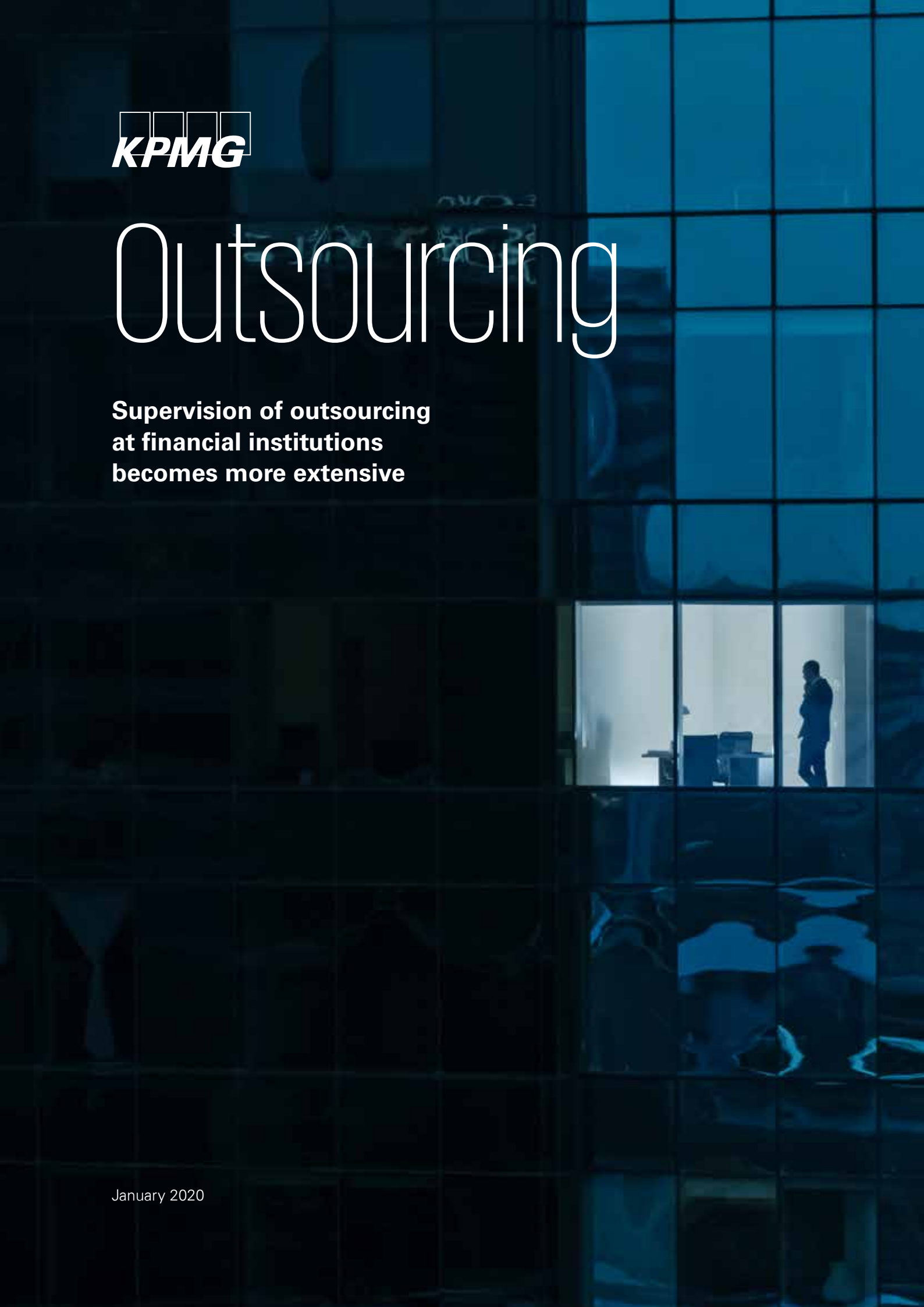
KPMG

Outsourcing

Supervision of outsourcing at financial institutions becomes more extensive



January 2020

Table of content

KPMG

1. New EBA Guidelines for outsourcing[1]

The European Banking Authority (EBA) published the final version of the "EBA Guidelines on outsourcing arrangements" (hereafter Guidelines) on 25 February 2019. The Guidelines describe the way in which financial institutions enter into, monitor and control outsourcing relationships and entered into force on 30 September 2019. 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 which the contract can be awarded, but in any case before 31 December 2021.

Kiruna van Schip
Manager |
Risk & Regulatory
FRM

Maarten Visser
Manager |
Digital Sourcing

Damien Misonne
Senior Manager |
Digital Enablement -
IT sourcing

[1] 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 IT or data services.
[2] Specifically, this applies, but is not limited, to sound governance arrangements and third-party risk management, the due diligence process and the contractual phase, security of data and systems, including outsourcing to cloud providers, access to information and audit rights. Ultimately, the aim is to ensure the protection of customer data across the entire institution, as well as the outsourced functions that financial institutions fall under within the scope of application of the GDPR.

KPMG

Comprehensive outsourcing guidelines at European level

1 — 25 February 2019
Final Guidelines published

2 — 30 September 2019
EBA Guidelines become applicable

3 — 31 December 2021
End of transition period for existing contracts

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 expired 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 updated Guidelines, the EBA is introducing harmonized outsourcing 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.

Guideline/Recommendation	Status
EBA Guidelines on Outsourcing Publication year: 2019	Valid as from 30 September 2019
Circular PPB_2004/5 on proper management practices relating to outsourcing by credit institutions and investment firms;	Repealed as from 30 September 2019
EBA Recommendation for Cloud Outsourcing Publication year: 2018	Repealed as from 30 September 2019
Communication NBB_2012_11 on prudential expectations regarding cloud computing	Repealed as from 30 September 2019
Communication of the CBFA of 6 November 2007 on its policy regarding the outsourcing of asset management services of assets of non-professional clients to a service provider in a State that is not a member of the European Economic	Repealed as from 30 September 2019

2. Guidelines for outsourcing: the financial institution must not become an empty shell

The Guidelines require that the outsourcing policy of financial institutions be consistent with the outsourcing life cycle, with risks and responsibilities being addressed on a stage-by-stage basis.

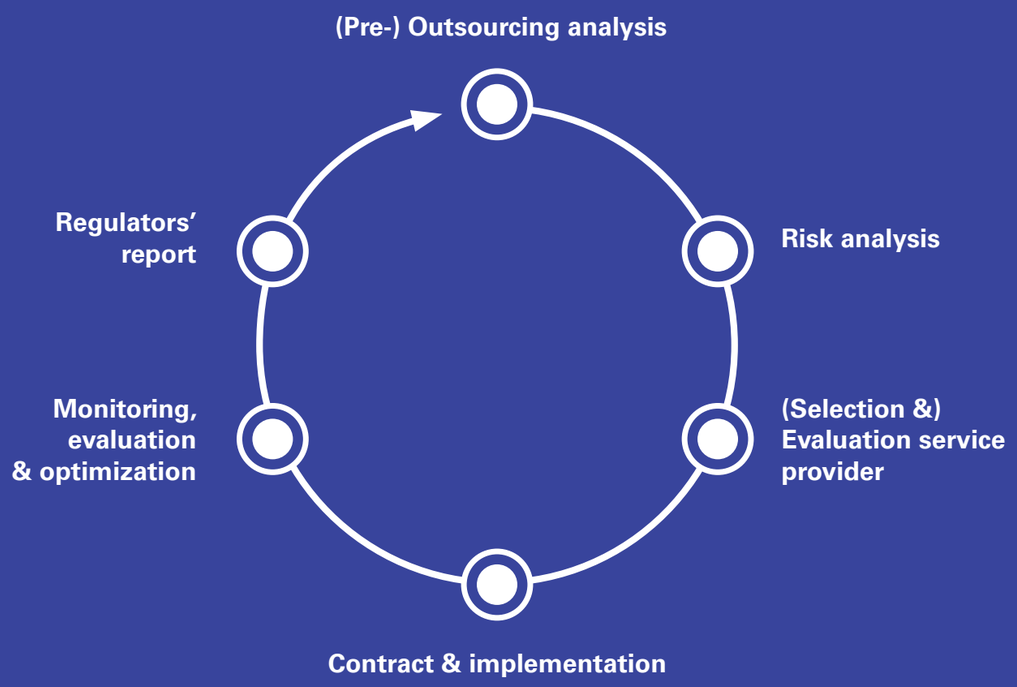
In order to clearly indicate the requirements for each phase, the Guidelines consist of the following components:

A. Proportionality and group application

B. Assessment of outsourcing agreements

C. Governance framework

D. Outsourcing process



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 the subsidiaries. In 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. This does not mean, however, 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 final responsibility will always remain with the administrative 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.

B. (Re-)assessment of outsourcing agreements

In the first instance, it must be determined whether outsourcing exists. The Guidelines stipulate that outsourcing exists when the outsourcing of activities is ongoing and recurrent in nature. One-time 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 not otherwise be carried out by the financial institution. These include cleaning services, catering and logistical 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 with 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 outsourcing critical or important functions, while 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.

The Guidelines primarily focus on outsourcing to service providers that are established in third world countries. Aspects that must be considered concern, among others, social and ethical responsibility, information security and privacy, but also specifically concern 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 financial institutions' governance framework. 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 here. These must be identified, assessed and managed by management;

— Before entering into an outsourcing agreement, it should be assessed whether the service provider is suitable during the selection and assessment process. The financial institution must also analyze where the services are being provided (in or outside the EU, for example). With special attention for critical & important functions or those that can become so.

— 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.

— 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;

— The rights and obligations of the financial institution and the service provider must clearly be assigned and established in a written agreement;

— The service provider's performance and the outsourcing risks must be constantly monitored for all outsourced services, with a focus on critical and important functions. All outsourcing must be reported to the supervisory authority by mid-2020;

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 the 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:

3. Impact on the financial sector

While, the new Guidelines not only affect financial institutions, but also regulators and service providers, the impact of the new regulations on outsourcing activities and the associated risk will vary from one party to another.

3.1 Regulators will monitor a new form of concentration risk

The National Bank of Belgium (NBB) issued circular BNB_2019_19 on 19 July 2019, integrated in their regulatory practice, which specifies the practical arrangements for reporting and communication to the supervisory authority when outsourcing certain activities to third parties[1].

On 31 December 2021 the circular will replace:

- circular PPB_2004/5 on proper management practices relating to outsourcing by credit institutions and investment firms;
- circular NBB_2018_20 on recommendations on outsourcing to cloud service providers;
- communication NBB_2012_11 on prudential expectations regarding cloud computing;
- communication of the CBFA of 6 November 2007 on its policy regarding the outsourcing of asset management services of assets of non-professional clients to a service provider in a State that is not a member of the European Economic Area.

In addition to the supervision of financial institutions, the new Guidelines make the NBB 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 if the service provider runs into (financial) problems. As outsourcing agreements are currently not, or not fully, registered centrally, there is currently no complete picture.

The Guidelines stress that financial institutions should include a clause in the outsourcing policy and agreement that gives the NBB 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.

3.2 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. Competition and reputation riks

[1] https://www.nbb.be/en/articles/circulaire-nbb201919-orientations-de-lautorite-bancaire-europeenne-abe-du-25-fevrier-2019

A. Retaining (final) 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 NBB's notification obligation, 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.

1.3.3 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.

4. 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 rise in outsourcing, it is becoming increasingly important for financial institutions to have good internal control. Built-in controls play an important role in this, such as the "three lines of defense" model in which segregation of duties and monitoring by independent departments 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.

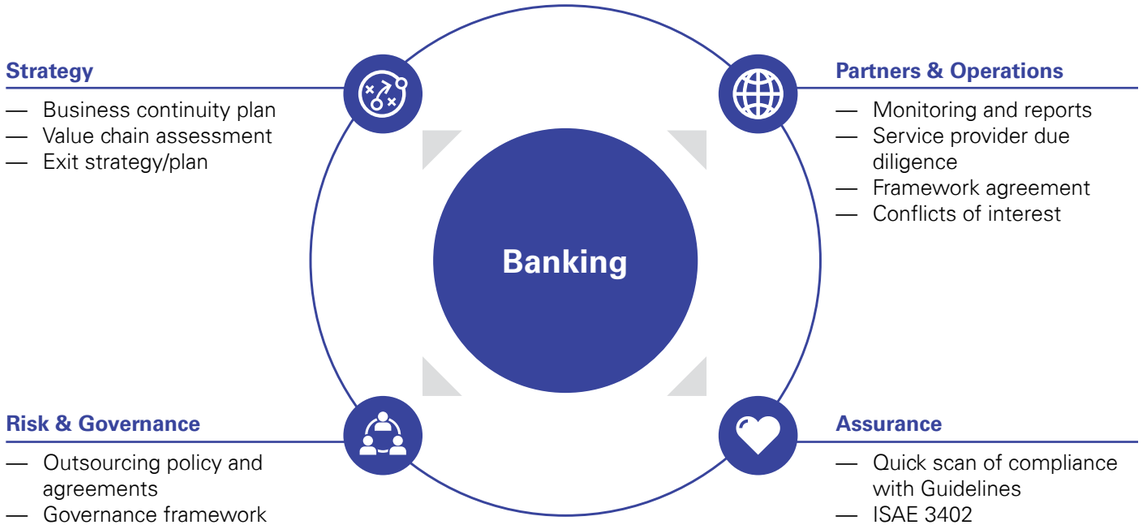
5. Next steps

The Guidelines entered into force 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.

In practice, we see that financial institutions 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 financial institutions must be careful not to become a "letter-box-entity" 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.

KPMG can assist with every phase of the outsourcing life cycle. Our team has the end-to-end expertise, experience and sector knowledge to help with detailed risk analysis and the approach for effective management of outsourcing risks. The KPMG control framework ensures that all aspects of the Guidelines are considered and that you comply with the requirements of the new regulation.



[1] https://www.nbb.be/en/articles/circulaire-nbb201919-orientations-de-lautorite-bancaire-europeenne-abe-du-25-fevrier-2019

Questions?

If you have any questions
please contact our team.

Anthony Van de Ven
Partner
T: +32 3 821 18 59
E: avandeven@kpmg.com

Paul Olieman
Executive Director
T: +32 3 821 18 56
E: paulolieman@kpmg.com

Filip Weynants
Partner
T: +32 2 708 37 82
E: fweynants@kpmg.com

kpmg.com/be