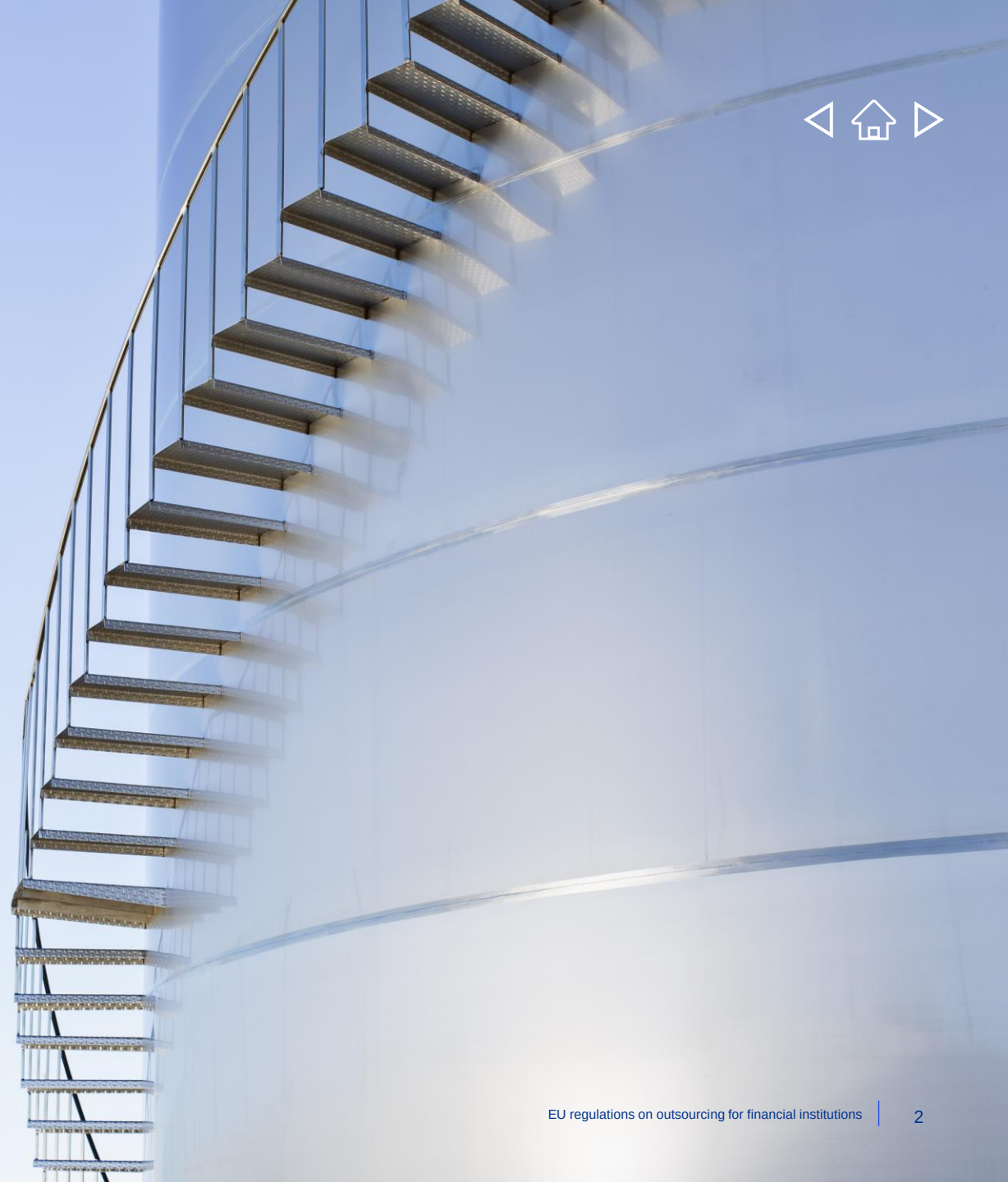
EU regulations on outsourcing for financial institutions

A proven remediation approach to ensure compliance

March 2023

Table of contents



Introduction

Outsourcing is a popular method to gain access to (technological) innovations, flexibility and economies of scale. However, outsourcing also creates new risks for financial institutions and supervisors. Hence EU regulators (EBA, EIOPA and ESMA) have already published guidelines aimed at identifying, addressing and mitigating these risks. With the introduction of the Digital Operational Resilience Act (DORA), requirements on ICT outsourcing now apply to a broad range of financial institutions (including institutions that are not subject to the earlier EBA, EIOPA and ESMA Guidelines).

Over the past years, KPMG has assisted several financial institutions with the implementation of EU regulations on outsourcing. The purpose of this document is to provide a remediation approach and good practices for becoming compliant, based on our experiences with financial institutions.

This document is intended for financial institutions in the EU who are subject to regulatory requirements on outsourcing. We use the term 'financial institutions' broadly, to include any entity that is regulated and supervised by an EU regulator (e.g., credit and payment institutions, insurance companies, pension funds and investment funds). This document is particularly addressing the EU regulations related to outsourcing listed below and does not include country-specific regulation. Which regulatory requirements apply to your situation depends on, for instance, the classification of the organization. It is important to take note of the differences in sector, scope and timelines.

Regulation	Sector	Scope	Enter into force	End transition period
DORA *Chapter V: 'Managing of ICT third-party risk'*	Financial entities (e.g., credit and payment institutions, insurance companies, pension funds and investment funds)	ICT outsourcing	16 January 2023	17 January 2025
ESMA Guidelines	Securities markets (e.g., investment funds)	Cloud outsourcing	31 July 2021	31 December 2022
EIOPA Guidelines	Insurance (e.g., insurance companies)	Cloud outsourcing	1 January 2021	31 December 2022
EBA Guidelines	Banking (e.g., credit and payment institutions)	Outsourcing	30 September 2019	31 December 2021

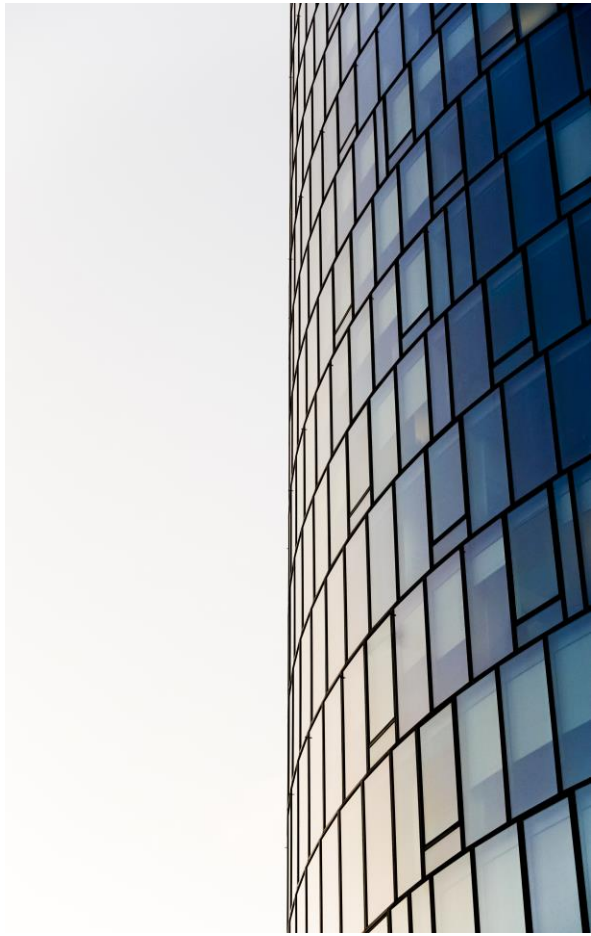
Disclaimer: The remediation approach described in this document is generic of nature and does not cover all individual requirements from the above EU regulations. Please ensure that you gain insight into all requirements that are applicable to your situation.

Remediation approach

A proven remediation approach for financial institutions

Financial institutions that are subject to regulatory requirements can deploy a remediation approach that entails a set of activities in order to become compliant. The below illustration presents essential steps (non-exhaustive) that should be part of this remediation approach. These steps are described in more detail in this document. For more information, please click on the different steps in the illustration.

Most steps in the remediation approach can be performed in parallel and are not sequential, however it is recommended to start with the classification of third party arrangements. During the implementation of the remediation approach, it is furthermore recommended to prioritize the critical or important outsourcing arrangements.



Steps in the remediation approach

- Classification of third party arrangements
- Notifications to the supervisor
- Outsourcing register
- Outsourcing agreements
- Outsourcing files
- Policies

Accelerators used in the remediation approach

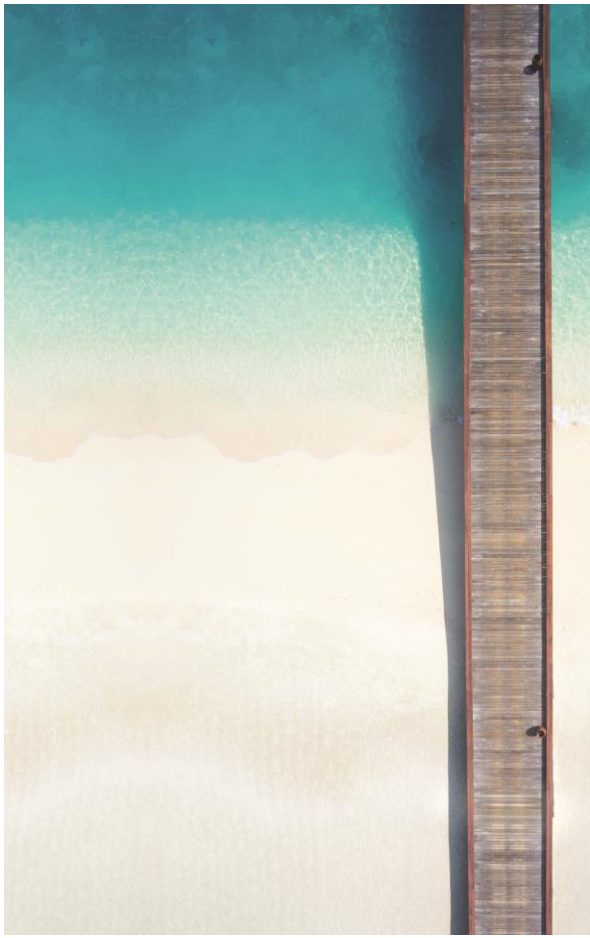
Based on experience and numerous engagements with financial institutions, KPMG has developed a set of proven tools and templates that can be used in order to meet regulatory requirements. These accelerators strengthen the governance framework and help institutions to improve their outsourcing policies and processes. The table below provides an overview of tools and templates that are often used.

Tool or template	Description
Outsourcing classification	Template used for the classification of third party arrangements
Risk assessment	Template used for the assessment of the potential impact of outsourcing arrangements on operational risk
Notification fill-in form	Fill-in form used to gather the required information to notify the supervisor on critical or important outsourcing arrangements
Outsourcing register	Comprehensive register that records information on the outsourcing arrangements
Outsourcing policy	Policy that includes the main phases of the lifecycle of outsourcing arrangements and defines the principles, responsibilities, and processes in relation to outsourcing
Contract checklist	Checklist used to assess whether the mandatory clauses are included in an outsourcing agreement
Regulatory Compliance addendum	Contractual amendment to the (existing) outsourcing agreement to ensure mandatory clauses are included in the agreement
Exit strategy	Template used for critical or important outsourcing arrangements to assess various exit scenarios including the impact and risks
Conflicts of interest analysis	Template used to identify and assess actual and potential conflicts of interest with regard to (intended) outsourcing arrangements
Knowledge retention analysis	Template used to assess the required knowledge at the institution to sufficiently manage the outsourced function and avoid becoming an empty shell
Due diligence checklist	Checklist used to perform a due diligence on a candidate service provider

Project management during the remediation approach

The remediation approach will benefit from a project organization with clearly defined roles and responsibilities. The project organization required depends on several factors, including the size of the company, its maturity on outsourcing management and the outsourcing landscape. Some disciplines that are essential to successfully manage the remediation project are listed below.

Discipline	Involvement (non-exhaustive)
Sourcing and Procurement	Ensuring that outsourcing policies and processes are compliant and implemented
Business	Ownership of the outsourcing agreement and providing information on the function that is outsourced
ICT	Identifying services, applications and systems that can be regarded as outsourcing and handling them accordingly
Legal	Creating contractual amendments such as the Regulatory Compliance addendum as well as any other legal implications that need to be assessed
Risk Management	Reviewing of risk assessments and assessing possible risks for the organization
Compliance	Adapting existing policies (e.g., conflicts of interest policy)
Internal Audit Function	Ensuring that outsourcing is sufficiently covered in the annual audit plan and that the regulatory requirements are in scope of the performed audit activities



Stay in control and sustain compliancy

In order for a financial institution to stay in control and sustain compliancy, a number of operational processes and practices will have to be implemented during the remediation approach. We have highlighted some of the most important ones below.

Maintenance of outsourcing files

Develop a set of concrete criteria (including frequency) for reviewing outsourcing files such as risk assessments and exit strategies. A periodic review ensures that these documents remain relevant and up-to-date. Our experience is that a fixed frequency helps to ensure that such a periodic review is performed.

Roles and responsibilities

Roles and responsibilities for reviewing the outsourcing arrangements and maintaining the outsourcing files have to be defined within the organization. For this purpose, a RACI model covering all phases of the outsourcing lifecycle is recommended.

Approval and decision making

A formal committee must be responsible for approving important documents and decisions, such as the risk assessments or the decision to enter into a new outsourcing arrangement.

Notifications to the supervisor

A process needs to be in place to ensure that the supervisor is informed in a timely manner about any planned critical or important outsourcing arrangements as well as when an existing outsourcing arrangement becomes critical or important.

Quality and consistency

All employees involved in reviewing the outsourcing arrangements and maintaining the outsourcing files must be aware of the degree of quality and consistency that is required. Providing training and assistance can help to ensure a sufficient level of quality.

Tooling and automation

Tooling and automation can be used to comply with regulatory requirements in a standardized and digitized way, often by eliminating manual tasks in the process.

Visual management

Visual management (e.g., dashboards) can provide relevant insights in, for instance, the completeness of the outsourcing register or the degree of compliance for each of the outsourcing arrangements.

Internal Audit Function

The Internal Audit Function will need to ascertain that the financial institution's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulations.

Remediation approach:

Classification of third party arrangements

Classification of third party arrangements

Financial institutions must establish whether an arrangement with a third party falls under the definition of outsourcing. The EBA Guidelines, for instance, provide the following guidance:

> *"Within this assessment, consideration should be given to whether the function (or a part thereof) that is outsourced to a service provider is performed on a recurrent or an ongoing basis by the service provider and whether this function (or part thereof) would normally fall within the scope of functions that would or could realistically be performed by the institution, even if the institution has not performed this function in the past itself."*
>
> Source: EBA Guidelines on outsourcing arrangements (2019)

Classification of third party arrangements is an essential step in becoming compliant as its outcome determines which arrangements must comply with the regulatory requirements. To ensure consistent and reliable classification, we recommend the following steps:

1. Ensure there is a complete overview of third party arrangements

A logical starting point is a complete list of all third party arrangements. Careful preparation of this list prevents surprises later on in the process. Various methods can be used to validate the completeness and correctness of the list. One could think of work sessions, cost analysis and verification based on existing lists (application list, contracting parties etc.). Arrangements that are already phased out should be removed for obvious reasons.

2. Create classification template

Next, a template must be created that can be used for the classification. The template preferably is embedded in a tool but alternatively can also be built in Excel. If a source-to-pay solution is used by the institution, it is preferable that this functionality is embedded in the existing solution. Through a series of questions, the classification template should provide clarity on topics such as:

- Does the arrangement fall under the definition of outsourcing?
- Does the arrangement fall under an exception?
- Is the outsourced function considered critical or important?
- Does the outsourcing involve cloud services?

3. Perform classification

Once the classification template is created, the next step is to fill in the template for all identified third party arrangements. This process requires in depth knowledge of the scope of the third party arrangement as well as the regulatory requirements. Hence this often is performed in collaboration between the business and the project team responsible for the implementation of the regulatory requirements.

It is recommended to follow a review and approval process before the classification is marked as completed. Depending on the organization, reviews can for instance be performed by IT Risk Management, Operational Risk Management, Sourcing and/or Procurement. We recommend to approve the classification in a formal committee (often an already existing outsourcing and/or risk committee can be used for this purpose).

Completed classification templates (including motivation) must be documented so that they always can be consulted in the future and updated if needed.

Remediation approach:
Notifications to the supervisor

Notifications to the supervisor

Institutions need to inform their supervisor in a timely manner about any planned critical or important outsourcing arrangements as well as when an existing outsourcing arrangement becomes critical or important. During the transition period of the regulation, this requires financial institutions to notify their supervisor of already existing critical or important outsourcing arrangements.

Although the regulatory requirements apply across Europe, the methods and procedures used by national supervisors for processing the notifications can differ. For gathering the required information, it can be useful to use a fill-in form which corresponds with the portal and process used by the supervisor. This fill-in form is populated by the project team and once completed it is shared with the person who actually submits the information to the supervisor. The fill-in form contains clear instructions so that information is included in an accurate manner and additional time and effort required to correct mistakes or false information is reduced.

It is of great importance that the information shared with the supervisor is accurate and complete. Hence we recommend a thorough review and approval process prior to submitting the information to the supervisor.

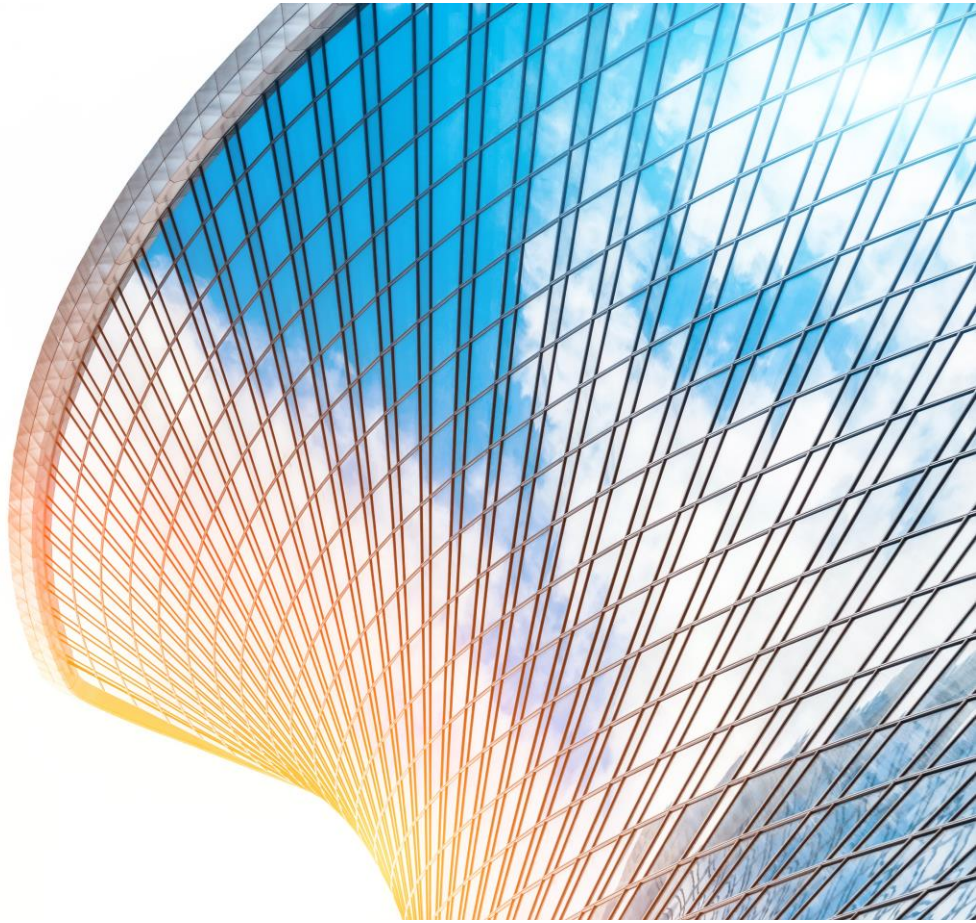
Remediation approach: Outsourcing register

Outsourcing register

Regulation requires that institutions maintain an up-to-date register with information on outsourcing arrangements. The regulatory requirements define which information needs to be registered and for which arrangements. Based on our experience we recommend considering adding additional information in the register on top of the regulatory requirements. One could think of information on the notification of critical or important arrangements to the supervisor (e.g., the date of the notification and the related case number).

Before registering an outsourcing arrangement, it is important to ensure that the complete and final contract is available (i.e., the version signed by both contracting parties). The register itself, which is basically a list of outsourcing arrangements with a large number of information fields, can be maintained in tools that already provide the needed functionality (such as a source-to-pay solution) or can be built in programs such as Excel, SharePoint Online or Power Apps.

An explanation and instruction for each of the information fields in the outsourcing register as well as fixed drop-down menus can limit the potential mistakes or interpretation differences during the registration. We also recommend to carefully register the source of the information, so that the information always can be verified.



Remediation approach:

Outsourcing agreements

Outsourcing agreements (1/2)

Regulation requires that outsourcing agreements include several mandatory clauses. For critical or important outsourcing agreements, more stringent requirements apply. We typically see that existing outsourcing agreements do not sufficiently cover these clauses. Clauses that are often missing are for instance the right to audit, right to examine and the conditions that apply to subcontracting. In order to ensure compliance of existing outsourcing agreements, a contract remediation process is recommended. In the below overview we describe a generic approach which can be used for this purpose.

1. Draft a standard Regulatory Compliance addendum (e.g., “DORA addendum”)

One way of making existing agreements compliant is through a so called Regulatory Compliance addendum. In this addendum, all mandatory clauses are included. For topics that often already are included in the contract (e.g., the governing law and commencement date of the agreement) we recommend to include this only when not already provided in the existing agreement.

When drafting the standard Regulatory Compliance addendum please consider that you probably have agreements in multiple languages, therefore we advise to draft the Regulatory Compliance addendum in the most commonly used languages. In the Netherlands for instance this will often be Dutch and English. Furthermore, the requirements for critical or important outsourcing agreements are more stringent than for regular outsourcing agreements. Hence we advise to draft a “light” Regulatory Compliance addendum for regular outsourcing agreements.

Always involve your Legal department when drafting the standard Regulatory Compliance addendum. An external advisory or law firm can be requested to review the Regulatory Compliance addendum. A thorough process upfront can save a lot of time later. Hence only send out the Regulatory Compliance addendum to service providers when you have convinced yourself that the addendum is of sufficient quality.

2. Assess the compliance of existing outsourcing agreements

For all existing outsourcing agreements it is required to assess whether the mandatory clauses are sufficiently covered. For this purpose a checklist can be used which includes the regulatory requirements for the contract.

3. Prioritize the outsourcing agreements

It is recommended to prioritize critical or important outsourcing agreements before regular outsourcing agreements. Furthermore, based on the outcomes of the previous step you are able to prioritize the individual outsourcing agreements for the contract remediation process. The agreements that are least compliant, are often remediated first.

Outsourcing agreements (2/2)

4. Share the Regulatory Compliance addendum with the service providers

Service providers of non-compliant agreements should be approached with the request to add the Regulatory Compliance addendum to the agreement. When doing so, it is of importance to emphasize that this is driven based on regulatory requirements. In our experience, most service providers are willing to accept the Regulatory Compliance addendum, but unfortunately there are also exceptions. Barriers can be reduced by already pre-populating the Regulatory Compliance addendum with the available information before it is shared with the service provider. If the service provider does not accept the Regulatory Compliance addendum, involve your Legal department to decide on follow-up actions. If the disagreement cannot be resolved by making minor adjustments to the Regulatory Compliance addendum, it can be required to review the exit strategy and decide on next steps.

The described approach assumes that a standard Regulatory Compliance addendum is used which is then customized for each agreement (e.g., by including the details of the service provider). Another option is to have a tailor made Regulatory Compliance addendum for each individual agreement. In this alternative approach, the contractual clauses in the Regulatory Compliance addendum are tailor made so that they are perfectly aligned with or in addition to the existing agreement. This however is a very time consuming process, hence it is not recommended when confronted with a compliance deadline.

5. Ensure that new outsourcing agreements are compliant by design

Although not a real step in the contract remediation process, we advise to make sure that all new outsourcing agreements are compliant from the start. This requires to review the standard outsourcing agreement that is used within your organization (including general terms and conditions for purchasing) and to ensure that it is compliant with regulatory requirements. For services in which the standard contract of the service provider is used, it is recommended to ensure that all regulatory requirements are covered in the contract or to supplement the contract with the Regulatory Compliance addendum.

Some service providers (e.g., Microsoft and Amazon Web Services) have standard contract amendments for the financial services industry based on EU regulations. As these amendments have been adjusted over time, please ensure that you have the latest version attached to the outsourcing agreement.

Remediation approach:
Outsourcing files

Outsourcing files

Regulation requires financial institutions to have available and periodically update several outsourcing files. We have described some of them in more detail below.

Risk assessment

Regardless of the criticality or importance of the outsourced function, institutions should assess the potential impact of the outsourcing arrangement on operational risk. If not done already, institutions should assess for all individual outsourcing arrangements scenarios of possible risk events and identify and implement mitigating measures wherever required. For outsourcing arrangements with an IT component, this also requires the institution to classify the IT systems and data in categories reflecting the degree of availability, integrity and confidentiality.

Exit strategy

Institutions should have a documented exit strategy when outsourcing critical or important functions. Common exit scenarios that should be identified and assessed are:

- An alternative service provider taking over the outsourced function;
- Insourcing the outsourced function;
- Taking over the outsourced function in collaboration with another financial institution.

Business continuity plans

Financial institutions should have in place, maintain and periodically test appropriate business continuity plans with regard to outsourced critical or important functions. For this purpose, it needs to be determined whether the service provider has a business continuity plan that is suitable for the services provided. In some cases, (partial) assurance on business continuity can be provided through a third-party audit report (e.g., ISAE 3402 or SOC) made available by the service provider.

Audit

Financial institutions should exercise its access and audit rights on service providers of outsourced critical or important functions. In some cases, third-party certifications and third-party or internal audit reports made available by the service provider can be used for this purpose. While in other cases the financial institution (or a third-party appointed by the institution) has to perform the audit by itself or jointly with other clients of the same service provider.

Remediation approach:
Policies

Policies

Regulation requires financial institutions to review and update existing policy documents, with particular focus on the outsourcing policy. In practice, we see that the required efforts for a detailed review are often underestimated and that necessary adjustments to comply with regulatory requirements prove to be more complex than initially thought. Reviewing and adjusting the outsourcing policy is often not possible without an update of for instance the governance policy or conflicts of interest policy. This creates the risk that parts are overlooked and inconsistencies occur between the various policy documents.

In our engagements, we often encounter the following shortcomings when reviewing the outsourcing policy:

- Regulatory requirements are not (sufficiently) embedded in policy statements;
- Not all phases of the outsourcing lifecycle are sufficiently covered (e.g., the exit phase is missing);
- Roles and responsibilities throughout the outsourcing lifecycle are not clearly defined;
- The outsourcing policy is not formally approved by the management body;
- Periodic reviews of the outsourcing policy have not been carried out.

When conducting a thorough policy review, the dependencies with other policy documents should be taken into account. This requires sufficient coordination with internal stakeholders. In addition, the process to approve the outsourcing policy must be prepared in time to avoid delays. Finally, the review offers the possibility to implement other improvements that are not necessarily related to regulatory requirements.

Conclusion

In the past years we have seen significant developments in EU regulations on outsourcing for financial institutions. In practice, we see that financial institutions often underestimate the implementation of regulatory requirements and that necessary adjustments to ensure compliance prove to be more complex or time consuming than initially thought. Furthermore, due to increased EU and national law and regulations, we see that institutions struggle to understand the full set of regulatory requirements that apply to their situation. We are confident that the presented remediation approach can help financial institutions in ensuring compliance in a structured manner. Please contact our experts on the next page for more information.

Contact

Kees Stigter
Partner
Digital Sourcing

Tel: +31 (0) 6 46 70 69 33
E-mail: stigter.kees@kpmg.nl

Maarten Visser
Senior Manager
Digital Sourcing

Tel: +31 (0) 6 10 17 98 30
E-mail: visser.maarten@kpmg.nl

home.kpmg/socialmedia