Maj 2020

Outsourcing in the financial sector
Compliance handbook

KROMANN
REUMERT

Intended readers

This handbook is intended as a guide for financial institutions who need to revise their outsourcing compliance approach or need a brush-up on the new regulatory requirements entering into force on 1 July 2020. This handbook has its focus on the Danish regulatory regime and the Danish market. However, parts of the handbook relate to non-legal aspects such as risk assessments, internal project management and best practice contract management, which can be used universally.

While we hope that this guide will be useful to anyone with an interest in compliance within financial regulations and outsourcing we have focused our attention on supporting people in the following roles:

- **Compliance functions** – *providing an overview of the compliance requirements and a structured approach to ensure continuous compliance*
- **Procurement functions** – *on recommended focus areas when contracting with new service providers.*
- **Vendor management functions** – *clarifying requirements for ongoing contract management and monitoring of service providers.*
- **Legal functions** – *providing an overview of the legal aspects of all the above to enable legal support of the business functions.*

Institutions

The new executive order on outsourcing applies to the following financial institutions:

- credit institutions (banks);
- mortgage-credit institutions;
- investments firms;
- investment management companies;
- savings undertakings;
- shared data centres (in Danish: "fælles datacentraler")
- operators of regulated markets;
- e-money institutions;
- payment institutions; and
- Danmarks Skibskredit A/S.

E-money institutions and payment institutions are now subject to the same regulation as the other financial institutions, whereas previously they were subject to the regulation set out in the Danish Payment Act (Betalingsloven). Shared data centres are now also covered.

A number of institutions which were previously subject to the same regulation as the above are no longer included. These include ATP, Lønmodtagernes Dyrtidsfond and Group-2 insurance companies, all of which are now subject to regulation set out in a separate executive order on outsourcing (No. 723 of 28 May 2020). The overall ambition of that executive order is to align the regulation of ATP, Lønmodtagernes Dyrtidsfond and Group-2 insurance companies with the regulation that applies to Group-1 insurance companies under the Solvency II Regulation.

The new regulation and its background

The new executive order on outsourcing for credit institutions etc.

The Danish Financial Supervisory Authority (FSA – "Finanstilsynet") published a new executive order on outsourcing for credit institutions etc. on 16 June 2020 (No. 877 of 12 June 2020) (the "Executive Order"). Entering into force on 1 July 2020, the Executive Order replaces the current executive order from 2010 on outsourcing of significant areas of activity. The FSA is expected to publish a set of guidelines to assist in the interpretation of the Executive Order, however, as of now it has not yet been released.

EBA guidelines on outsourcing arrangements

On 25 February 2019, the European Banking Authority (EBA) published its revised Guidelines on outsourcing arrangements, which entered into force on 30 September 2019. The EBA guidelines are implemented in Denmark by the Executive Order.

The revised guidelines contain EBA's supervisory expectations and in general serve to establish a more harmonized framework for financial institutions across Europe, including by:

- Ensuring that financial institution can rely on one legal framework on outsourcing for all banking, investment and payment activities.
- Clarifying the responsibilities, as the guidelines specify that the management body is responsible for each financial institution and its activities at all times.
- Specifying which arrangements with third parties must be considered outsourcing and providing guidance on which are critical or important.

Purpose of the new regulation

The overall ambition and rationale behind the outsourcing regulation is to ensure that the entity outsourcing at all times has an overview of and is in control of its outsourcing arrangements. Further, and on a practical level, the rules seek to avoid a situation where all material activities of the institution have been outsourced, leaving the institution an "empty shell".

Therefore, the regulation on outsourcing establishes a set of requirements that must be met by undertakings that outsource – or plan to outsource – business processes or functions. The revised regulation also seeks to secure internal and external transparency with outsourcing arrangements.

What has changed?

Comparing to the old regulation

The old regulation was to a large extent based on the CEBS guidelines of 2006. The increased use of outsourcing and the nature of such outsourcings – including the introduction of cloud technologies – have meant that these guidelines and the previous Danish executive order on outsourcing over time have become outdated.

One major change is the scope of the regulation. Where the old regulation only applied to the extent that the outsourcing was deemed a significant area of activity, the new regulation will apply to all outsourcings by default but will in some areas have less strict requirements on outsourcings which are not critical or important. This means that there is a greater need to be aware of all outsourcings across the institutions and the individual outsourcings – regardless of size and nature.

Focus on internal governance and oversight has increased. The institution can only use outsourcing if this does not jeopardize operations. The board of directors is ultimately responsible (article 10,1 of the Executive Order) for outsourcing arrangements and cannot outsource this responsibility (article 10,2 of the Executive Order). This means, among other things, that the board of directors defines the institution's risk approach and outsourcing policy (article 10,4 and 11 of the Executive Order), provides clear boundaries for the use of outsourcing (and critical or important outsourcing) and continuously monitor the executive management's decisions and risk management related to outsourcing (article 10,3 of the Executive Order).

Further, the new regulation includes a number of elements that – as will be further described in this guide – will drive additional compliance steps to be taken, including

- Requirement of an outsourcing officer
- Preparation, maintenance and testing of contingency plans
- Requirements of an outsourcing registry
- Requirement of written exit-strategies

In conclusion, the new regulation will require most institutions to revise their compliance approach.

Defining outsourcing

What is outsourcing?

Outsourcing covers arrangements between a company and a service provider employed to carry out a service or activity that the company *would normally carry out itself.* Under the Executive Order, "outsourcing" covers services or activities which are performed either repetitively or on an on-going basis by a service provider, meaning that "one-off" purchases or tasks falls outside the scope of "outsourcing". Certain tasks are not considered outsourcing in the Executive Order. These are:

i) tasks that the institution is required by law to delegate to
a service provider,

ii) procurement of market information services,

iii) global payment network infrastructure

iv) clearing and settlement schemes between clearing centrals, central counterparts, settlement institutions and their members,

v) correspondent banking services,

vi) purchase of services, goods or supplies that would normally fall outside the institution's areas of activity

Item vi) above is the one which leaves the most room for interpretation and calls for particular attention. The institution should test whether the service i) is in fact one that the institution can do or is doing itself or realistically could be carried out by the institution – meaning that a service can only be "outsourced" if the institution itself is realistically capable of delivering it in-house, this would typically exclude utility providers (electricity, internet, telecommunications, etc.) and ii) whether the service generally falls outside the institution's areas of activity.

Such activities may to some extent be carried out by the institution but are not within its key business areas. The EBA has provided guidance that such excluded services may include:

- External legal services,
- Facility management and catering, and
- Office supplies.

Outsourcing to group companies: It is important to bear in mind that "outsourcing" also covers (i) services provided from one company to another within the same group (this could be a group internal service provider (e.g. IT)) or (ii) transitional services agreement entered into in connection with a transaction ("TSA"). Group internal service agreements and TSAs are therefore subject to the same requirements as outsourcing agreements with third-party providers.

§ 3. Outsourcing omfatter enhver form for ordning mellem en virksomhed og en leverandør, i henhold til hvilken leverandøren udfører en proces, en tjenesteydelse eller en aktivitet, som outsourcingvirksomheden ellers selv ville udføre.

Stk. 2. Ved vurderingen af, om en ordning udgør outsourcing, skal outsourcingvirksomheden overveje, hvorvidt processerne, tjenesteydelserne eller aktiviteterne eller dele heraf udføres gentagne gange eller løbende af leverandøren. Outsourcingvirksomheden skal desuden overveje om processerne, tjenesteydelserne eller aktiviteterne eller dele heraf normalt ville falde inden for rammerne af processer, tjenesteydelser eller aktiviteter, der realistisk set ville eller kunne udføres af outsourcingvirksomheden. 2. pkt. gælder også, selvom outsourcingvirksomheden ikke har udført disse processer, tjenesteydelser eller aktiviteter selv tidligere.

Stk. 3. Indeholder en ordning med en leverandør flere processer, tjenesteydelser eller aktiviteter, skal outsourcingvirksomheden inddrage alle aspekter af ordningen.

Stk. 4. Følgende udgør ikke outsourcing:

1) En proces, tjenesteydelse eller aktivitet, som virksomheden i henhold til lovgivning er forpligtet til at få udført af en leverandør, herunder lovpligtig revision.
2) Brug af markedsinformationstjenester.
3) Globale betalingsnetværksinfrastrukturer.
4) Clearing og afviklingsordninger mellem clearingcentraler, centrale modparter og afviklingsinstitutter og deres medlemmer.
5) Korrespondentbankydelser.
6) Køb af tjenester, varer eller forsyning, som ikke normalt ville blive udført af outsourcingvirksomheden.

Illustration of article 3 of the Executive Order, which holds the definition of what constitutes an "outsourcing".

Critical or important outsourcing

Critical or important outsourcing

While the regulatory requirements in the Executive Order generally apply to all outsourcings, there are additional, stricter requirements for critical or important outsourcings. The reasoning behind this is a principle of proportionality, with stricter requirements on outsourcings that carry a higher risk in respect of the institution's ability to carry out its business. Therefore, it is necessary to determine when an outsourcing is critical or important before looking at the different requirements.

Defining critical or important outsourcing

In article 4 of the Executive Order, an outsourcing is defined as "critical" or "important" if any defects, faults or lack of availability of the outsourced services will significantly impair the institution's:

- ability to comply with the requirements in its license/ authorization to operate,
- financial results, or
- ability to conduct its business and provide its services to its customers with due care.

Outsourcing of tasks that are subject to licensing approval and operational tasks in internal control functions are deemed critical or important outsourcing by default.

Whether an outsourcing arrangement is critical or important will depend to a large extent on the outcome of the risk assessment, and it is a requirement under the Executive Order that the outcome of the risk assessment is included in the evaluation of whether the outsourcing is critical or important. Additionally, article 5 of the Executive Order sets out which aspects the institution must take into consideration when assessing the criticality or importance of the outsourcing.

Within the boundaries defined by the Executive Order, it is the institution's own assessment whether each individual outsourcing is critical or important outsourcing. The FSA may subsequently disagree, but the initial assessment lies with the institution. We recommend that the assessment is documented in the outsourcing register.

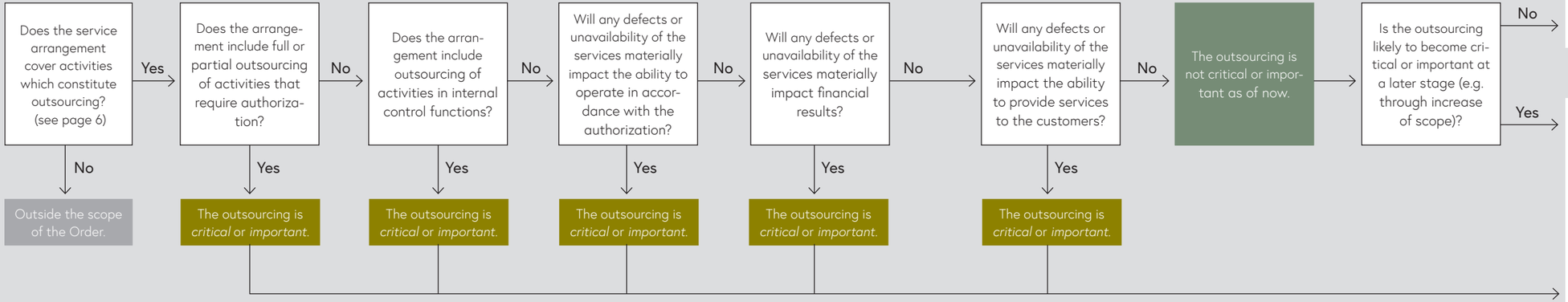
The aspects to be taken into account are:

- Whether the outsourced services are directly connected to the activities the institution is authorised for.
- The potential impact of any disruption to the services or the service provider's failure to provide the services at the agreed service levels on an ongoing basis on the institution's:
  - short and long-term financial resilience and viability;
  - business continuity and operational robustness;
  - operational risk;
  - reputational risks; or
  - any recovery or resolution planning, resolvability and operational continuity in connection with early intervention, recovery or resolution
- The potential impact of the outsourcing on the institution's ability to:
  - identify, monitor and control risks;
  - comply with all legal and regulatory requirements; or
  - conduct audits of the outsourced services.
- The potential impact on the institution's provision of services to its customers.
- All other outsourcing agreements, the institution's total exposure to the same service provider, and the potential total impact of outsourcing arrangements in the same business area.
- The size and complexity of any business area affected by the outsourcing.
- The possibility that the intended outsourcing may increase in scope without entering into a new or revising the existing outsourcing agreement.
- The ability to transfer the services to another service provider.
- The ability to insource the services back into the institution.
- The level of protection of data and the potential impact of a breach of confidentiality or failure to ensure the availability and integrity of the data regarding the institution and its customers.

Critical or *important* outsourcing

Decision tree for critical or important outsourcing

For help in determining whether a contemplated outsourcing is a critical or important outsourcing or not, the institution can go through the decision tree outlined below.



Remember to always;

- **Document the decision(s) from the decision tree**
- **Perform due diligence of the intended provider(s)**
- **Ensure compliance with contractual requirements**
- **Ensure compliance with any procedure in the policy, including obtaining board or executive approval**
- **Include the outsourcing in the outsourcing register**

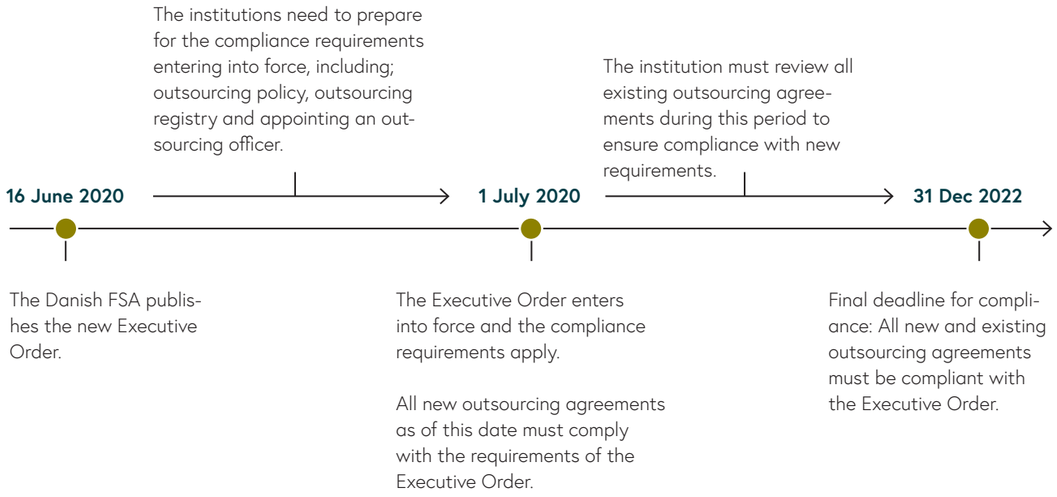
Remember to always;

- **Document the decision(s) from the decision tree**
- **Perform due diligence of the intended provider(s)**
- **Ensure terms for sub-contracting of critical or important parts of the services**
- **Ensure compliance with all contractual requirements**
- **Ensure compliance with any procedure in the policy**
- **Prepare contingency plan(s)**
- **Prepare exit strategy**
- **Obtain board approval**
- **Notify the FSA**
- **Include the outsourcing in the outsourcing register**

Compliance timeline

We have identified a number of focus areas that need to be considered on the short term in order to ensure compliance . These areas are described in this chapter and include; appointment of outsourcing officer, drafting an outsourcing policy, setting up the outsourcing register, revising the risk assessment approach and complying with other documentation requirements.

The Executive Order will enter into force on 1 July 2020, and it introduces a list of new requirements for financial institutions. Some institutions may already have started the implementation, while others might need to begin to plan a structured approach to become compliant in time. The FSA has indicated that it will take the short implementation time into account when assessing each institutions compliance with the Executive Order in the first few months.



Outsourcing officer

Appointment of an outsourcing officer

The Executive Order requires the institution to appoint a so-called "outsourcing officer" (In Danish; *outsourcingansvarlig*). The outsourcing officer is an individual, who is responsible for managing the risks associated with the outsourcing activities.

Responsibilities include monitoring, control and audit of outsourcing arrangements and the associated documentation, and the officer reports to the executive management for compliance purposes. The outsourcing officer may delegate these tasks within the organization and will likely have to do so – at least to some extent – but will remain responsible for compliance.

Under the Executive Order it is not possible for the board of directors to delegate responsibilities, and the board of directors remains fully responsible for monitoring and following-up on the outsourced activities.

Outsourcing policy

Legal requirements

The Executive Order requires the board of directors to approve, revise and continuously update a written outsourcing policy. The minimum requirements for the policy are defined in appendix 1 to the Executive Order The new requirements are far more detailed than previously and will most likely require institutions to update their prior guidelines to become a proper outsourcing policy.

The requirements for the outsourcing policy can be grouped into four main categories:

1. **The outsourcing in all its phases.** The policy should define all internal roles and responsibilities in all phases of an outsourcing, as well as laying down the principles for the use of outsourcing in the institution. This includes assigning the responsibilities between the executive management and the board of directors, which other business units and control functions to include (e.g. compliance and/or legal), how to plan and structure an outsourcing process, and how to use group internal outsourcings and the applicability of the policy across the group.

2. **Ensuring compliance.** The policy must outline how the institution intends to ensure compliance when and during outsourcing, including (i) compliance with ethical standards or codes of conduct, (ii) how to ensure an effective right of audit and not to limit the FSA's supervisory rights, and (iii) how the institution ensures that it will not outsource any tasks or responsibilities which it must not outsource (e.g. the responsibilities towards its customers or the internal control functions).

3. **Confidential Data and Personal Data.** The policy should describe the approach (risk based) to any outsourcing where confidential and/or personal data is transferred to or otherwise processed by the service provider. The policy should set out the principles for how to assess the risks related to specific types of data and data locations and assist in determining the mitigating actions required to minimize those risks.

4. **Specific requirements to *critical* or *important outsourcing*.** For critical or important outsourcings, the outsourcing policy must include a description of the boundaries of such outsourcings on: the overall risk profile of the institution (e.g. the boundaries of "acceptable risks"), the possibility to continuously monitor and audit the provider, to control and mitigate risks (e.g. minimum reporting and audit access), and the contingency plans (e.g. how far can the institution rely on contingency plans).

Best practice

As each financial institution will have its own strategic goals, internal competencies and risk appetite, the use of outsourcing and the content of an outsourcing policy will be different from institution to institution. However, as the appendix to the Executive Order sets out minimum requirements, all policies will have the same starting point. We always recommend using the structure of the appendix when drafting the outsourcing policy, as i) this provides a starting point, ii) ensures that all areas are covered, and iii) it is easy to map against the appendix if needed to demonstrate compliance.

The outsourcing policy can be drawn up simply to ensure compliance with the requirement to have an outsourcing policy with the minimum content set out in the Executive Order. However, we recommend that the outsourcing policy is drafted to support compliance with other requirements under the Executive Order as well and provide practical guidance for the employees working with the area. As examples, the outsourcing policy can define and describe the information – and the structure of such information – which the outsourcing officer needs to share with the management to support the management in its governance of the institution's use of outsourcing.

We have developed a standard outsourcing policy template, structured to follow the appendix, including helpful guidance and notes to the drafter.

Outsourcing register

Legal requirements

The institutions must establish and maintain an outsourcing register. The outsourcing register must include all outsourcings – not only critical or important outsourcings.

While the requirement to have a formal register is a new legal requirement, many institutions will already have a similar document or overview in place. As the requirements are now detailed and formalised in the Executive Order, the institutions should therefore review whether their existing registers, if any, are still sufficient to meet the new legal requirements.

The information required to be included in the register is set out in Appendix 2 to the Executive Order and includes, among other things:

- Master data on the supplier (name, ID-number, address, etc.)
- A description of the outsourced services and any data included, including whether the services are considered critical or important and when the assessment of this was made.
- Country(-ies) where the services are provided from (including whether data is stored there)

For critical or important outsourcings additional information must be included in the register, including the possibility of insourcing or finding alternative suppliers, additional information on the risk assessment of the supplier, and information on subsuppliers. For outsourcing to cloud, an additional requirement to describe the implementation model of the cloud services applies.

Best practice

Appendix 2 to the Executive Order sets out the detailed requirements to the register. We have created a template in the form of a simple Excel spreadsheet, to ensure all areas are covered, and which should allow anyone to start from scratch. Further, our contract management system is configured to also function as an outsourcing register.

We recommend that the register is kept as part of the institution's contract management system. This will ensure easy access and ensure that the register is accessible in only one updated version (i.e. no old Excel sheets lying around). As long as the information can be extracted and presented to the FSA, there are no further requirements as to how the register is kept.

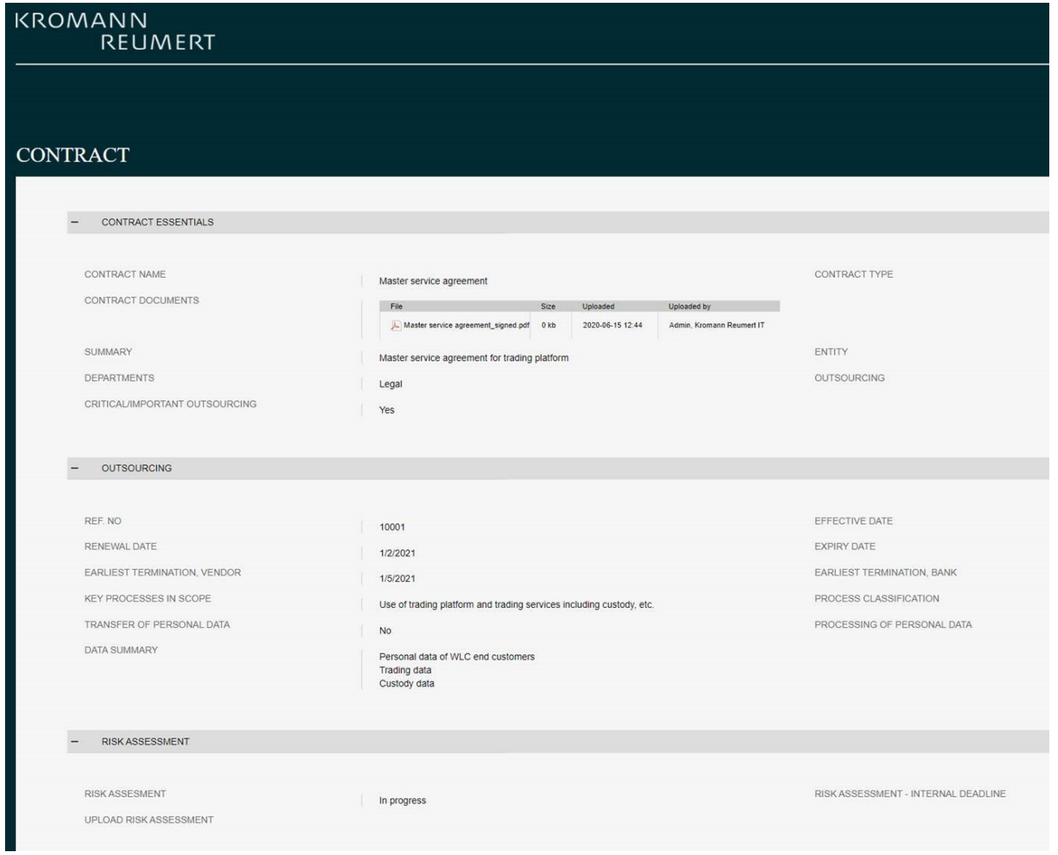


Illustration of Kromann Reumert's contract management system, which is set up to hold all information necessary to perform efficient contract management and also serve as outsourcing register.

Risk assessments

Risk management is one of the foundations of the new regulation. The institution should generally use a risk-based approach when determining how and to what extent outsourcing should be used in the operation of the institution.

Legal requirements

The institution must complete a risk assessment of all outsourcing arrangements. The Executive Order includes a number of specific risk areas which the institution must take into consideration in its risk assessments of a contemplated outsourcing. Additionally, the institution should consider having a general risk approach set out in the outsourcing policy. A risk assessment takes its starting point in each individual outsourcing, but it should also take into account both (i) the risk in outsourcing multiple services to the same service provider (concentration risk) and (ii) the risk in the institution's total use of outsourcing across the institution.

The risk assessment must take into account the outsourced processes and activities – including the impact of the services not being available, the amount and nature of data processed by the service provider, and the intended security measures, as well as the location of the service provider, including the political and economic stability in such location.

The transfer of the services – either through insourcing or transferring to another provider – may also provide significant risks as the service provider may be in breach or financial distress, or simply disinterested in providing high-quality services to a customer leaving.

Kapitel 6

Risikovurdering ved anvendelse af outsourcing

§ 19. Outsourcingvirksomheden skal før en beslutning om outsourcing eller videreoutsourcing

1) vurdere de potentielle konsekvenser for outsourcingvirksomhedens operationelle risici og
2) træffe nødvendige foranstaltninger til at begrænse operationelle risici i forbindelse med outsourcingen.

Stk. 2. Vurderingen efter stk. 1, nr. 1, skal som minimum indeholde:

Illustration of article 19 of the Executive Order, which sets out the requirements to the risk assessment.

Best practice

For a consistent approach to risk assessments, the institution should adopt a standard risk assessment framework describing the approach and providing a framework for making conclusions on each risk. One of the most used and well-known risk assessment methods is the "impact x likelihood" matrix, in which the different risks are identified and subsequently classified on both the impact the risk will have if it materializes and how likely it is that the risk occurs.

Each risk is assessed in this way, and the impact and the likelihood are both given a score, which combined will result in the overall risk score.

The result of the risk assessment can also assist in determining the mitigating measures – risks that are very likely to occur (but may not have a high impact) should be able to be mitigated effectively, as they are probably well-known and will likely have occurred previously, whereas risks that occur less frequently may be more difficult to mitigate up front – for such risks, it is important to have proper contingency plans in place.

Additional documentation requirements

Apart from the outsourcing register, the Executive Order introduces additional new documentation requirements. While many institutions will have much documentation in place already, even those institutions should revisit the documentation, as more specific and strict requirements have been included in the Executive Order.

- **Documentation of assessments and decisions.** A general requirement to establish an information trail that can document how the institutions arrived at the conclusions they did (e.g. the result of a risk assessment or whether an outsourcing was critical or not). The manner and extent of the documentation is not set out in the Executive Order but should be set out in the outsourcing policy to ensure consistency throughout the institution.

- **Exit strategies.** The institution must have in place exit strategies for all critical or important outsourcings. The requirements to the strategies are set out in an appendix to the Executive Order, and the overall objective of the exit strategies is that the outsourcing agreement can be terminated without negative impact on the institution's: (i) business activities, (ii) ability to comply with regulatory requirements and (iii) ability to continuously deliver its services to its customers in the same quality as always.

- **Contingency plans.** The institution must have in place contingency plans for all critical or important outsourcings. The contingency plans should clearly describe the roles and responsibilities (both internally and between institution and service provider) in an event where the contingency plan must be activated. The contingency plans should be reviewed, tested, and updated continuously.

How to structure a compliance project

Introduction

If the institution is not already compliant with the requirements in the new regulation, the process towards becoming compliant is best made as one consolidated compliance project rather than large number of adhoc tasks. In the following, we have included our high-level guidance for such project.

Identify stakeholders and task – and form a working group

First, the relevant stakeholders must be identified. The key stakeholders will to a large extent comprise the executive management, who has responsibility for controlling and governing the use of outsourcing. With the support of the relevant stakeholders, a working group should be formed and the specific tasks defined and prioritized.

The working group would normally include the following functions to ensure all parts of the business are included:

- Vendor management – who has the formal contact with suppliers and has an overview of the relevant contracts,
- Legal / compliance functions (including the outsourcing officer) – who have knowledge of the existing compliance set-up,
- Operational functions – who often use the outsour ced services on a daily basis and can clarify the needs and potential risks if services are not available, and
- Technical functions / IT – who have knowledge of technical possibilities (e.g. data flows and storage, redundancy in delivery setup, etc.).

Project initiation

The working group should define the concrete tasks required to address due to the new regulation and draw up an action plan linked to a timeline.

Priority should be given to the set of compliance obligations described above as the "*short term focus areas*". As noted, and although the FSA has stated that it will give regard to the short implementation period of the Executive Order, the requirements will apply as of 1 July 2020. Further, completing these tasks will support other compliance tasks:

- It is easier to monitor the outsourcing and follow up when you have the register in place,
- It is easier to make risk assessments when the standard risk assessment models are in place, and
- The internal processes of decision making and obtaining approvals are easier done once the outsourcing policy sets the framework for communication.

Identifying and reassessing existing outsourcing contracts

The foundation for compliance is knowing what is already outsourced and the risk profile associated with the existing outsourcings.

Step 1:

Is to locate all current service agreements with third parties – including group internal agreements and transitional services agreements.

↓

Step 2:

Information on all agreements should be included in the outsourcing register.

↓

Step 3:

The institution should also reassess and group the agreements in either **critical or important outsourcing** and other outsourcings based on the new definition, which may result in other agreements than before being deemed **critical or important outsourcing**.

↓

Step 4:

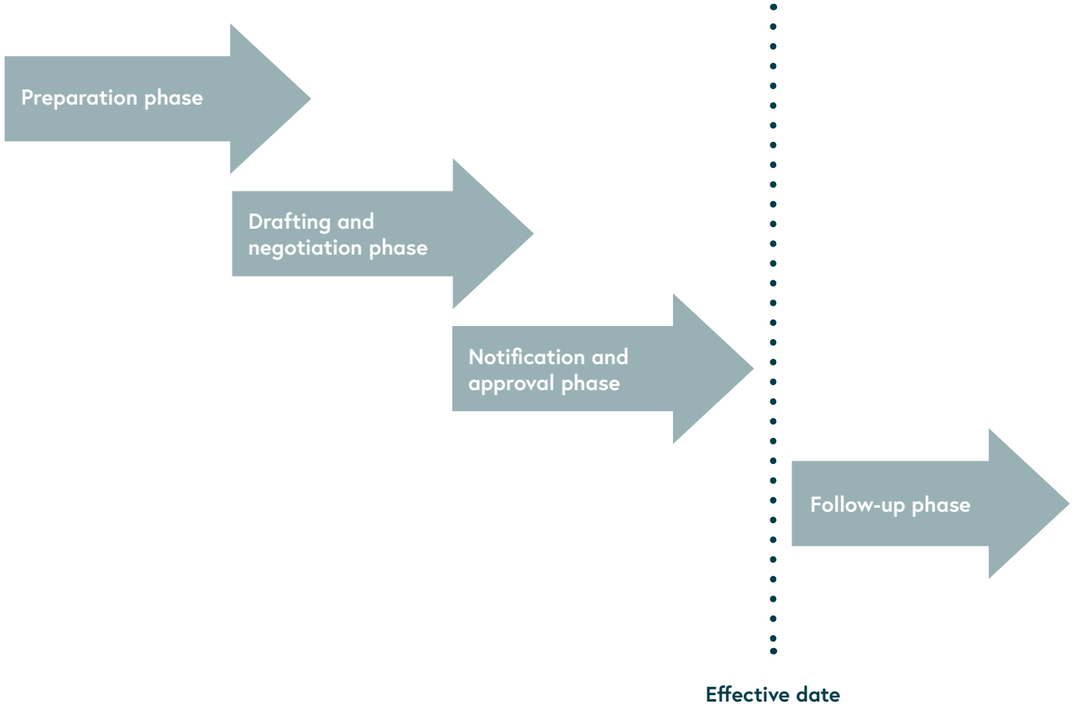
For those outsourcings deemed **critical or important outsourcings**, additional information must be included in the register.

↓

Step 5:

Road-map should be planned for renegotiating those agreements that do not already comply with the new minimum requirements for **critical or important outsourcing** agreements – the deadline for carrying out such renegotiations is 31 December 2022.

A number of activities must be undertaken when entering into new agreements. The process of entering into new agreements can be divided in the following four phases, which are described on the following pages.



Preparation phase

Regardless of whether the outsourcing is critical or important, all outsourcings must be documented by a written agreement with some minimum requirements defined in Appendix 3 to the Executive Order. The extent and degree of requirements vary depending on whether the outsourcing is a critical or important outsourcing or not.

Risk Assessment

Prior to each outsourcing, the institution must carry out a risk assessment of the contemplated outsourcing. The risk assessment should be carried out in accordance with the standard framework adopted by the institution and should include outcome of the vendor due diligence.

Due Diligence

Before entering into new outsourcing agreements, the institution must carry out a due diligence of the intended vendor(s). This requirement, which applies to all outsourcing arrangements, and not only to critical or important outsourcings, aims to ensure that any risks pertaining to the specific vendors are known and addressed by the institution. The outcome of the due diligence should form part of the risk assessment.

The Executive Order sets out the minimum requirements for the due diligence, which include:

- The size, business model and financial stability of the service provider.
- Long-term relations with the provider.
- Is the service provider a group company or subject to the FSA's supervision?
- Is the service provider able to protect data (including personal data) using the right technical and organizational measures.
- Can the service provider adhere to the institution's values and code(s) of conduct.

Both the risk assessment and the supplier due diligence should also be carried out for any new services outsourced to an existing service provider – the increased scope of services may pose additional risks (e.g. concentration risk) and require more knowledge of the service provider's capabilities

Drafting and negotiation phase

Drafting and negotiation phase

The drafting and negotiation phase is where the contractual requirements are agreed and subsequently set out the terms for the parties' relationship in the coming years. In addition to what is normally set out in an outsourcing agreement (e.g. services, quality, price, and legal terms), it is a requirement under the Executive Order that all outsourcing agreements have certain minimum content – with additional requirements for critical or important outsourcings.

The institution should be aware that as some of these requirements are burdensome on the service provider, the requirements should be brought to the negotiations early on, to ensure that compliance (i) will be possible and (ii) will not negatively impact indicative pricing.

> The requirements of the Executive Order apply to the institution, and it is the institution that holds regulatory responsibility ensure that the requirements are met – not the service provider

Ensure alignment with outsourcing policy

The institution may have defined additional requirements to the outsourcing agreement, or may have prescribed specific solutions to frequently-occurring issues when negotiating outsourcing agreements, e.g. certain companies may exclude service providers from certain countries, require specific organizational or technical measures to protect data, or require specific third-party certifications as a prerequisite for entering into an agreement.

Therefore, the outsourcing offcier should be aware of any such additional requirements when negotiating the agreement, and not limit the compliance check to the requirements of the Executive Order.

Ensure compliance contractual requirements

Appendix 2 to the Executive Order sets out minimum requirements to the outsourcing agreement. These requirements differ depending on whether the outsourcing is critical/important or not.

The institution should be aware that especially in larger outsourcings, the factual circumstances may change during the drafting and negotiation phase – e.g. new requirements from the business units or the need to lower prices may result in a change of the scope of services or the delivery model – therefore, the institution should continuously monitor whether any such changes have or could have an impact on the assessment on whether the outsourcing is critical or important.

Similarly, the institution should be mindful of the possibility that an outsourcing which initially was not considered critical or important might later during the term of the outsourcing qualify as such. An outsourcing that is not critical or important could become critical or important, if for example scope is or can be increased through calling options or increase the number of users or data stored with the service provider without having to re-negotiate the agreement.

Many service providers will need to use subsuppliers or have subsuppliers as part of their standard operating model. The use of subsuppliers ("chain-outsourcing") is allowed under the Executive Order. For critical or important outsourcings the institution must ensure (i) that the provider and the subsupplier have a written agreement which requires the sub-supplier to comply with applicable law and the contractual obligations, and (ii) that the chain-outsourcing does not limit the institution's, its auditor's or the FSA's right to audit and inspect the services.

The Executive Order dismisses the mandatory requirement under the old regulation of an 'active approval' of chain-outsourcing when the outsourcing is critical or important. Instead, the new regulation introduces the possibility for the parties to agree on an 'opt-out' model, according to which the institution can terminate the outsourcing agreement in the event the chain-outsourcing is not acceptable, e.g. if the risk profile is too high or if data would be transferred to locations that are not deemed safe.

Notification and approval phase

Notification of FSA

Prior to any critical or important outsourcing, the institution must notify the Danish FSA of the outsourcing in accordance with article 27 of the Executive Order and provide the FSA with certain information, which is to be included in the outsourcing register as described above. The current requirement is to provide the notification "in due time before the outsourcing" – further guidance is expected to be provided in the upcoming guidelines for interpretation. Outsourcing project managers should also be aware of the timing of the notification, as the notifications will likely have to be given at a time when the project will be in the negotiation phase and when there are plenty of other tasks to bear in mind.

Board approval

If the outsourcing requires the approval of the board of directors of the institution, the project responsible for the outsourcing should be aware that the process of obtaining board approval can be timeconsuming and requires preparation of background material which will form the basis for the decision – this work should not be underestimated and will often be required at key moments during the contract negotiations.

Best practice

We recommend that the institution adopts a standardized documents for the notification and approval processses. The institution could benefit from having a standard template for FSA notifications, which can serve as a checklist to ensure that all required information is provided to the FSA in due time.

Furthermore, the institution should adopt a "board approval framework", which sets out (i) which information in addition to the risk assessment needs to be provided to the board in order for them to make an informed decision, (ii) the format for such documentation, and (iii) the timeframe for providing the information to the board. The framework should be described in the outsourcing policy.

Follow-up phase

Outsourcing register and contract management

Whether or not the outsourcing is critical or important outsourcing, the necessary information must be included in the outsourcing register and, if the register is not kept as part of the contract management system, the contract management system must also be updated to ensure easy monitoring and follow-up.

The institution should start the ongoing monitoring and follow-up on the service provider's compliance with the terms of the agreement shortly after the agreement is signed. This includes following up on the reporting provided by the provider and ensuring that the business receives the services and receives them at the agreed quality levels.

Additionally, the institutions must continuously monitor whether the risks pertaining to the outsourcing change, e.g. additional concentration risks following new outsourcing to the same provider, change of ownership of the provider, or in some cases a deterioration of the political or economic situation of the location of the service provider.

Best practice

In order to fulfill ongoing follow-up requirement a structured approach to contract/vendor management should be adopted. This can be supported by simple artefacts such as checklists etc. to more sophisticated contract and vendor management support systems.

How can we assist you?

Kromann Reumert has one of the largest outsourcing practice groups on the Danish market and have several teammembers specialized in outsourcing in the financial sector. Below we have highlighted some of the areas in which we can assist you.

Drafting and Negotiation: Our key competence is assisting in drafting and negotiating outsourcing agreements which are both operational, flexible and compliant. We have assisted both financial institution and service providers in outsourcings subject to outsourcing regulation in a variety of different service areas.

We generally adopt pragmatic and businessoriented approach, while also ensuring compliance with all regulatory requirements – we do not attempt to overimplement the requirements, but seek to find operational solutions, which will meet the minimum requirements of the regulation and the institution' policy.

Compliance Artefacts: As highlighted throughout this handbook, we have developed template documents for all key compliance requirements, including for;

- Outsourcing policies,
- Outsourcing registries,
- Due Diligence checklists, and
- Standard contractual clauses.

Assessments: We have extensive experience in facilitating internal assessments of the financial institutions (e.g. risk assessments and assessments of critical or important outsourcing).

Contract Management: We can also provide access to our contract management system, which can be set up to serve as an outsourcing register as well. In addition to the master data on the agreements and suppliers, the contract management can be set up to include the additional information required – both for outsourcings in general and for critical or important outsourcings.

Our team

Søren Skibsted
Partner
Direct: +45 38 77 43 83
Mobile: +45 24 86 00 19
ssk@kromannreumert.com

Jette Hessellund Lauridsen
Partner
Direct: +45 38 77 43 57
Mobile: +45 24 86 00 49
jhl@kromannreumert.com

Carl Emil Alexander Frost
Attorney
Direct: +45 38 77 43 58
Mobile: +45 61 63 54 57
cef@kromannreumert.com

Thomas Wernblad Hansen
Attorney
Direct: +45 38 77 44 19
Mobile: +45 61 20 35 22
twh@kromannreumert.com

KROMANN REUMERT

At Kromann Reumert, we set the standard. Together. We provide value-adding solutions and advisory services with dedication and focus. We are driven by our four core values: quality, commercial understanding, spirited teamwork, and credibility. We are Denmark's leading law firm with offices in Copenhagen, Aarhus and London.

COPENHAGEN
SUNDKROGSGADE 5
DK-2100 COPENHAGEN Ø

AARHUS
RÅDHUSPLADSEN 3
DK-8000 AARHUS C

LONDON
65 ST. PAUL'S CHURCHYARD
LONDON EC4M 8AB

LAW FIRM
KROMANNREUMERT.COM
TEL +45 70 12 12 11