regulated firms and are consistent with provisions of the second Payment Services Directive, MiFID II and the CRD. They may nonetheless require some firms to review and amend their existing outsourcing arrangements to address any apparent gaps or shortfalls in light of the Guidelines.

What is an outsourcing for these purposes?

The definition of an outsourcing is derived from Commission Delegated Regulation (EU) 2017/565 and is defined as: *"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."*

The acquisition of services *"that would otherwise not be undertaken by the institution or payment institution"*, goods or utilities is generally not considered to be an outsourcing for these purposes.

It is worth highlighting a few key messages:

- The Guidelines contain a transitional period, meaning all documentation requirements should be completed after the first renewal date but no later than 31 December 2021. Where the

review of outsourcing arrangements of "critical or important functions" is not finalised by 31 December 2021, institutions and payment institutions should "inform their competent authority of that fact, including the measures planned to complete the review or the possible exit strategy."

- The outsourcing of "critical or important functions" is subject to stricter requirements than other outsourcing arrangements, but the Guidelines apply generally to all outsourcings by relevant entities, including intra-group outsourcings.

Critical or important functions

The Guidelines define "critical or important functions" in line with MiFID II and Commission Delegated Regulation (EU) 2017/565. Consideration should be given to whether "a defect or failure" in the performance of a function being outsourced would "materially impair" regulatory compliance, financial performance or business continuity. Firms are expected to assess for themselves whether outsourced functions meet the "critical or important" threshold.

- Not every outsourcing to a cloud solution provider is "critical or important", according to the EBA. The same test applies as with other non-cloud service providers, albeit taking into account "cloud specificities". The ability of a cloud service provider to protect the confidentiality, integrity and availability of data (in transit or at rest) is regarded as particularly important.

- Firms that outsource critical or important functions intra-group must be able to demonstrate that they have selected the group entity based on objective reasons; the conditions for those arrangements should be arm's length, addressing any conflicts of interest considerations.

- A firm's management remains responsible for all of its activities, so should ensure that there are sufficient resources to oversee and manage appropriately the risks and relationship aspects of any outsourcings. This responsibility cannot be delegated, even if the services relied upon are standardised or offered by a single or small number of providers, such as web hosting and cloud storage services. (In the UK, executive oversight is encouraged through the allocation of responsibility for outsourcing to a Senior Manager.)

- Firms are to maintain, review and update a comprehensive outsourcing policy. All outsourcings must be documented in a register, accessible by regulators, with more information required for the outsourcing of critical or important functions. The rights and obligations of the parties should be set out in a written agreement, with certain minimum mandatory details prescribed in the Guidelines.

- In many cases, the EBA allows for firms to use third-party certifications and reports made available by the service provider, but not as a substitute for audits; "pooled audits" (i.e. organised jointly with clients of the same service provider) may be used subject to conditions.

- The Guidelines neither require nor prevent competent authorities from applying a prior approval process for outsourcing arrangements but at a minimum there should be some form of supervisory dialogue when a firm plans to outsource a "critical or important function" and/or where an outsourced function has become "critical or important".

Comment

Third party service providers are a common feature in the operations of financial services firms in Europe. The Guidelines make clear that risks resulting from third party arrangements need to be identified, assessed, monitored and managed, regardless of whether they amount formally to an outsourcing. This theme can best be considered in the context of an increasing regulatory focus on "operational resilience" (i.e. how firms and other market participants are taking steps to maintain the continuity of their most important business services).

The Guidelines, together with recent FCA and PRA fines for failure to manage outsourcing risk (see box), act as a timely reminder for all financial services firms to revisit their existing outsourcing arrangements.

Recent Regulatory Fines

The FCA and PRA investigation into Raphaels Bank earlier this year culminated in fines for the bank's failures to manage its outsourcing arrangements effectively. The PRA said: "*Raphaels' specific failings … resulted from deeper flaws in its overall management and oversight of outsourcing risk from Board level down. … Firms' ability to manage outsourcing of any critical activities is a vital part of maintaining their safety and soundness. Such outsourcing is an important part of a firm's operational resilience, and particularly so in the case of Raphaels given the level of reliance on outsourcing in its business model.*"

The Guidelines will also be of interest to the technology service providers who supply to financial services firms. Such suppliers are not directly caught by their remit, despite an ongoing debate as to whether dominant technology providers could present a systemic risk to the financial system such that they should become subject to direct regulatory oversight. However, they should be aware that their financial services customers may now need to examine their existing contractual and operational requirements (e.g. on sub-contracting, access and audit rights), as well as new arrangements, in light of the Guidelines.

At a glance, the Guidelines aim to ensure:

- effective day-to-day management and oversight by the management body of the outsourcing firm;
- a sound outsourcing policy and processes that reflect the institution's strategy and risk profile;
- an effective and efficient internal control framework;
- proper identification of critical or important functions and suitability of potential service providers;
- that all the risks associated with the outsourcing of critical or important functions are identified, assessed, monitored, managed, reported and, as appropriate, mitigated;
- protection of customer data across the whole institution, including the outsourced functions;
- 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.

If you have any queries relating to the Guidelines or outsourcing generally, please contact a member of the team below or your usual Slaughter and May contact.

Duncan Blaikie
T +44 (0)20 7090 4275
E duncan.blaikie@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com

Selmin Hakki
T +44 (0)20 7090 5153
E selmin.hakki@slaughterandmay.com

Ben Kingsley
T +44 (0)20 7090 3169
E selmin.hakki@slaughterandmay.com

© Slaughter and May 2019. This material is for general information only and is not intended to provide legal advice. For further information, please speak to your usual Slaughter and May contact.

561786174