Outsourcing

Supervision of outsourcing at financial institutions becomes more extensive, also impacting service providers including payment service providers

Service providers of payment and account information services are required to obtain a license issued by De Nederlandsche Bank (hereafter DNB) or by another supervisory authority in the European Union. The license application process covers various topics. One topic that is increasingly receiving attention from the supervisory authority in the application process is outsourcing. With the introduction of the "EBA Guidelines on outsourcing arrangements" (2019), the requirements for financial institutions on how to enter into, monitor and control outsourcing relationships became more stringent. Ensuring compliance with these guidelines and associated laws and regulations is key for payment service providers to obtain their license in a timely manner.

Kiruna Boll-van Schip MSc RA
is Manager Risk & Regulatory FRM at KPMG Netherlands.
vanschip.kiruna@kpmg.nl

Maarten Visser MSc
is Manager Digital Sourcing at KPMG Netherlands.
visser.maarten@kpmg.nl

INTRODUCTION

On 30 September 2019, the "guidelines on outsourcing arrangements" (hereafter Guidelines) of the European Banking Authority (hereafter EBA) entered into force. The Guidelines ([EBA19]) describe the way in which financial institutions enter into, monitor and control outsourcing relationships. All outsourcing agreements entered into on or after this date must comply with the new Guidelines. Existing outsourcing agreements are subject to a transitional regime, whereby the agreements must be adapted in accordance with the Guidelines on the next occasion when the contract can be awarded, in any case before 31 December 2021. Refer to Figure 1 for a graphic overview of the timeline.

The General Data Protection Regulation (Regulation (EU) 2016/679) also includes provisions on the management of third parties strictly applicable to financial institutions, which have been woven into the Guidelines without adding any specific new data obligations. Hence, it is imperative for financial institutions to ensure that personal data are adequately protected and kept confidential when outsourcing for example IT, Finance, data or payment services.

Ensuring compliance with these Guidelines and associated laws and regulations is key for payment service providers to obtain their license in a timely manner. This applies specifically and is not limited to sound governance arrangements, third-party risk management, the due diligence process, the contractual phase, security of data and systems, outsourcing to cloud providers, access to information and audit rights.

This article will first outline the key requirements from the Guidelines for each phase of the outsourcing lifecycle before providing direction concerning the impact on the financial sector, including regulators, financial institutions and service providers.

COMPREHENSIVE OUTSOURCING GUIDELINES AT EUROPEAN LEVEL

Outsourcing is a popular way to gain access to (technological) innovations and economies of scale. However, outsourcing also creates new risks for financial institutions, third parties and regulators. The new Guidelines aim to identify, address and mitigate these risks.

The Committee of European Banking Supervisors (CEBS), the predecessor of the EBA, published outsourcing guidelines in 2006. These guidelines were repealed when the Guidelines entered into force on 30 September 2019. The new Guidelines also replace the EBA recommendations for outsourcing to cloud service providers published in 2018. With the new Guidelines on Outsourcing arrangements, the EBA is introducing harmonized guidelines, which will set a new standard for financial institutions within the EU. This is in line with the call from supervisory authorities for more overarching regulations instead of a complex collection of separate and local directives. In addition, more stringent requirements are introduced. For instance, financial institutions now have to report all outsourcing of critical or important functions whilst earlier this was only the case for outsourcing critical or important functions to cloud service providers. Table 1 shows an overview of new and repealed guidelines.

Table 1. Status guidelines and recommendations.

Guideline/recommendation	Status
EBA Guidelines on Outsourcing Publication year: 2019	Valid as of 30 September 2019
EBA Recommendation for Cloud Outsourcing Publication year: 2018	Repealed as of 30 September 2019
CEBS Guidelines on Outsourcing Publication year: 2006	Repealed as of 30 September 2019
DNB Guidelines (e.g. "Governance on Outsourcing" (updated 2020) and "Good practices for managing outsourcing risks" (2018))	Valid

Figure 1. Timeline implementation of EBA Guidelines on outsourcing arrangements.

GUIDELINES FOR OUTSOURCING: THE FINANCIAL INSTITUTION MUST NOT BECOME AN EMPTY SHELL

The Guidelines require that the outsourcing policy of financial institutions cover the full outsourcing lifecycle, with risks and responsibilities being addressed for each phase in the lifecycle. Figure 2 shows a graphic overview of the outsourcing lifecycle. In order to clearly indicate the requirements for each phase, the Guidelines consist of the following components:

A. Proportionality and group application
B. Assessment of outsourcing agreements
C. Governance framework
D. Outsourcing process

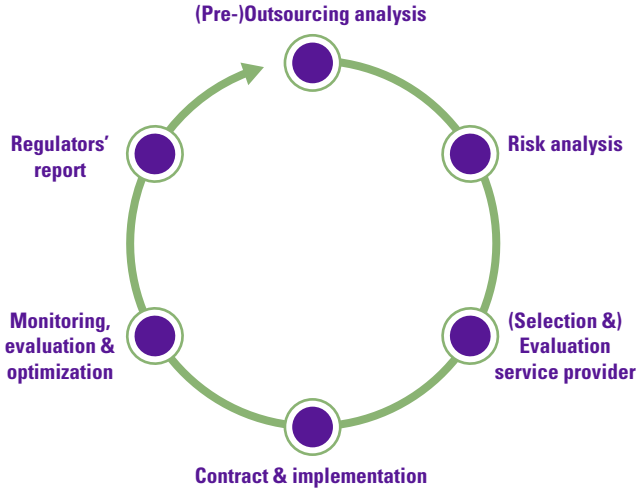


Figure 2. Outsourcing lifecycle.

In order to ensure full compliance with the guidelines in each phase of the outsourcing lifecycle, a detailed analysis should be performed to draft an approach for effective management of outsourcing risks. Each entity should assess which particular controls and measures are already in place and identify the gaps to the Guidelines. The KPMG control framework (see Figure 3) is an example of which aspects of the Guidelines are considered and which aspects can help you comply with the requirements of the new regulation.

Below you will find a short explanation of the most important requirements of the Guidelines.

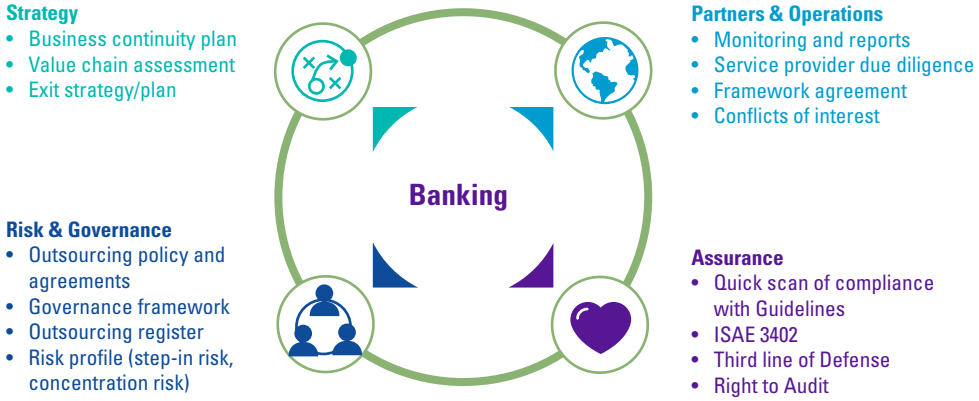
A. Proportionality and group application

The Guidelines apply to the entire corporate group and therefore also to its subsidiaries. This way, an adequate and consistent application of the Guidelines is imposed, also when subsidiaries are established outside the EU.

The Guidelines emphasize the principle of proportionality. Financial institutions that wish to outsource business activities are required to weigh up the nature, scale and complexity of these activities so that the outsourcing risks can be estimated, and appropriate measures can be implemented. However, this does not mean that the responsibility for the business activities can be transferred to the service provider. Both the Guidelines and regulator's publications emphasize the importance of financial institutions retaining responsibility. The EBA specifies that certain management tasks may never be outsourced, including determining the financial institution's risk profile and management decision making.

Even though ultimate responsibility will always remain with the governing body, financial institutions must ensure that a succession of outsourced activities is not created while they only retain final responsibility, a so-called "empty shell". Sufficient in-house knowledge and experience must be present to guarantee the continuity of the financial institution and to maintain effective supervision of (the quality of) the services offered by the service provider.

Figure 3. KPMG control framework.



B. (Re-)assessment of outsourcing agreements
In the first instance, it must be determined whether the activities qualify for outsourcing. The Guidelines stipulate that outsourcing exists when the outsourcing of activities is ongoing and recurrent in nature. One-off advice for a legal matter or the hiring of a third party for maintenance work on a building is therefore not considered as outsourcing. The EBA has also included a number of examples in the Guidelines of activities that are not considered as outsourcing, regardless of the recurrent nature:

- Outsourcing services that would otherwise not be carried out by the financial institution. These include cleaning services, catering and administrative support, such as mail rooms, receptions and secretariats;
- Outsourcing services that, due to the laws and regulations, are assigned to third parties (for example, an external accountant for auditing the annual accounts);
- Market information service providers, such as Bloomberg and Standard & Poor's;
- Clearing and settlement activities for securities transactions.

The Guidelines hold the financial institution responsible for having a proper outsourcing policy that addresses all aspects in detail. They contain extra requirements for the outsourcing of critical or important functions, and a thorough analysis of the outsourcing risks must be carried out. Furthermore, with intra-group outsourcing the "arm's length principle" must be followed, meaning that this should be carried out as if one were dealing with an independent third party.

Sufficient in-house knowledge and experience must be present to prevent the institution from becoming an "empty shell"

The Guidelines particularly focus on outsourcing to service providers that are established in cost competitive countries outside of the EU. Aspects that must be considered are, among others, social and ethical responsibility, information security and privacy, but also specifically consider the powers of local supervisors and the assurances that must be provided to ensure effective supervision (such as access to data, documents, buildings and personnel).

C. Governance framework
The Guidelines have strict requirements when it comes to the governance framework of financial institutions. Below are a number of framework conditions:

- Outsourcing may never lead to the delegation or outsourcing of responsibilities relating to the management of the financial institution;
- The responsibilities for the documentation, management and monitoring of outsourcing agreements must be clearly established in the outsourcing policy. This policy must be reviewed and/or updated on a regular basis;
- Business continuity and exit plans must be present for the outsourcing of critical or important functions. These plans must be tested regularly and revised where necessary. Sufficient in-house knowledge and experience must be present to guarantee the continuity of the company and prevent the institution from becoming an "empty shell";
- The internal audit function carries out an independent review of the outsourcing agreements and in doing so, follows a risk-based approach. It is important that conflicting interests are also assessed as part of the review. These must be identified, assessed and managed by management;
- An outsourcing register must be maintained that includes all the information about outsourcing agreements at group and entity level. This register is necessary for providing an accurate and complete report on outsourcing to the supervisory authorities.

D. Outsourcing process
The Guidelines describe the requirements for the outsourcing process. A number of framework conditions are briefly summarized below, whereby the Guidelines follow the outsourcing lifecycle:

- A pre-outsourcing analysis must be carried out before an outsourcing agreement is entered into;
- Before the outsourcing commences, the potential impact of the outsourcing on the operational risk must be assessed so that appropriate measures can be taken;
- Before entering into an outsourcing agreement, it should be assessed during the selection and assessment process whether the service provider is

suitable. The financial institution must also analyze where the services are being provided (in or outside the EU, for example);
- The rights and obligations of the financial institution and the service provider must be clearly assigned and established in a written agreement;
- The service provider's performance and the outsourcing risks must be continuously monitored for all outsourced services, with a focus on critical and important functions. Outsourcing of critical and important functions must be reported to the supervisory authority. Any necessary updates to outsourcing risks or performance should have appropriate change management controls in place;
- There must be a clearly defined exit strategy for the outsourcing of critical and important functions that is in line with the outsourcing policy and business continuity plans.

IMPACT ON THE FINANCIAL SECTOR

The new Guidelines do not only affect financial institutions, but also regulators and service providers. However, the impact of the Guidelines will vary between those who are affected.

Regulators will monitor a new form of concentration risk

Technological innovation is one of the key themes of DNB's "Focus on Supervision 2018-2022". The analysis of the consequences and emerging risks of a more "open" banking industry on the prudential and conduct supervision are strongly related to the publication of the new Guidelines on outsourcing arrangements.

In addition to the supervision of financial institutions, the new Guidelines make the DNB responsible for monitoring concentration risk. This risk arises when certain business activities are outsourced by different financial institutions to the same service provider. This can jeopardize the continuity and operational resilience of financial institutions when the service provider experiences (financial) problems. As outsourcing agreements are currently not, or not fully, registered centrally, there is currently no complete overview of the concentration risk.

In 2017, DNB conducted a thematic review of banks, investment firms and payment institutions into the scope and control of outsourcing risks. In June 2018, this resulted in the "Good practices for managing outsourcing risks", which explains, among other things, the requirement for financial institutions to report outsourcing of significant activities to the supervisory authority. Currently, DNB maintains a register of all ongoing outsourcing agreements to cloud service providers. The new Guidelines further expanded this reporting obligation to all outsourcing of critical and important functions in order to obtain a complete overview of (sub-)outsourcing by financial institutions. This enables the regulator to monitor the concentration of outsourcing and manage the concentration risk more effectively. Furthermore, it enables the DNB to monitor that no financial institutions are emerging where virtually all activities have been outsourced and the institution itself is no more than an "empty shell".

The Guidelines stress that financial institutions should include a clause in the outsourcing policy and agreement that gives the DNB and other supervisory authorities the right to carry out inspections as and when deemed necessary. Although this clause was already made mandatory in previous EBA guidelines, in practice, it appears that the clause is often not included in outsourcing agreements.

Financial institutions are reminded of their duty of care

The new Guidelines will have a major impact on financial institutions, whereby the problems and challenges can be divided into four general categories:

A. Retaining (ultimate) responsibility and preventing an "empty shell"
B. Operational resilience of financial institutions
C. Central recording of outsourcing and management information
D. Increasing competition for banks

A. Retaining (ultimate) responsibility and preventing an "empty shell"
To determine the tasks and responsibilities of both the financial institution and the service provider, the outsourcing policy must be evaluated and revised where necessary in order to ensure alignment with the Guidelines. Furthermore, it is recommended to appoint one responsible party (unit, committee or CRO) to monitor the risk and compliance with the regulations so as to manage the outsourcing risks effectively. It is therefore important that outsourcing agreements concluded with service providers are reviewed and adapted to ensure alignment with the requirements set out in the Guidelines.

B. Operational resilience of financial institutions
With the increasing interest in outsourcing business activities, a clear shift from operational risks to supplier risks can be seen. The concentration risk has already been briefly described above, but to an increasing extent there is also the step-in risk that the financial institution itself must provide support to help the service

provider remain operational when it finds itself in (financial) difficulty. This step-in risk must be evaluated prior to entering into an agreement and must be managed throughout the duration of the outsourcing and included in the Internal Capital Adequacy Assessment Process (ICAAP).

C. Central recording of outsourcing and management information
Analyses, inspections and surveys of supervisory authorities, among others, have shown that many institutions do not have a central outsourcing register and that management information concerning outsourcing is often sparse. Management often has insufficient insight into the scope of the outsourcing and the relevant risks. In order to fulfil the notification obligation to DNB, financial institutions must create and maintain their own outsourcing register. In addition, there is also the risk that the outsourcing of activities is wrongfully not considered as outsourcing. As a result, the outsourcing is not included in the outsourcing register and is not reported to the regulator. Finally, the assessment of whether functions are critical or important can be somewhat subjective and may lead to an incorrect categorization, with the danger being that the risks are not evaluated and managed according to the outsourcing policy.

D. Increasing competition for banks
In addition to the expansion and tightening of laws and regulations, the banking sector is also facing a rise in new entrants such as FinTech and BigTech companies. With the arrival of non-banking institutions that offer payment services and more, banks are facing increasing competition. A strategic choice can be made to outsource instead of innovating themselves, whereby faster and more efficient access to (technological) innovations can be obtained.

Necessary adjustments to comply with the Guidelines prove to be more complex and time-consuming than initially thought

Service providers are not excluded: new requirements set by the Guidelines

The new Guidelines will have a major impact not only on financial institutions, but also on service providers. Although they do not directly fall within the scope of the Guidelines, financial institutions are expected to impose the requirements on service providers in order to comply with the new Guidelines. As a result, FinTech companies and other entrants will face the challenge of remaining innovative and competitive in a rapidly changing market, while at the same time confronting the administrative challenges of (indirectly) complying with the Guidelines. In particular, implementing robust management processes and meeting (internal) documentation requirements can significantly increase the burden on emerging service providers.

IN SHORT, THE NEW GUIDELINES HAVE A FAR-REACHING IMPACT

The Guidelines have a far-reaching impact on the financial sector and on banks and their service providers, in particular. The governance framework of the institutions should be reviewed and possibly revised regarding several aspects to ensure compliance with the new regulations. In addition, with the increase in outsourcing of activities, it is becoming increasingly important for financial institutions to have good internal controls in place.

Built-in controls play an important role in this, such as the "three lines of defense"[1] model in which segregation of duties and monitoring by independent functions are maintained. Adapting the governance framework, outsourcing policy, processes, outsourcing agreements, etc. is time-consuming and needs to be done thoroughly, but above all, in a timely manner in order to avoid sanctions by supervisory authorities.

CONCLUSION

The Guidelines came into effect on 30 September 2019. It is therefore important that financial institutions and service providers carry out a detailed review of, among other things, the outsourcing policies and agreements and revise them where necessary in order to comply with the new Guidelines. Specifically for service providers of payment and account information services who find themselves in the license applications process, ensuring compliance with the Guidelines and associated laws and regulations is key to obtaining the license in a timely manner.

In practice, we see that organizations often underestimate the detailed review and that the necessary adjustments to comply with the Guidelines prove to be more complex than initially thought. Reviewing and adjusting the outsourcing policy is often not possible without an update of the governance policy, which creates the risk that parts are overlooked and inconsistencies occur between the various documents. It is therefore important that institutions carry out a timely and thorough review in order to avoid challenges due to time pressure and complexity.

In addition, we would like to stress that institutions must be careful not to become an "empty shell" due to the lack of substance. As described above, the institution must retain ultimate responsibility. With the new Guidelines, there will be a renewed regulatory focus on this area, with potentially far-reaching consequences if the conditions of the licenses are no longer met.

1 In the "three lines of defense" model, the risk management, compliance and actuarial function form the second line and the internal audit function forms the third line, while the operational business is conducted in the first line. In such an arrangement, the four key functions operate independently from the first line and from each other. The operationally independent functioning of key functions does not exclude effective cooperation with other (key) functions ([DNB18]).

References

[DNB18] De Nederlandsche Bank (2018). Operationeel onafhankelijke en proportionele inrichting van sleutelfuncties. Retrieved from: https://www.toezicht.dnb.nl/3/50-237420.jsp

[EBA19] European Banking Authority (2019, 25 February). Guidelines on outsourcing arrangements. Retrieved from: https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

About the authors

Kiruna Boll-van Schip MSc RA is Manager Risk & Regulatory FRM at KPMG Netherlands. She has over ten years of experience providing advisory and assurance services to both listed and non-listed clients within the Financial Services and Corporate sectors. In the last four years, Kiruna has been working at the KPMG Amstelveen and KPMG Sydney offices, providing advisory services to major and large banks in the Netherlands and Australia with a primary focus on non-financial risk management.

Maarten Visser MSc is Manager Digital Sourcing at KPMG Netherlands. In his work, Maarten is primarily focused on sourcing strategy and service provider selection engagements in both the public and private sector. In his role as advisor he emphasizes the value of business relationships and supports clients in their journey to move away from traditional client-supplier relationships towards effective partnerships.