

The monitoring of outsourcing arrangements

In short The Dutch Authority for the Financial Markets (AFM) has conducted an assessment in the asset management sector and finds that the monitoring of outsourcing arrangements can be improved in several areas. The AFM provides recommendations concerning the qualification, the setup, the monitoring activities themselves, and monitoring in cases of intra-group outsourcing and ICT outsourcing. The AFM expects companies to incorporate the recommendations in this report into the ongoing management of outsourcing arrangements.

Management summary

Fund managers and investment firms are increasingly outsourcing more of their activities. Outsourcing can contribute to the efficiency and quality of business operations, but it also carries risks.

In recent years, the Dutch Authority for the Financial Markets (**AFM**) has therefore conducted assessments among investment firms, managers of AIFs and managers of UCITS regarding outsourcing arrangements in the asset management sector. This has provided the AFM with an overview of the material activities carried out by third parties and the control measures taken by companies in this regard ('Keten in Beeld').

In 2023, the AFM launched a new assessment into outsourcing arrangements. The aim of the assessment was to determine the extent to which investment firms, managers of AIFs and managers of UCITS comply with the laws and regulations applicable to them with regard to the ongoing management of outsourcing risks. This report provides an overview of the findings of the assessment and provides recommendations on how to manage outsourcing risks.

The assessment focused on the ongoing management of outsourcing risks. This mainly takes place during the monitoring of existing outsourcing arrangements, but already starts earlier in the process of the outsourcing cycle. Essential for the management of outsourcing risks is also the qualification of the outsourcing arrangements and the

set-up of the outsourcing relationship, which includes concluding contractual agreements with the service provider and determining which control measures are required.

This report therefore contains recommendations for the qualification, set-up and monitoring of outsourcing arrangements in the asset management sector.

Key findings include:

1. Companies do not always have a well substantiated approach to determining what should be considered outsourcing and which outsourcing qualifies as material.
2. When engaging in outsourcing arrangements, companies often insufficiently consider measures and agreements to anticipate appropriate monitoring.
3. Companies have very different approaches to the monitoring of outsourcing arrangements; a more consistent and substantiated risk-based approach is necessary.
4. For intra-group outsourcing arrangements, there is often (too) much reliance on informal measures and agreements.
5. Companies are not always aware of ICT components in outsourcing arrangements and the associated ICT risks.

Based on the assessment and the findings, the AFM has a number of recommendations for companies. An overview of these recommendations is provided in Annex I. Not all recommendations are equally relevant to every company. For example, some

recommendations are more relevant for companies of a certain size or for companies that outsource a specific type of activity.

The recommendations are intended to provide further guidance to legal requirements. They are not intended to serve as an exhaustive checklist for complying with laws and regulations on outsourcing, but should be read in conjunction with existing laws, regulations and guidelines on outsourcing.

In its assessment, the AFM also specifically reviewed ICT outsourcing arrangements. These are usually already covered by the current outsourcing rules. In most cases, the recommendations in this report are therefore also relevant to ICT outsourcing.

In this report, the AFM does not provide specific recommendations regarding the management of ICT risks in outsourcing arrangements. On 17 January 2025, financial entities will have to comply with DORA (Digital Operational Resilience Act, (EU) 2022/2554), which introduces a specific legal framework for third-party ICT services. We expect that companies are already working on implementing the DORA requirements. The AFM has included several observations on ICT outsourcing arrangements in the report.

Chapter 1 of the report contains an introduction that provides further information about the AFM's assessment, the legal framework and an outsourcing cycle, based on which the AFM explains the focus of the assessment. Chapter 2 of the report presents an overview of the findings identified by the AFM based on the assessment. Based on these findings, the AFM includes recommendations in Chapter 3 of this report, along with an explanation for each recommendation. ICT outsourcing is discussed in a separate chapter, where the AFM provides several observations. Finally, Chapter 4 of the report contains the conclusion.

Contents

Management summary	1
1. Introduction	4
1.1 Introduction	4
1.2 The outsourcing cycle and the focus of the research	4
1.3 Structure of the assessment	6
1.4 Legal framework	6
2. Findings	7
3. Recommendations	9
3.1 Qualification	9
3.2 Set-up	10
3.3 Monitoring	13
3.4 Intra-group outsourcing	16
3.5 Use of third-party ICT	18
4. Conclusions	21
Annex I: Recommendations	22
Annex II: Outsourcing flowchart	23
Annex III: Legal framework	26
Annex IV: ‘Keten in Beeld’ sector letter 2019, “assessing outsourcing” section	28

This is an English translation of the original Dutch text, furnished for convenience only. In the event of any conflict or difference in interpretation between the English and the Dutch versions, the original Dutch version will prevail.

1. Introduction

1.1 Introduction

Financial companies are increasingly outsourcing their activities. This development also applies to investment firms, managers of AIFs and managers of UCITS, hereinafter referred to as 'companies'. Outsourcing can increase the efficiency and quality of business operations, but it also carries specific risks. For this reason, the AFM has designated outsourcing as a supervisory priority for several years.

In 2018 and 2020, the AFM conducted the 'Keten in Beeld' assessments. These primarily focussed on the set-up of outsourcing, aimed at determining what companies outsource, to which service providers, and whether companies have written policies and procedures in place. Findings from these assessments have been shared with the sector by means of sector letters. These sector letters contain observations and points of attention that are still relevant for the management of outsourcing risks. See the letters from 28 November [2019](#) and 21 July [2021](#).

In 2023, the AFM launched a new assessment into outsourcing arrangements in the asset management sector¹. The aim of the assessment was to determine the extent to which companies comply with the laws and regulations applicable to them with regard to the ongoing management of outsourcing risks. This report provides an overview of the findings of the assessment and provides recommendations on how to manage outsourcing risks.

1.2 The outsourcing cycle and the focus of the research

A number of phases and activities can be distinguished in the management of outsourcing arrangements. These are represented in different ways in the industry and in literature. The outsourcing cycle below summarises these phases and activities for the purposes of this report.

Policy and governance

The organisational structure that facilitates controlled business operations is central to the outsourcing cycle. This includes, but is not limited to, written policies and procedures and a sound governance structure. Part of this is also a company's vision on outsourcing and how it qualifies outsourcing.

Phase 1. The selection of an outsourcing partner.

The first phase of a specific outsourcing arrangement includes the decision-making process regarding the outsourcing of activities, the subsequent selection process and due diligence on selected companies. This is followed by the completion of the analysis of the objective reasons for outsourcing, including the Cost Benefit Analysis (CBA).

Phase 2. The engagement with the service provider in the outsourcing arrangement.

This phase includes shaping the relationship with the service provider based on the scope of the services and the risks identified on that basis. The risk analysis forms the basis for the set-up of appropriate control measures, such as the identification of performance indicators (KPIs) and the design of continuity and exit plans. This will eventually be laid down in a contractual agreement.

1 Outsourcing arrangements specifically related to investment activities were not included in the assessment

Phase 3. The monitoring of outsourcing

Monitoring can be divided into continuous, periodic and event-driven control of the outsourcing relationship. Which form of monitoring and which monitoring measures are prioritised will vary per outsourcing arrangement.

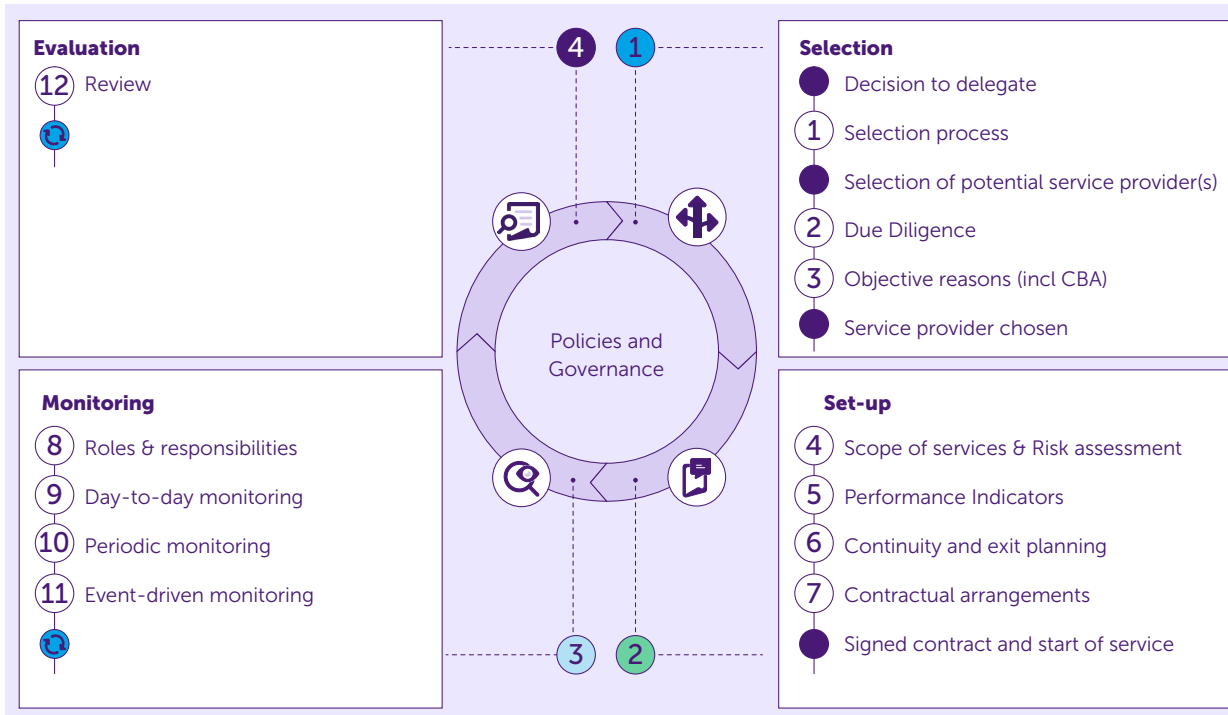
Phase 4. The evaluation of the outsourcing relationship.

This phase includes a periodic review of whether the outsourcing arrangement should be continued.

Managing the risks of outsourcing arrangements mainly occurs during the monitoring of existing outsourcing arrangements, but starts earlier in the process. Essential to the management of outsourcing risks are the qualification of the outsourcing and the set-up of the outsourcing relationship, including the arrangements made with the service provider and determining which control measures are required.

In addition to the monitoring phase (phase 3 in the figure below), the AFM will therefore also reflect on the set-up of outsourcing arrangements which takes place in the engagement phase (phase 2 in the figure below) and the qualification of outsourcing arrangements (in the central part of the figure below).

Figure 1. The outsourcing cycle - The below outsourcing cycle depicts four phases of an outsourcing arrangement, namely selection, set-up, monitoring and evaluation. Each phase has its own activities.



1.3 Structure of the assessment

With this assessment, the AFM aimed to gain further understanding of the extent to which companies are doing enough to manage the risks of outsourcing on an ongoing basis and, if necessary, to provide guidance for managing such risks.

The assessment consisted of two phases. First, the AFM selected fifty companies, varying in size and activities. These companies received a questionnaire containing questions about, for example, the (updated) scale of outsourcing arrangements, the set-up of monitoring measures, which functions are involved in monitoring and the risks that companies identified.

On the basis of the results of the questionnaire, six companies were selected from the previous selection of fifty companies. In-depth discussions about the monitoring of outsourcing were held with these six companies. These discussions focused on how companies practically implemented continuous risk management of outsourcing arrangements. Discussions were also held with several service providers in order to gain further understanding of their role in and vision on the management of outsourcing arrangements and the associated risks.

1.4 Legal framework

When outsourcing activities, companies must comply with Dutch and European laws and regulations. These rules also apply to the monitoring of outsourcing arrangements.

The AFM has previously drawn up a schematic overview of the relevant legal requirements for each type of company, included in Table 1 of the 'Keten in Beeld' sector letter of 2019. This is included as Annex III to this report. Furthermore, both the sector letter from 2019 and the sector letter from 2021 include guidance for the qualification of the outsourcing of activities and the set-up of control measures, including monitoring, included as Annex IV to this report.

If a company is unsure how best to set up control measures in accordance with the regulations that apply to it, guidelines on managing outsourcing risks under other regulations or by other (supervisory) bodies, such as the good practices of the Dutch Central Bank or the guidelines of the European Banking Authority (EBA)², may provide practical depth.

The report is based on the laws and regulations as they apply at the time of publication. Following the publication of this report, on 17 January 2025, DORA will come into force. DORA includes requirements on the control of ICT third-party risk, which aligns with this report.

This report contains recommendations for the practical implementation of the existing standards for outsourcing in general. In principle, these are relevant to all outsourcing arrangements, including ICT outsourcing. To the extent that compliance with certain recommendations in this report would be incompatible with the obligations under DORA, the latter should take precedence.

To the extent that specific recommendations are needed with regard to ICT outsourcing, these are more appropriate within the framework of DORA. Therefore, this report does not contain any specific recommendations on outsourcing arrangements with ICT components. However, the AFM did have several observations about ICT outsourcing during the assessment. These are included in the report.

The AFM expects outsourcing to remain high on the agenda of international legislative and supervisory bodies. For example, the recently published AIFMD review (Directive (EU) 2024/927) also includes several developments in the field of outsourcing. The AFM advises companies to closely monitor developments and, if necessary, to follow up in a timely manner.

² For example the EBA Outsourcing Guidelines (EBA/GL/2019/02, 25 February 2019), which are currently not applicable to companies in the asset management sector (except class 1 investment firms). The guidelines will be revised in the future, and their scope may be adjusted.

2. Findings

Broadly speaking, the AFM's assessment results in five overarching findings. The first three findings are generic, while the last two relate to specific situations. In the next chapter, the AFM makes recommendations for each of the five findings.



Finding 1 - Qualification

Companies do not always have a well substantiated approach to determining what should be seen as outsourcing and which outsourcing qualifies as material.

As part of the assessment, a list of both material³ and non-material outsourcing arrangements was requested. Upon further inquiry, it became clear that the concept of outsourcing was often interpreted too narrowly. Additionally, the approaches companies used to determine which outsourcing was material were often unsubstantiated and not consistent. Notably, the guidelines with regard to the qualification of outsourcing, as included in the 'Keten in Beeld' sector letter of 2019, were frequently not followed. Misclassification may result in insufficient control measures being implemented.



Finding 2 - Set-up

When engaging in outsourcing arrangements, companies often insufficiently consider measures and agreements to anticipate appropriate monitoring.

The monitoring activities related to outsourcing take place (among other things) on the basis of documents provided by the service provider, such as reports and certifications. This requires that the risks have been identified at an earlier stage, and that proper agreements have been made on this basis about the services and documents that the service provider will provide. The assessment showed that the link between this earlier set-up phase and the later monitoring phase had not been sufficiently established in all cases. This can lead to a lack of clarity about the responsibilities and rights between the company and the service provider during the monitoring phase, as a result of which risks are insufficiently identified and managed by the company.

³ The term 'material' is used in this report to refer to outsourcing of activities that fall within the scope of the outsourcing rules in the Financial Supervision Act and European sectoral regulations. For the purposes of this report, 'material' is understood to mean outsourcing as referred to in the definition of outsourcing in Section 1:1 of the Financial Supervision Act 'critical and important' as referred to in Article 16, paragraph 5, of MiFID II (Markets in Financial Instruments Directive, (EU)2014/65) and Article 31 of MiFID II Delegated Regulation 2017/565, the 'functions' as referred to in Article 20 of the AIFMD and Annex I of the AIFMD (Alternative Investment Fund Management Directive, (EU)2011/61) and as referred to in Article 13 of the UCITS Directive and Annex II of the UCITS Directive (Undertaking for Collective Investment in Transferable Securities Directive, 2009/65/EC).



Finding 3 - Monitoring

Companies have very different approaches to the monitoring of outsourcing arrangements and do not always use the most appropriate methods to manage the risks of outsourcing; a more consistent and substantiated risk-based approach is necessary.

It is up to companies to determine the necessary form and frequency of monitoring, depending on the specific risks associated with outsourcing arrangements. It is expected that the monitoring of outsourcing of similar activities, with similar risks, will take place in a similar way. The assessment indicated that the outsourcing of similar activities was monitored differently by different companies, which could not always be explained by the specific risks. For example, companies have very different approaches to assessing certifications from the service provider. The form and frequency of review interviews with the service provider also differ from company to company, even if the same services are used. Companies were often insufficiently able to explain these differences. It is important that companies can sufficiently substantiate why they opt for a certain form and frequency of monitoring.



Finding 4 - Intra-group

For intra-group outsourcing arrangements, there is often (too) much reliance on informal measures and agreements.

Within groups, resources are often utilised through arrangements such as central services provided by the group ('shared services'). From a practical point of view, companies often do not see this as outsourcing, whereas according to the laws and regulations it often is. In practice, monitoring of these intra-group arrangements is also often informal and/or (too) limited. When weighing the risks, the degree of control over the service that has been outsourced and the group service provider can be taken into account, but this does not mean that monitoring does not have to be set up. Although companies often assume that interests within the group are always the same, this is not always the case in practice. Companies can therefore not rely entirely on the group function and must implement appropriate control measures themselves.



Finding 5 - ICT-specific

Companies are not always aware of ICT components in outsourcing arrangements and the associated ICT risks.

In many outsourcing arrangements, the service provider uses ICT, including (web) applications, data processing and storage. However, these ICT components in outsourcing have their own ICT risks. Companies do not always pay sufficient attention to these ICT components and their risks, such as risks related to the availability, integrity and confidentiality of the processed data.

3. Recommendations

In this part of the report, the AFM makes a number of recommendations for each finding, as described in Chapter 2, with regard to the ongoing control of outsourcing arrangements. This part of the report also contains specific observations with regard to ICT outsourcing.

3.1 Qualification

Companies have different approaches to determining what should be considered outsourcing and what outsourcing qualifies as material. The AFM has previously provided guidance on this in the 'Keten in Beeld' sector letter (see Annex IV). This guidance still applies but does not seem to have been followed sufficiently.

The AFM therefore makes a number of recommendations for a more appropriate qualification with regard to outsourcing.



Recommendation 1 - Definition

Draw up a written policy that outlines how to determine whether an arrangement qualifies as outsourcing.

It is important for companies to draw up policies and procedures that clearly define when arrangements qualify as outsourcing. In doing so, companies may take into account the considerations set out in Annex II. It is also important to document the analyses and their results for each situation. When applying the procedures, sub-outsourcing must also be taken into account. Sub-outsourcing occurs when the service provider to whom the contract has been outsourced also outsources all or part of the activities in question. After all, a company that outsources is responsible for all risks, and that includes sub-outsourcing. Sub-outsourcing is particularly common in the use of ICT systems, for example through the hosting of ICT systems in the cloud.

The AFM's assessment showed that many companies often do not qualify arrangements with third parties as outsourcing without a documented analysis or substantiation. This mainly concerns outsourcing to parties where personnel, services or systems are used. Many companies see this as '*procurement*', '*insourcing*', '*standardised services*' or '*support*'. We note that in those cases the arrangement often actually constitutes an outsourcing arrangement.

Due to an incorrect classification, possible risks are potentially insufficiently identified and the control measures are often insufficient. For example, companies regularly assumed that the exception for standardised services in MiFID II could be applied broadly, such as for software. The term 'standardised service' should however be interpreted narrowly. For example it does not necessarily include all 'off-the-shelf' products.



Recommendation 2 - Material activities

Establish written procedures that specify how to determine which activities are considered material. Do not interpret these concepts too narrowly.

It is important to describe clearly in the written policies and procedures how a company determines whether activities are material. As with the qualification of outsourcing, it is also important to document this for each outsourcing arrangement.

For the sake of completeness, we note that companies must always take appropriate control measures to ensure controlled business operations. This means that even if activities are not material, appropriate control measures must be implemented.

The term 'material' is used in this report to refer to outsourcing of activities that fall within the scope of the outsourcing rules in the Financial Supervision Act and European sectoral regulations, to which no exception applies. This is explained below in more detail for companies that fall under MiFID II and companies that fall under the AIFMD.

Companies covered by MiFID II were regularly found to assume incorrectly that activities are not material. The explanation was, for example, that alternative service providers were available or that the activities did not relate to a primary process. However, the criterion of 'critical and important' that applies under the MiFID II framework should be interpreted broadly. For example, it is important not only whether the continuity of the company is impaired when problems arise in the outsourcing arrangement, but also whether the company can no longer meet legal and regulatory obligations due to problems with the outsourced activities. As a result, in practice, many outsourcing relationships will in fact have to be regarded as critical or important. For example, activities such as financial administration and support for control functions (compliance, risk management, and internal audit) should, in principle, be considered outsourcing of 'critical or important' functions or activities that support those functions.

Companies that are subject to the AIFMD regularly appeared to apply too narrow a scope to the outsourcing rules in the AIFMD, frequently based on overly restrictive interpretations of the activities listed in Annex I of the AIFMD. The limits on the application of the outsourcing rules under the AIFMD relate to supporting tasks and these should be interpreted in a limited way (e.g. catering, cleaning and 'one-off' expertise and advice).

During the assessment, the AFM noticed that, in the context of property management, activities beyond day-to-day operational management at the object level were sometimes not considered part of Annex I of the AIFMD. However, as indicated in point 2(c) of Annex I, these activities should be included, particularly regarding facilities management and property management.

3.2 Set-up

The set-up of the outsourcing relationship is essential for proper monitoring. When initiating an outsourcing arrangement, companies do not always think sufficiently about measures and agreements that anticipate appropriate ongoing management of the outsourcing arrangement. Below, the AFM makes a number of recommendations for a more appropriate set-up of outsourcing relationships.



Recommendation 3 - Policies and procedures

Draw up written procedures detailing how outsourcing risks are identified and managed **for each outsourcing arrangement**.

Written policies and procedures are fundamental for the continuous management of possible risks associated with outsourcing arrangements. However, the assessment showed that written procedures were often insufficiently detailed, resulting in a lack of a structured process with regard to monitoring.

A procedure should specify who does what, when and how, for the ongoing management of outsourcing risks. It is therefore relevant to draw up a procedure for each outsourcing arrangement in which this is specified. For an consistent and efficient approach, companies could benefit from using standard templates and, for example, templates with fixed review criteria or evaluation criteria.



Recommendation 4 - Comprehensive overview

Maintain a comprehensive overview that includes essential elements of all established outsourcing arrangements.

The assessment showed that companies did not always have an overview of outsourcing arrangements. As a result, the process of identifying existing outsourcing arrangements was sometimes complicated and lengthy. In order to manage outsourcing arrangements and the associated risks, it is essential to have a comprehensive overview.

This overview should include the following key elements of sub-outsourcing relationships⁴:

1. a unique number for each sub-outsourcing arrangement;
2. important information about the service provider, such as name, address and contact details;
3. the start date, the date of contract renewal and/or the end date of the outsourcing agreement, including any termination notice periods;
4. the type of outsourced activities;
5. the classification of the service as material or not-material;
6. whether an ICT service is involved, including the type of data associated with the outsourcing;
7. the country from which the activities are performed/from which the data is processed;
8. essential information on sub-outsourcing.

This is not an exhaustive list. It is up to the company to decide for itself which information is useful to include in this overview.

⁴ These are some of the requirements that apply with the entry into force of DORA with regard to a register in the case of agreements on the use of ICT services provided by third-party providers, see Article 28(3) of DORA. The ESMA Guidelines on Outsourcing to Cloud Service Providers also provide requirements for a register of outsourcing of cloud services. These requirements could also be used for other forms of outsourcing.



Recommendation 5 - Risk analysis

Conduct a risk analysis both ex-ante and at least annually. Then determine, for each outsourcing arrangement, which control measures are appropriate.

It is important for companies to carry out a risk analysis prior to entering into an outsourcing arrangement. The aim is to identify the control measures that need to be implemented. A risk analysis may include examining the nature and type of performance indicators, the use of access rights, information and audit rights, the frequency and content of reports, certification, review and escalation options.

A risk analysis should be repeated at least annually in order to identify any changes in risks and to adjust control measures in a timely manner if appropriate. In the case of specific events, such as changes or incidents, it may be necessary to evaluate the risk analysis on an ad hoc basis and revise it where necessary.

In principle, the risk analysis is carried out by the first-line functions, with the control and involvement of the second-line risk function. These functions must therefore have sufficient knowledge of possible risks associated with the outsourcing arrangement and the activities that are outsourced.

It is clear that the control measures will not be the same for all outsourcing arrangements, as the risks of outsourcing arrangements may differ. For example, the risks of outsourcing compliance and risk functions will often focus on quality and timeliness, where control through regular review interviews may be one of the appropriate measures. When outsourcing investment management, it is easier to measure the risks quantitatively, so that reporting, certifications and information and audit rights can be (partly) used as control measures.



Recommendation 6 - Responsibility

Assign the (ultimate) responsibility for the outsourcing arrangement and the monitoring activities to specific persons who have appropriate knowledge and experience. Make sure there is a clear division of tasks within the board, determining who is responsible for which outsourcing arrangement.

It turned out that most companies appoint a specific director as the person ultimately responsible for each outsourcing arrangement. This is usually the director who already has the relevant process in their portfolio. The ultimate responsibility for the outsourcing of the compliance and risk function or activities is often assigned to the Chief Compliance Officer or Chief Risk Officer. First-line functions are often assigned to the Chief Operational Officer or Chief Investment Officer. Responsibility for the internal audit function generally lies with the Chief Executive Officer.

A number of companies assessed chose not to appoint one or more specific responsible directors. The following reasons were given:

1. The board has collective responsibility for the outsourcing arrangement.
2. The responsibility is not assigned to the board, but it is, for example, assigned at a lower (management) level.
3. The responsibility lies outside the company, for example with a group entity or with the third party to whom the activity has been outsourced.

According to the AFM, the reasons above do not provide for proper governance of outsourcing arrangements. The board ultimately has collective responsibility for the company, including arrangements. It is good to agree on and document a division of tasks, because in practice not everything can be done by the collective board. In this division of tasks, take into account the knowledge and experience of the board member. Failure to appoint a specific responsible board member reduces the chance that sufficient responsibility can be taken at board level for the outsourced activities.

Additionally, more employees are involved in the monitoring of outsourcing arrangements, including first-line monitoring as well as the risk and/or compliance functions. Along with having clear responsibilities, they must also possess the appropriate knowledge and experience for their monitoring roles.



Recommendation 7 - Contractual agreements

Establish contractual agreements that specify how the services will be evaluated, who is responsible for the assessment, the minimum topics to be covered in the service reports, and the reporting frequency.

Companies need to have contractual agreements that specify the service provision and what the company needs for its monitoring. These points are laid down in an agreement. Several legal requirements apply in this regard. For example, the agreement, including the service level agreement (SLA), must in any case contain a clear description of the service, and inspection and audit rights must be included. In addition, the agreement should also set out the most important criteria for monitoring, such as:

1. The performance goals;
2. The content and frequency of reports;
3. The information that the service provider provides to the company about its control measures, for example the type and frequency of certifications and external audits;
4. The procedure in the event of incidents within the service provider and the resolution of the incidents;
5. The process on the use of sub-outsourcing, including the exchange of information necessary to manage the risks of sub-outsourcing;
6. The escalation line in case of possible problems in the service. It is preferable that, when mitigating the problem, consideration is given not only to seniority but also to who has the knowledge or skills. If necessary, a lower-level employee is involved;

7. The way in which the company is informed by the service provider in the event of impactful changes (e.g. sub-outsourcing) that affect the outsourced activities;
8. Agreements regarding a (typically) annual review of the outsourcing arrangement, as well as ad hoc meetings when necessary;
9. Testing the service provider's business continuity plan, including the reporting on it.



Recommendation 8 - Agreements on escalation

Set up an escalation structure with escalation options at different levels and, if relevant, for both operational functions and second-line functions.

Setting up an escalation structure in advance is important in order to respond to problems or concerns in a timely manner when necessary. The escalation structure contains escalation options at different levels of the company. In this way, a minor operational issue requiring urgent attention can be escalated immediately at work floor level and discussed with the service provider. In addition, a significant problem can be escalated to the relevant board member with ultimate responsibility.

If relevant, the escalation structure will also consider different escalation options for the operational functions and for the second line functions. In the event of operational risks, first line functions will be principally involved. The second line function must be involved if certain risks occur, such as privacy-related risks.

3.3 Monitoring

Monitoring of outsourcing arrangements includes the continuous, periodic and event-driven oversight of the outsourcing relationship. Continuous monitoring mainly refers to daily oversight by the first line using tools such as dashboards and reports. Periodic monitoring involves testing service delivery at set intervals, with control functions often playing an important role. Companies may exercise their right to information, inspection and access, such as reviewing audit reports.

Monitoring not only takes place on a daily and periodic basis, but may also be triggered due to certain events or deviations. This mainly concerns incidents in the company and/or the service provider, as well as changes in services.

The AFM has observed that companies deal with monitoring very differently and do not always manage the risks of outsourcing arrangements properly. Below, we provide recommendations for appropriate monitoring of outsourcing arrangements.



Recommendation 9 - 3 Lines of Defence (3 LoD)

When outsourcing activities, assign tasks and responsibilities to operational functions ('first line') and control functions ('second and third line') for monitoring the outsourcing arrangement (3 LoD).

The first line is primarily responsible for monitoring the outsourced activities. This is done by analysing and monitoring the service provider's performance on a daily basis. The presence of staff with sufficient knowledge, capacity and resources to perform these tasks is required.

It is the responsibility of the second-line functions (risk and compliance) to periodically check that the monitoring has been adequately set up and carried out. The third line, or the internal audit function, is involved in periodically reviewing the process regarding the outsourcing arrangement and its monitoring.

In the outsourcing of control functions, the first line is generally not involved in monitoring the outsourcing arrangement, with responsibility resting directly with the second and third lines. If the control function consists of one person and the function is outsourced, the responsibility for monitoring lies with one of the directors.

If there is an outsourcing of first-line functions, it is not desirable that tasks and responsibilities are only assigned to the control functions for monitoring the outsourcing arrangement.

**Recommendation 10 - Control framework**

Maintain a central control framework in which the control measures are documented.

A well-documented central control framework is important because it sets out how the risks are mitigated in a consistent and balanced manner. The control framework contains information for each outsourcing arrangement and for each control measure it specifies the action that must be taken to implement the control measure, who is responsible, with what frequency and what the deadline is for carrying out the control measure, what reporting and recording must be done and what the status is of the (execution of the) control measure.

The control framework is not static. The control measures are linked to a risk analysis as their purpose is to mitigate risks. The risk analysis should be reviewed periodically or after an incident. If necessary, the control framework must be adjusted.

**Recommendation 11 - Performance indicators (KPIs) for reporting**

Monitor outsourcing arrangements by means of both quantitative and qualitative KPIs and use service reports with an appropriate frequency.

As mentioned in recommendation 7, it is important to include performance targets in the contractual agreements. Quantitative and qualitative performance indicators make it possible to continuously monitor the agreed service levels so that immediate corrective action can be taken if necessary. Adequate KPIs can also contribute to effective management of the service provider.

Once the performance goals have been set, the next step is to make these goals measurable and convert them into quantitative and qualitative performance indicators. Quantitative performance indicators include, for example, the number of hours someone performs certain activities or the benchmark in case of investment management. Qualitative performance indicators relate, for example, to satisfaction with the service or the quality of incident handling.

Subsequently, agreements can be made with the service provider about the frequency and access to service reports on individual KPIs. These reports can be made available in various ways: written reports by e-mail, access to a dashboard or access to the systems from which the necessary reports can be requested. Finally, it is important not only to assess whether the agreed service levels are being met, but also to monitor trends and developments that may exceed threshold values over the long term. For example, by setting preventive thresholds and proactive alerting, such as a 10% increase in incident resolution time or one minute of downtime of a portal, it is possible to prevent this negative trend continuing unnoticed in the longer term and the KPI ultimately not being met. The performance targets can be periodically evaluated together with the service provider.

The AFM believes that both quantitative and qualitative criteria should generally be used to gain comprehensive insight into performance. It is important to tailor the set of quantitative and qualitative criteria to the specific outsourcing arrangement.



Recommendation 12 - Audit reports

Review available third-party audit reports periodically in terms of the validity, scope, depth and findings.

Available audit reports must be included in periodic monitoring. They offer deeper insights into the controls of outsourced activities and assess compliance with established agreements or applicable standards. An audit can be carried out by the company on the service provider's premises or by an independent party on behalf of the company, for example as part of a certification. Based on the audit/information right in a contract, many service providers make their own certifications or assurance reports available to reduce the number of audits of their customers. The independence of these reports can be guaranteed by having them conducted by an external party on the basis of internationally recognised standards.

A well-known example concerns the annual accounts audits or a ISAE3402 statement. In the ISAE3402, the controls of the service provider are tested, which may include the financial control measures and the ICT control measures. To test the control measures regarding information security, there are a number of more specific audit reports that are often used, such as an ISO 27001 certification or a SOC2 type II (ISAE 3000) report. Reports provide insight into the controls that the service provider has set up and/or used through an independent auditor and are internationally recognised. The various reports are different in methodology and depth.

For periodic monitoring, it is therefore important for a company to consider which (independent) audit reports are needed to gain more insight into the control of the outsourced activities by the service provider. Available audit reports must be provided to enable the company to conduct its own assessment. During the evaluation, companies should pay attention to the validity, scope and depth of the reports received. The company then discusses their evaluation with the service provider and monitors the resolution of any findings. If the available audit reports are insufficient to adequately review the controls, the company should consider conducting or commissioning a periodic audit.



Recommendation 13 - Incidents within the service provider

Establish a clear and documented incident procedure for handling incidents involving service providers.

If an incident occurs within the service provider, a pre-established procedure ensures that any negative consequences for the company remain limited. It is therefore important to make agreements with the service provider about resolving incidents. Among other things, a clear division of tasks must be established for all parties involved and agreements must be in place, regarding communication in the event of impactful incidents. It is important for companies to have access to information related to incidents. Progress can be monitored, for example by accessing the service provider's ticketing system. This allows companies to effectively monitor incident management.

An incident within a service provider may pose a threat to the integrity of the company's business operations and therefore fall under a company's legal obligation to report incidents to the AFM without delay. A condition for complying with this requirement to notify the AFM is making agreements with the service provider about the delivery of incident reports, with a root cause analysis and an action plan.

3.4 Intra-group outsourcing

For intra-group outsourcing arrangements, there is usually (too) much reliance on informal measures and less robust controls. Companies assume that the group's interests always align with the company's interests and the various customer interests. This is not always the case.

In principle, everything that is arranged for external outsourcing must also be arranged for intra-group outsourcing. The laws and regulations, as well as the explanatory notes, are clear about this. The above-mentioned recommendations are therefore also intended for intra-group outsourcing arrangements. However, it may be appropriate to apply different nuances to intra-group outsourcing. Below, the AFM provides a number of recommendations and clarifications, specifically for the purpose of intra-group outsourcing arrangements.



Recommendation 14 - Group staff support

In the case of intra-group outsourcing arrangements, reflect in the written policy that staff support from group entities often qualifies as outsourcing and ensure appropriate control measures are in place.

Companies often mistakenly do not qualify personnel support from the group (often referred to as 'shared services' or 'support') as outsourcing. This support is not necessarily exempt from the outsourcing requirements. Also, the same risks are often present, which means that control measures remain necessary. However, the company may have influence over the measures taken by the service provider. This can be taken into account, for example in the depth of the application of certain control measures.

In addition, we regularly see that companies that qualify staff support from the group as outsourcing do not take sufficient control measures because they do not consider this necessary given the group situation.

The qualification can indeed be complex. The diagram in Annex II therefore contains considerations that can be used to obtain an indication of whether or not an arrangement constitutes outsourcing.



Recommendation 15 - Managing risks of intra-group

In the case of intra-group outsourcing arrangements, ensure that appropriate control measures are in place, aligned with the intra-group practices and associated risks.

In the case of intra-group outsourcing, a company remains responsible for the management of possible risks of outsourcing. Therefore, the mere fact that an outsourcing arrangement is of an intra-group nature is not in itself a reason to implement more limited control measures.

In the case of intra-group outsourcing, group policies and procedures can be (partially) utilised in order to pursue consistency within the group. However, documented procedures specific to the company that describe how the company implements its own controls need to be in place. The interests of the company relative to the group or the influence of the company on the service provider may be taken into account.

Invoking the principle of proportionality is not self-evident for intra-group outsourcing. Reliance on Article 31(4) of MiFID Delegated Regulation 2017/565 – which allows taking into account the extent to which the company controls the service provider or can influence its actions in complying with the outsourcing obligations – is also not justified for every intra-group outsourcing arrangement. Companies cannot simply assume that, because their service provider is a group company, they can actually influence the actions of the service provider, especially when the service provider is the parent company.

In addition, companies should not automatically assume that intra-group outsourcing arrangements involve fewer risks. However, intra-group outsourcing often has a different risk profile and this can be taken into account in the set-up of the outsourcing arrangement

and the associated control measures. For example, direct access to systems or people can influence the type, frequency or intensity of required reports.

In the case of intra-group outsourcing, the legal requirements regarding outsourcing should be appropriately implemented. For example, in some cases the cost-benefit analysis may be more concise, with less comprehensive mapping of the cost framework of multiple external service providers. However, it is important that the costs of the service are also determined in the case of outsourcing within the group, partly in order to make a clear cost comparison and assessment when appointing a service provider.



Recommendation 16 - Intra-group agreements

Ensure that monitoring arrangements for intra-group outsourcing are formalised in a contract.

Drawing up a written outsourcing contract is a legal requirement, also for intra-group outsourcing arrangements. The AFM notes that companies generally comply with this, but that the contracts are often insufficiently specific, especially in the case of intra-group outsourcing arrangements.

If outsourcing takes place within the group, specific contractual agreements should clearly state that the company remains responsible for the outsourced activities. With regard to monitoring, it is crucial for intra-group outsourcing arrangements that the scope of the services and activities is clearly specified, that clear quantitative and qualitative performance indicators are agreed upon and that contractual agreements are made regarding the reporting and evaluation of the outsourced activities. This applies to all types of intra-group outsourcing.



Recommendation 17 - Intra-group interests

Create and document a written analysis specifically regarding intra-group conflicts of interest.

The AFM's assessment showed that the identification, prevention and management of potential conflicts of interest is not always given explicit attention in intra-group outsourcing arrangements. Companies often assume that all interests within the group are aligned.

The AFM notes that, at least in parts of the relationship, there may be potentially divergent interests. An example is the allocation of resources across entities. It is therefore important to carry out a thorough analysis in this area, both when initiating the outsourcing relationship and on an ongoing basis.



Recommendation 18 - Dual functions

Establish a documented process around dual roles (dual hatting) and associated potential conflicts of interest.

The AFM's assessment showed that in the case of intra-group outsourcing arrangements there are often situations of dual hatting in which daily policymakers, managers and employees have a role both in the company and in the intra-group service provider. In that case, it is not always clear in what capacity or role the employee in question is acting.

It is therefore important to appoint a person with ultimate (local) responsibility in the board of the company. In this case, a dual function is only possible if, besides the ultimate responsibility for the outsourcing relationship, the relevant person is not directly involved in the outsourcing from the side of the (internal) service provider.

Furthermore, it's important to document how roles and responsibilities are divided in the event of dual functions during outsourcing, and how potential conflicts of interest are managed.



Recommendation 19 - Group monitoring

Define the company's responsibilities regarding the monitoring activities if a group entity conducts all or part of the monitoring of the (intra-group) outsourcing arrangement.

If activities are outsourced within a group, monitoring is also required. Sometimes, parts of the monitoring activities are carried out by individuals within the group. In such cases, it is important to clearly define and document the tasks and responsibilities between the company and the (group) service provider in advance. Potential conflicts of interest should also be considered. It is crucial to ensure that the management of outsourcing risks remains sufficiently autonomous and independent.

If outsourcing takes place within the group and the monitoring of the outsourcing is carried out by a group entity, the company remains responsible and ensures that the monitoring is performed adequately. This requires, at a minimum, a review of the monitoring, such as on the basis of monitoring reports. The company must document the controls.

In the case of outsourcing of activities to a group entity, there may be sub-outsourcing if contracts are concluded at group level with service providers. The rules on sub-outsourcing are then fully applicable.



Recommendation 20 - Escalation in intra-group outsourcing

In case of intra-group outsourcing arrangements, make sure that escalation can take place up to the level of the company's board.

If outsourcing takes place within the group, the company's staff must have the opportunity to escalate problems with the intra-group service provider to the level of the company's board.

In some cases, we have seen that there was no escalation to the board of the company but only to a group entity. Therefore, we stress that the possibilities for escalation should not only be set-up to a group entity, in order to avoid possible conflicts of interest within the group.

3.5 Use of third-party ICT

The business operations of financial companies have become increasingly dependent on ICT resources. As a result, ICT risks have also increased. This development also has consequences for situations in which the company uses ICT provided by third parties.

In this report, the AFM does not make any specific recommendations with regard to the management of ICT risks in the event of outsourcing. This is because financial entities will have to comply with the requirements of DORA from 17 January 2025. DORA contains detailed requirements for the use of ICT services from third parties. It is expected that the European Supervisory Authorities will provide additional information and guidance (such as Q&As). The AFM expects that the companies have already started implementing DORA in order to comply with these regulations on time.

In the assessment, the AFM made a number of observations with regard to the monitoring of ICT outsourcing that received insufficient attention. As these observations can have a substantial impact on the control of business operations, they are included in this report and are explained on the next page.

**Observation 1 - ICT knowledge within companies is sometimes insufficient**

During the assessment, the AFM identified instances where basic knowledge about ICT was lacking. This can lead to additional risks for the company. The AFM expects individuals within a company to have appropriate knowledge, as referred to in recommendations 6 and 9. This includes knowledge of ICT risk management and information security. This also applies to ICT supplied by third parties. ICT knowledge is needed by all individuals involved, such as daily policymakers and the control and monitoring functions.

**Observation 2 - ICT risks are not always fully taken into account in the risk analysis**

Outsourced activities often involve the use of ICT resources. It turned out that the associated ICT risks were not always fully included in the company's risk analysis. The AFM points out that adequate insight into the activities of the service provider is important in order to identify the ICT components and the associated data processing. Subsequently, in addition to recommendation 5, it is important that companies explicitly consider specific ICT risks in their risk analysis, such as the risks related to the availability, integrity and confidentiality of the processed data.

**Observation 3 - Responsibility for information security is not always clearly assigned**

The AFM's assessment showed that companies assume that the responsibility for information security often lies (at least in part) with the service provider. In such cases, companies take little or no control measures of their own. However, the company itself remains ultimately responsible for its information security. It is important to reflect this in the written procedures and the agreement with the service provider.

Based on the conducted risk analysis, the company can determine an adequate level of protection for the processed data. As mentioned in recommendation 10, it is important to make agreements with the service provider about the necessary control measures and how they can be monitored. Companies must determine which control measures must be set up and monitored by the company itself. An example is that a service provider conducts the technical implementation of identity and access management in an ICT system, but that the company itself approves changes to access rights and periodically checks them.

It is therefore important that the division of tasks between the company and the service provider for ICT control measures is clear and properly defined. The division of tasks depends on the type of service and the appropriate level of protection based on the associated risk analysis.

**Observation 4 - Information sources for monitoring ICT outsourcing are not always used**

In the case of ICT outsourcing, it is essential that companies monitor the performance and capacity of the outsourced ICT components themselves. Many companies receive (automated) reports or have access to dashboards provided by the service provider. These are crucial sources of information to monitor quantitative KPIs. They enable companies to take timely measures in collaboration with the service provider to ensure the availability and security of the systems, such as scaling up capacity in a timely manner.

**Observation 5 - Agreements do not always contain sufficient detail about the approach to impactful changes**

The AFM's assessment also reveals that not all companies have established a clear approach on how to deal with impactful changes by the service provider, such as sub-outsourcing, patching and

system upgrades. Impactful changes can pose risks to the quality and continuity of the service. To effectively monitor these risks, it is crucial to have contractual agreements in place with the service provider specifying how the company will be notified of any impactful changes affecting the outsourced IT service. This ensures that the quality and continuity of the service are proactively monitored and any necessary precautionary measures can be implemented.



Observation 6 - Insufficient use of resilience testing reports

Some companies use penetration tests for periodic monitoring of their ICT risks. These tests are designed to assess the effectiveness of information security measures by identifying vulnerabilities in ICT systems or applications. These vulnerabilities are then exploited to gain access to the systems. Often, service providers will carry out these tests or have them carried out by an independent party on their systems. If internal or external penetration testing is not being done, companies can make arrangements with the service provider to have these tests performed. In this context, it may be relevant to make agreements with the service provider about the type of tests, the scope, the frequency and whether they are performed by an internal or external party.

Penetration testing is a useful tool to ensure continuity of services and thus effectively manage the risks of outsourcing. From 17 January 2025, DORA will require many companies to test their digital operational resilience.

4. Conclusions

In its assessment, the AFM notes that companies have set up and are implementing monitoring of their outsourcing arrangements. However, companies regularly use assumptions that lead to insufficient management of outsourcing risks. This is reflected in the five findings described in this report. For example, companies sometimes do not have a consistent process in place to reach a correct conclusion about what is and is not covered by the outsourcing regulatory requirements. In addition, the set-up of the outsourcing arrangement is often insufficiently geared to monitoring and sometimes lacks a consistent and substantiated risk-based approach. Also, specific situations are sometimes not handled properly, in particular outsourcing within the group and ICT outsourcing.

The AFM has drawn up recommendations for the management of outsourcing risks. It expects companies to take the recommendations in this report into account in the ongoing management of outsourcing arrangements.

Annex I: Recommendations

1. Draw up a written policy that outlines how to determine whether an arrangement qualifies as outsourcing.
2. Establish written procedures that specify how to determine which activities are considered material. Do not interpret these concepts too narrowly.
3. Draw up written procedures detailing how outsourcing risks are identified and managed for each outsourcing arrangement.
4. Maintain a comprehensive overview that includes essential elements of all established outsourcing arrangements.
5. Conduct a risk analysis both ex-ante and at least annually. Then determine, for each outsourcing arrangement, which control measures are appropriate.
6. Assign the (ultimate) responsibility for the outsourcing arrangement and the monitoring activities to specific persons who have appropriate knowledge and experience. Make sure there is a clear division of tasks within the board, determining who is responsible for which outsourcing arrangement.
7. Establish contractual agreements that specify how the services will be evaluated, who is responsible for the assessment, the minimum topics to be covered in the service reports, and the reporting frequency.
8. Set up an escalation structure with escalation options at different levels and, if relevant, for both operational functions and second-line functions.
9. When outsourcing activities, assign tasks and responsibilities to operational functions ('first line') and control functions ('second and third line') for monitoring the outsourcing arrangement (3 LoD).
10. Maintain a central control framework in which the control measures are documented.
11. Monitor outsourcing arrangements by means of both quantitative and qualitative KPIs and use service reports with appropriate frequency.
12. Review available third-party audit reports periodically in terms of the validity, scope, depth and findings.
13. Establish a clear and documented incident procedure for handling incidents involving service providers.
14. In the case of intra-group outsourcing arrangements, reflect in the written policy that staff support from group entities often qualifies as outsourcing and ensure appropriate control measures are in place.
15. In the case of intra-group outsourcing arrangements, ensure that appropriate control measures are in place, aligned with the intra-group practices and associated risks.
16. Ensure that monitoring arrangements for intra-group outsourcing are formalised in a contract.
17. Create and document a written analysis specifically regarding intra-group conflicts of interest.
18. Establish a documented process around dual roles (dual-hatting) and associated potential conflicts of interest.
19. Define the company's responsibilities regarding the monitoring activities if a group entity conducts all or part of the monitoring of the (intra-group) outsourcing arrangement.
20. In case of intra-group outsourcing arrangements, make sure escalation can take place up to the level of the company's board.

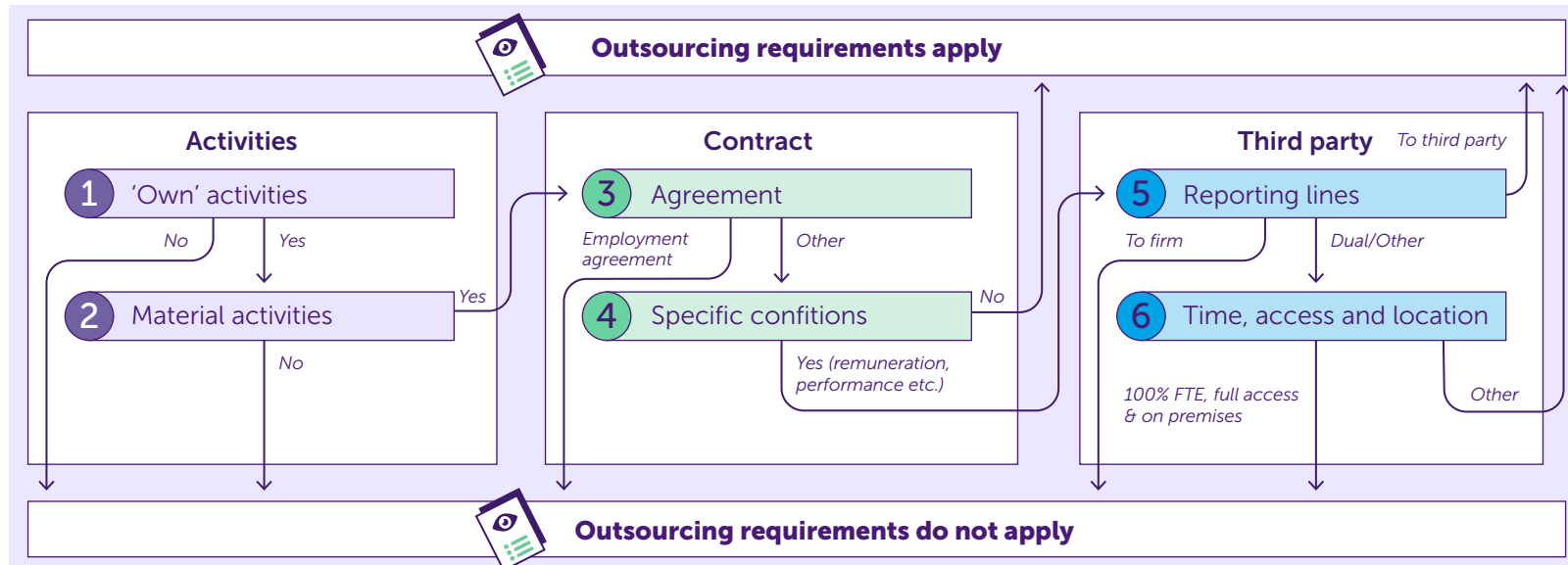
Annex II: Outsourcing flowchart

This appendix contains a number of considerations that, in the opinion of the AFM, are relevant in determining whether an assignment from a company to a third party to perform certain activities (e.g. by means of shared services, secondments, insourcing, support, etc.) qualifies as outsourcing within the scope of the outsourcing rules. These considerations can be summarised in a simplified manner as shown in the flowchart below. The considerations and the diagram below are expressly intended as guidance and cannot fully account for the variety of arrangements that may qualify as outsourcing. Companies themselves remain responsible for the correct qualification of their outsourcing arrangements.

For the sake of completeness, the AFM notes that, even for activities that the company assigns to third parties which do not qualify as outsourcing under the outsourcing regulations, companies are still required to implement sufficient control measures to ensure sound and controlled business operations.

Whether an arrangement constitutes legally as outsourcing and its consequences depend on the applicable legal framework. Therefore, the company must first determine which laws and regulations apply to the outsourcing arrangement. This is relevant, for example, for managers of AIFs or UCITS in the event of outsourcing of a core function, where the manager also has activities carried out by third parties (whether or not within the group) that relate to the second core function. After all, the outsourcing of two core functions is not permitted.

Figure 2. Outsourcing flowchart



Own activities

Companies can only outsource their own activities. Activities that a company is not (legally) allowed to carry out itself cannot therefore be outsourced. This includes the services of the depositary, external audit and broker services (to the extent to which this is not allowed under the company's licence). The fact that activities are new and therefore have not previously been carried out by the company itself does not alter the fact that such new activities are part of the company's own activities.

Material activities

In this report outsourcing of activities that fall within the scope of the outsourcing rules in the relevant legal framework is referred to as material, as explained in more detail in finding 1 of this report. Pursuant to article 1:1 of the Wet op het Financieel Toezicht ('Financial Supervision Act' or FSA), material activities are activities that arise from the conduct of the business of the company or the provision of financial services, or activities that are part of the substantial business processes in support thereof.

The term substantial in the FSA is a materiality limit and can be translated into various European laws. For example, Recital 82 of Delegated Regulation (EU) No 231/2013 states that: *'The delegation limitations and requirements should apply to the management functions set out in Annex I to Directive 2011/61/EU, whereas supporting tasks like administrative or technical functions assisting the management tasks such as logistical support in the form of cleaning, catering and procurement of basic services or products, should not be deemed to constitute delegation of AIFM functions. Other examples of technical or administrative functions are buying standard software 'off-the-shelf' and relying on software providers for ad hoc operational assistance in relation to off-the-shelf systems or providing human resources support such as sourcing of temporary employees or processing of payroll.'*

This means that support tasks, as mentioned in the text, should not be seen as material and therefore do not qualify as outsourcing within the meaning of the outsourcing rules.

Within the MiFID II framework, this requirement can be found under the 'critical and important' criterion, as included in the first subparagraph of Article 16(5) of MiFID II and further elaborated in Article 30 of the MiFID II Delegated Regulation (EU) 2017/565.

Agreement

When an employment contract is entered into with the person who carries out the activities, there is generally no outsourcing arrangement in place, as the individual works for the company itself. Any other form of agreement can constitute outsourcing. The considerations under 4, 5 and 6 are relevant here. Note that, one-off services are more likely to fall under support (see point 2) and are generally not seen as outsourcing.

Specific provisions

Where the contract contains specific provisions with regard to the individuals performing the relevant activities for the company, this is an indication that there is no outsourcing arrangement in place. In this case, considerations 5 and 6 are relevant. These specific provisions can relate, for example, to the specific activities, the number of hours, holidays, appraisal interviews, etc. per individual. If the contract does not contain specific provisions regarding these individuals, this is a sign that there is outsourcing.

Reporting lines

If the company has control over the activities and performance of the individuals who perform the activities, they work under the responsibility of the company. In that case, there is probably no outsourcing. This is clearly the case if the individuals who perform the activities only have a reporting line within the company itself. If the individuals only have a reporting line to persons within the service provider, that is an indication that the arrangement constitutes outsourcing. Sometimes there is a dual reporting line, in which case the following consideration is relevant.

Time, access and location

If the individuals who perform the activities for the company fully work for the company, the control is greater. This is an indication that there is no outsourcing. The same applies to access to systems for the individuals who carry out activities for the company and the location where these individuals carry out the activities. When these individuals work in the company's office full-time or work in accordance with the working from home policy that applies to all employees of the company and use the company's ICT, the arrangement is less likely to constitute outsourcing.

Annex III: Legal framework

The legal framework is an excerpt – in updated form – from the ‘Keten in Beeld’ sector letter of 2019.

When outsourcing activities to a third party, companies must comply with Dutch and European laws and regulations. These rules also apply to the monitoring of outsourcing. Various guidelines also apply. These are detailed in the overview below for each sector.

Tabel 1. Type of financial enterprise

Articles from legal frameworks that concern outsourcing	Investment firm	Manager of an AIF	Manager of a UCITS
Financial Supervision Act (Wft)	4:16 paragraphs 1 and 3	4:16, paragraphs 1-3	4:16, paragraphs 1-3
Decree on the Supervision of the Conduct of Financial Enterprises under the Financial Supervision Act (Bgfo)	37	37 37a	37 38 38a
Directive 2011/61/EU on Alternative Investment Fund Managers (AIFMD Directive)	Not applicable	20	Not applicable
Delegated Regulation (EU) 231/2013 supplementing Directive 2011/61/EU (AIFMD Regulation)	Not applicable	75-82	Not applicable
Directive 2014/65/EU on markets in financial instruments (MiFID II Directive)	16(5), first subparagraph	Not applicable	Not applicable
Delegated Regulation (EU) 2017/565 supplementing Directive 2014/65/EU (MiFID II Regulation)	30-32	Not applicable	Not applicable
Delegated Regulation (EU) 2017/589 supplementing Directive 2014/65/EU with organisational requirements for investment firms engaged in algorithmic trading (MiFID II Regulation)	Art. 2(3) 4	Not applicable	Not applicable
ESMA Guidelines on Outsourcing to Cloud Service Providers, 10 May 2021, ESMA50-164-4285	Applicable in full	Applicable in full	Applicable in full
EBA Guidelines on Outsourcing, 25 February 2019, EBA/GL/2019/02	Class 2 investment firms	Not applicable	Not applicable
Guidelines on certain aspects of the MiFID II requirements for the compliance function, 6 April 2021, ESMA35-36-1952	Applicable in full	Not applicable	Not applicable

It can be derived from the table that the outsourcing rules for a manager of a UCITS, for example, are less detailed than the rules for a manager of an AIF, for example. After an analysis of the rules, it can also be construed that the rules for managers of an AIF, for example, are different from the rules for an investment firm, for example. This could give the impression that outsourcing rules encompass fewer (or more) requirements depending on the type of company.

The AFM considers that all outsourcing rules included in the above regulations have significance for companies. It considers that, despite deviations in the elaboration, the regulations all serve the same purpose in principle: the management of outsourcing risks by companies. Regardless of the financial service a company provides, a company remains responsible for the activities it outsources, both to its supervisor and its customers, and a company is expected to be "in control". This means, by way of illustration, that if a company is in doubt as to how best to organise control measures according to the legal framework to which it is subject, the rules from other frameworks may provide practical depth.

In addition, the arrangements are similar in important respects. For example activities can only fall under the legal definition of outsourcing if they relate to the "normal" activities of a company. Normal activities have been explained in more detail in Annex IV of this report. The AFM therefore sees important points of attention in the various rules that companies can apply consistently to help them to be and remain in control with regard to outsourcing. In addition, the AFM notes that various points of attention can also be used outside the framework of outsourcing: after all, even when a company purchases activities or simply collaborates with third parties, it must be in control as referred to in Article 4:14 of the Financial Supervision Act.

Annex IV: ‘Keten in Beeld’ sector letter 2019, “assessing outsourcing” section

Definition of outsourcing and “normal activities”

Companies must determine whether activities carried out by a third party qualify as outsourcing.

The FSA defines outsourcing as follows:

the assignment by a financial company to a third party to carry out activities for that financial company:

- a. *which are part of or arise from the conduct of its business or the provision of financial services; or*
- b. *which are part of the essential business processes in support thereof;*

A different definition specifically applies to investment firms:

an arrangement of any form between an investment firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the investment firm itself.

Despite the different wording in the above definitions, for all types of companies outsourcing in principle refers to activities that a company assigns to a third party and that would otherwise be carried out by the company itself. Activities that a company has to perform itself fall within its tasks (remit). The activities may have different characteristics. For example, activities can comprise an individual activity or a series of activities and they can be performed once or continuously. In addition, it may be that a company outsources activities that relate to new activities, as a result of which the company has not previously carried out the activities itself. In addition, the activities can be carried out in a concentrated manner within a department or a function, such as the

set of activities carried out by (or within) the compliance department (or function). When a company has activities carried out by a third party, and such activities are part of its own tasks, the arrangement may qualify as outsourcing. In the remainder of this letter, the activities that are part of a company’s tasks (remit) are included under the term ‘normal tasks’.

Table 2 provides an overview of normal activities in relation to the three different types of financial companies covered by this letter. Each of these activities consists of a variety of activities and, in principle, if a company has one or more activities carried out by a third party, this always falls under the definition of outsourcing. However, there are general and specific exceptions to this principle.

Tabel 2. Types of companies

Tasks	Investmentfirm (MIFID II Directive Article 16(5), first subparagraph)	Manager of an AIF (AIFMD Directive Annex I)	Manager of a UCITS (UCITS Directive Annex II)
1	Critical or important functions or tasks ("core activities")	Portfolio management	Investment management
2	Other tasks	Risk management	
3		<ul style="list-style-type: none"> • Legal and fund management accounting services; • Customer inquiries; • Valuation and pricing (including tax returns); • Regulatory compliance monitoring; • Maintenance of unit-/shareholder register; • Distribution of income; • Unit/shares issues and redemptions; • Contract settlements (including certificate dispatch); • Record keeping. 	
4		Marketing	
5		Activities relating to the assets of the AIF	

General exceptions

Every company has a unique interpretation of its business operations, business processes and financial services. That is why companies of the same type (with the same financial services) have similar normal tasks but can still perform different activities. It is therefore impossible to provide a general overview of activities that fall under the scope of outsourcing. However, there are exceptions that generally apply to the different types of companies. The following general exceptions can help a company in its assessment of which activities carried out by a third party generally in scope of outsourcing:

- activities that can (legally) only be performed by a service provider, such as the mandatory audit of the annual accounts by an auditor, the deposit of funds and financial instruments with a custodian bank or the execution of orders in financial instruments by a broker;
- providing advice that is not part of the normal activities of a company, such as (legal) advice;
- provision of other services which do not form part of the normal functions of a company, such as, for example, catering, cleaning or staff training;
- the purchase of standardised services, such as exchange rate and market information services.

In this context, the AFM notes that it is not unusual for service providers to combine multiple activities and offer them as an integrated service package. A first example of this is an appointed custodian bank or custodian who, in addition to custody tasks (not outsourcing), also performs compliance and administrative activities (possibly outsourcing) for a company. A second example is (a supplier of) a portfolio management system (not outsourcing), which actually incorporates all or part of a company's risk management function and customer reporting (possibly outsourcing). These examples show that it is possible for a third party to carry out a range of activities, some of which fall within the normal functions of a company. This means that some of the activities in these examples are not covered by the outsourcing rules and others (when they are normal tasks) may be covered.

The AFM considers it important that your company has a complete picture of which activities your company outsources at all times, including activities that may have been integrated into the broader services of a third party (potentially already for a longer period of time).

Specific exceptions

Specific exceptions apply for certain companies. These exceptions are explained below for each type of financial company covered in this letter.

Investment firms

For investment firms, activities subject to outsourcing rules are included in the description of 'critical or important' functions (core tasks – see Table 2). This means that if activities do not fall under the core tasks of a company, they are not formally covered by the outsourcing rules.

It is therefore particularly important for an investment firm to assess which activities fall within its core tasks. Again, due to a unique interpretation of the business operations of each company, a general overview of core tasks cannot be given. However, investment firms can get assistance with their assessment, as activities with the following characteristics always fall within the core activities:

Activities in which a defective or inadequate performance has material adverse consequences for the company in terms of:

- a. its obligation to comply with the general or company-specific licensing obligations on an ongoing basis;
 - b. its financial results;
 - c. the solidity or continuity of the investment services or activities.
- Activities relating to the company's internal control function

Activities relating to the tasks of the company for which a licence is required.

The AFM would like to stress that, despite the fact that outsourcing rules only apply to the outsourcing of core tasks, the control measures and points of attention that are mentioned later in this letter can also help companies to be in control with regard to the outsourcing of “other tasks” (see table in this appendix).

Manager of an AIF

At the very least, two investment management functions that an AIF manager should perform are portfolio and risk management (see Table 2). A manager of an AIF may decide to outsource activities that encompasses one of the functions. However, a manager of an AIF is not permitted to outsource the activities related to both functions.

The other functions that a manager of an AIF can perform (see Table 2) are, in principle, part of the normal tasks of a manager. However, certain elements do not apply to all managers of an AIF. An example is a manager of, for example, a closed-end fund who will not perform tasks related to the redemption of units. Another example is a manager of, for example, an equity fund who is unlikely to perform any tasks related to the assets of the AIF. Of course, if tasks do not apply, and therefore do not fall under the normal tasks of a company, it will not qualify as outsourcing.

Manager of a UCITS

There are no specific exceptions for a manager of a UCITS. For these managers, the general definition of outsourcing and the general exceptions apply.