SUPERVISION **REPORT**

Establishment of effective compliance and internal audit functions

In short – As part of a Common Supervisory Action (CSA), the Dutch Authority for the Financial Markets (AFM), conducted an investigation in 2025 into internal control functions. The purpose was to gain insight into the extent to which UCITS managers and managers of AIFs (hereinafter collectively referred to as 'fund managers') have set up effective compliance and internal audit functions. Many positive practices were observed, alongside a number of areas for attention. In this report, the AFM shares areas for attention relating to the design and execution of tasks performed by the compliance and internal audit functions. The AFM expects fund managers to carefully consider these points and, where necessary, implement appropriate adjustments within their organisations.

JULY | 2026

AFM

Summary

In 2025, the AFM participated in a Common Supervisory Action (CSA) initiated by ESMA, an investigation into the establishment of the compliance and internal audit functions of managers of Undertakings for Collective Investment in Transferable Securities (UCITS) and alternative investment funds (AIFs).

The aim of this CSA was to gain insight into the way in which fund managers have set up these functions and to what extent they effectively contribute to managing the risks of non-compliance with laws and regulations.

In this report, the AFM shares the findings and areas for attention arising from its investigation among Dutch fund managers. The findings show, among other things, that fund managers have taken important steps in the professionalisation of their governance and internal controls. At the same time, the AFM sees various points on which further improvement is required. The areas for attention mainly relate to the internal embedding and positioning of compliance, the quality and timeliness of documentation, the relationship between monitoring, reporting and follow-up, and the division of roles between the first and second line of defense. The AFM also notes that proportionality is regularly applied, but that the substantiation for this is not always complete.

The AFM observes that larger fund managers have generally established adequate internal audit functions. However, for smaller fund managers, the rationale for applying (or not applying) the principle of proportionality is not always sufficiently substantiated. In addition, further formalisation of audit methodology, reporting and follow-up is desirable to ensure that risks are addressed in a timely and complete manner.

In addition to these areas for attention, the AFM has also made positive observations. For example, roles, responsibilities and escalation lines are clearly defined in many cases, compliance is often a standing agenda item in board meetings, and internal audit uses various audit methods that match the risks within the organisation. These elements form a strong basis for further professionalisation.

Based on the areas for attention, the AFM formulates expectations for fund managers. They are expected to strengthen the internal embedding of the compliance function, update and tailor documentation to their own organisation, formalise monitoring and reporting processes, and provide a comprehensive substantiation of the application of proportionality. With regard to the internal audit function, the AFM expects fund managers to further formalise audit methodologies and role allocations, ensure that findings are fully documented, and periodically conduct a thorough assessment of the effectiveness of the function.

The AFM will continue to include these themes in its ongoing supervision and expects fund managers to use the results of this report to further strengthen their governance and internal controls.

Table of Contents

1. The CSA

Introduction

The reason for this investigation is a Common Supervisory Action (CSA) initiated by ESMA into the establishment and functioning of the compliance and internal audit functions of managers of UCITS and AIFs. The aim was to gain insight into how fund managers organise their internal control functions and to what extent these functions effectively contribute to the prevention of risks of non-compliance with laws and regulations.

As part of this CSA, the AFM conducted an investigation among Dutch fund managers. The extent to which the compliance and internal audit functions have sufficient expertise, independence and organisational embedding was examined. In this report, the AFM shares the findings of this investigation and formulates areas for attention and concrete expectations for fund managers.

ESMA has also published a separate report, *2025 CSA on compliance and internal audit functions of fund managers*, incorporating the findings of the CSA at the European level.

2. Areas for attention

2.1 Compliance function

The compliance function monitors, evaluates and tests the adequacy and effectiveness of the established rules of conduct and procedures. These rules and procedures aim to detect risks and provide for appropriate measures to minimise these risks. The AFM emphasises that this function is of great importance to the sound and controlled business operations of fund managers. The person who fulfils this task must have the necessary authority, resources and expertise. In addition, the compliance function must report to management at least annually.

2.1.1 Specific considerations related to the compliance function

The CSA identified several areas for attention. Based on these findings, the AFM highlights the areas for attention set out below.

Area for attention 1 – Insufficiently up-to-date and organisation-specific compliance documentation
The AFM expects fund managers to have detailed written compliance documentation. This documentation must be complete and aligned with the organisation's specific activities and risks.

The CSA showed that most fund managers have a compliance agenda, a compliance monitoring plan, and compliance reporting on the compliance activities performed. Many fund managers also have documents in which the tasks and responsibilities of the compliance function are written out, and possible escalation lines are defined in writing. It is important that this documentation is present and up-to-date in all cases.

However, the AFM observed that for a number of fund managers, the documentation was outdated, incomplete or too generic. The absence of a structured process for updating and quality assurance increases the risk that relevant risks and obligations are not incorporated into the documentation in a timely manner. Documentation that merely lists applicable laws and regulations, without tailoring them to the specific organisation, is insufficient.

In addition, the AFM observed significant differences in the level of detail and depth of compliance monitoring plans. These plans should provide a sufficiently detailed and concrete description of the monitoring activities performed by the compliance function.

The AFM also observed examples of good practice among fund managers, particularly with regard to the quality of their compliance documentation. For example, some fund managers maintain central overviews of all relevant policies and procedures, including the dates of the most recent and next scheduled review, as well as clearly assigned ownership.

The AFM also observed monthly compliance reports with clear board sign-off procedures, as well as compliance monitoring programmes featuring clear timelines, designated ownership, and a distinction between ad hoc, recurring and thematic monitoring activities. In several cases, these programmes also included a documented explanation where planned activities had not been completed on time.

The AFM encourages fund managers to review their compliance documentation and assess whether it adequately reflects the compliance activities performed and provides a sound basis for the effective functioning of the compliance function.

Area for attention 2 - Insufficiently integrated design and implementation of the compliance cycle
The AFM expects fund managers to have a well-integrated compliance cycle in place to promote effective control and the timely identification of risks.

A compliance agenda and monitoring plan help to provide structure to the activities of the compliance function. The compliance monitoring plan should include periodic reviews of policies and procedures, as well as compliance monitoring activities relating to the fund manager's activities. The resulting findings and observations should be reported to the management body.

Ideally, these elements are logically connected and together form a coherent compliance cycle. This supports both risk mitigation and the assessment of control measures and, where necessary, their adjustment. In practice, the compliance function may also undertake ad hoc activities in response to emerging risks or incidents.

However, the CSA showed that these documents do not always align logically. For example, compliance agendas do not always correspond with the activities planned for the remainder of the year, and compliance reports do not consistently refer to the monitoring activities set out in the monitoring plan. While compliance findings are often reported, the subsequent follow-up actions are not always reflected in the planning of future activities.

The AFM therefore expects fund managers to assess the coherence and consistency of their compliance documentation and, where necessary, strengthen the links between the various elements of the compliance cycle.

Area for attention 3 – Insufficient assurance and embedding of the outsourced compliance function
The AFM expects fund managers that outsource the compliance function to ensure that compliance activities and reporting are aligned with the organisation's specific circumstances and needs.

The AFM observed that the compliance function is not always sufficiently embedded within the organisation. In some cases, there is a heavy reliance on service providers, both within and outside the group. As a result, the visibility and positioning of the compliance function within the organisation may be limited, creating potential vulnerabilities. A larger group of Dutch fund managers tends to make use of service providers, while the allocated hours and physical presence of compliance staff are limited. This may hinder the timely identification of risks and reduce the effectiveness of the compliance function.

Outsourcing compliance activities does not diminish the fund manager's responsibility for ensuring an effective compliance function. The investigation showed that external compliance service providers sometimes use standardised formats. While this is acceptable, such formats must be sufficiently tailored to the specific characteristics, activities and risks of the organisation. The AFM observed that this is not always the case. An effective compliance function provides management with meaningful information on the organisation's level of compliance and that of its funds. Such information should be tailored to the organisation's specific circumstances, key risks and areas for improvement.

The AFM emphasises that sufficient time must be made available for compliance activities. In practice, the AFM observes that standard contracts with external service providers often provide for a limited number of hours. It is important that fund managers assess whether the number of hours allocated is appropriate for their organisation. In addition, the AFM notes that, when outsourcing compliance activities, fund managers must take into account the need to scale up those activities where necessary.

For the effective performance of the compliance function, the AFM considers it desirable that the compliance function is sufficiently physically present. Where this is not the case, or only to a limited extent, the compliance function becomes dependent on the provision of information to adequately fulfil its tasks. This may entail risks.

Another point is that the fund manager must retain control in the case of (intra-group) outsourcing of the compliance function. The fund manager remains responsible and must therefore be able to set its own priorities, tailored to its specific risks and needs.

The AFM also sees cases in which the compliance function is partially outsourced, but there is a high degree of compliance knowledge internally, for example through the appointment of an internal compliance officer or a board member with a compliance background. This contributes to the quality of the compliance function.

Area for attention 4 – Unclear separation between the first and second line of defense

The AFM expects fund managers to position the compliance function in the second line of defense, with a primary monitoring role. The distinction between the first and second line of defense must be clear.

The compliance function is a control function and, as such, is part of the second line of defense. This means that the compliance function focuses primarily on risk management and monitoring, and not on development or execution.

During the CSA, the AFM found that the compliance function regularly performs first-line tasks, such as operational AML checks or the drafting of first-line policies. This blurs the division of roles and may undermine the independence and effectiveness of the second-line function. The risk is that the compliance function becomes less able to monitor its own activities effectively and that conflicts of interest may arise. In some cases, a fund manager may not be able to maintain a strict separation of functions, for example due to limited staff capacity. In such cases, it is important that the fund manager consciously documents this and takes appropriate measures to ensure that its business operations remain sound and controlled. The AFM expects fund managers to handle such situations with due care and to clearly document which individuals and departments are responsible for which activities.

Area for attention 5 – Insufficient substantiation for combining the risk and compliance functions

The AFM expects fund managers to keep responsibility for the compliance function and the risk management function separate, both at the operational level and at the management level.

The compliance function and the risk management function perform different types of activities. The compliance function focuses on monitoring compliance with laws and regulations, internal policies, and standards of conduct. Its objective is to manage integrity risks and prevent the fund manager from acting in breach of applicable laws and regulations.

The risk function is responsible for identifying, mitigating, managing and monitoring all relevant risks arising from the fund manager's activities. This responsibility is separate from the tasks of the compliance function. It is important that the compliance function can operate with sufficient independence and effectively monitor the risk function.

The AFM notes that smaller fund managers regularly combine the risk and compliance functions without sufficient substantiation or safeguards to ensure independence and the management of conflicts of interest.

If the fund manager does not have sufficient staff to maintain a strict separation between the risk and compliance functions, this must be clearly justified. In such cases, the AFM expects the fund manager to explicitly document this choice and to take appropriate measures to ensure sound and controlled business operations.

Area for attention 6 – Insufficient independent documentation by the compliance function
The AFM expects the compliance function to independently and separately document its findings. This is consistent with the independent role performed by the compliance function.

Given its independent position, it is appropriate for the compliance function to document its findings independently and separately. During the CSA, however, the AFM noted that, for some fund managers, compliance reports were only reflected in the minutes of board meetings. It is important that the findings identified by the compliance function are discussed by the board. The AFM also emphasises that these findings must be formally documented in separate reports.

A number of fund managers lacked a complete overview of shortcomings, follow-up actions and root cause analyses, which makes targeted intervention by the board difficult. In addition, the AFM notes that fund managers apply very different standards for documentation, with the threshold for reporting to the board being very high in some cases. It is important that not only incidents are reported, but also compliance risks, monitoring activities and possible shortcomings. This helps the board to make timely adjustments.

For some fund managers, on the other hand, it was notable that reporting to the board was very complete and timely. In these cases, compliance was a standing agenda item at board meetings, and the minutes showed that the board paid considerable attention to this topic.

Area for attention 7 – Insufficiently substantiated application of proportionality
The AFM expects fund managers to provide a detailed substantiation of why the chosen application of proportionality is appropriate, taking into account the nature, size and complexity of the organisation.

When fund managers apply proportionality, for example by combining functions, there is often no clear substantiation as to why this design fits the nature, size and complexity of the organisation. In some cases, fund managers only refer to the size of assets under management (AuM) or the number of employees. The AFM considers this to be insufficient.

The AFM expects fund managers to consider the nature, size and complexity of the organisation when applying proportionality and to substantiate why the chosen structure is appropriate in that specific case.

2.2 Internal audit function

The internal audit function investigates, assesses and tests the soundness and effectiveness of the fund manager's internal procedures. Based on this, the internal audit function has findings and makes recommendations. The internal audit function then checks whether the fund manager has followed these recommendations. The internal audit function also reports on its findings.

2.2.1 Specific points of attention regarding the internal audit function

The CSA has brought several points to light. Based on this, the AFM provides points for attention below.

Area for attention 1 – Insufficiently structured audit plans
The AFM expects fund managers to have audit plans in place that clearly set out which priorities are set and why. This prioritisation must be aligned with the organisation’s specific risks.

Audit plans should provide structure for the activities of the internal audit function. The AFM therefore expects fund managers to explain how the selected priorities and audit topics have been determined.

The CSA showed that audit methodologies vary widely. It is not always clear how risks are weighed, how priorities are determined, or how the division of roles within the audit plan is established. As a result, there is a risk that material risks are insufficiently addressed.

Various audit plans lack a clear substantiation of the choices made. The process of risk assessment and selection therefore deserves further explanation. A clear description of the methodology used, including the assessment and weighting of risks, strengthens the basis for responsible prioritisation. Proper documentation of this contributes to robust governance.

Area for attention 2 – Internal audit activities performed by a third party
The AFM expects fund managers to ensure that sufficient internal knowledge and expertise are present within the organisation, even where internal audit activities are performed by a third party.

Internal audit activities can be carried out by a third party. However, the fund manager must retain sufficient internal knowledge to discuss and challenge the methodology used and the findings. This is necessary to understand the root causes of findings and recommendations and to effectively address underlying issues. This contributes to sound and controlled business operations and ensures that recommendations are concrete and can be followed up.

The fund manager remains responsible for the establishment and effective operation of the internal audit function. It must therefore be clear who within the organisation is responsible for overseeing and assessing the work performed by a third party. There must always be a member of the management body with ultimate responsibility for the internal audit function.

During the CSA, the AFM observed cases in which the person overseeing the internal audit activities performed by a third party was also external to the organisation. In such cases, the AFM considers the internal audit function to be insufficiently safeguarded within the organisation.

Area for attention 3 – Insufficient follow-up of reports
The AFM expects fund managers to clearly document the extent to which recommendations made by the internal audit function have been followed up.

A core task of the internal audit function is to make recommendations and assess whether these recommendations have been followed up. The reports of the internal audit function must therefore clearly explain whether, and if so how, follow-up has taken place. It is equally important that recommendations which have not (yet) been followed up are also reported, including a clear explanation as to why no follow-up has taken place.

This was well documented in the majority of the reports assessed in the context of the CSA. At the same time, the AFM observed significant differences in the level of detail. Delays in the follow-up of audit recommendations were often reported, but the substantiation of why these delays were considered acceptable was often lacking. In addition, clear deadlines, responsibilities or root cause analyses were not always established, making effective follow-up more difficult.

The reports of the internal audit function provide important insights. Fund managers can use these insights as management information to improve processes and address risks in a timely manner. A clear and structured record of the follow-up of recommendations is essential in this regard.

Area for attention 4 – Insufficiently robust governance around effectiveness assessment

The AFM expects fund managers to conduct a thorough assessment of the effectiveness of the internal audit function.

The CSA showed that the evaluation of the internal audit function by the board is not always sufficiently in-depth. Intragroup audit services sometimes lack clear safeguards for independence and individual responsibility, which may put pressure on the effectiveness of the function.

At the same time, the AFM sees elements that contribute to an effective structure of the internal audit function. For many fund managers, internal audit is a standing agenda item at board meetings, which promotes ongoing attention to audit matters. In addition, the internal audit function is generally clearly positioned for larger fund managers and is not combined with other functions. In many cases, delays in the follow-up of audits are also transparently reported to the board, which strengthens governance.

Area for attention 5 – Insufficient substantiation of proportionality

The AFM expects fund managers that invoke proportionality to substantiate this comprehensively and transparently. The substantiation must demonstrate how the chosen proportionality is aligned with the nature of the activities, the size of the organisation and its complexity.

Many fund managers choose not to establish an internal audit function and invoke proportionality, but they do not always explain why this is justified. In some cases, they still have audits carried out by external or intragroup parties, without making it clear how this fits in with their application of proportionality.

Smaller fund managers often lack internal capacity for an internal audit function. Alternatives, such as intragroup or external implementation, are not always substantiated on the basis of risks, independence and the required expertise. This may result in the board not obtaining a sufficient degree of independent and risk-based assurance regarding the functioning of the internal control and risk management framework.

3. Conclusions

The results of the 2025 CSA show that fund managers in the Netherlands generally meet the legal requirements for both the compliance function and the internal audit function. At the same time, the quality, professionalism and effectiveness of these functions still differ significantly in practice.

Important points of attention are:
- maintaining up-to-date and consistent documentation
- further strengthening monitoring and reporting
- the careful application of the principle of proportionality
- strengthening control over outsourced activities
- ensuring a clear separation of roles between the first and second lines of defense

Although there are still areas for attention, the AFM observes that many fund managers are taking steps towards further professionalisation. Compliance and internal audit are increasingly becoming standing agenda items at board meetings. This provides a solid foundation for further improvements.

The AFM expects fund managers to use the findings of this report to further strengthen their governance and internal controls. This requires targeted improvements and regular monitoring of what works well within the organisation and what can be improved, taking into account its nature, size and complexity.

The AFM will continue to monitor the extent to which fund managers implement these improvements and, where necessary, request further clarification.

Annex

Scope and approach

The selection included both UCITS managers and AIF managers of varying sizes, investment strategies and degrees of cross-border activity. The assessment was conducted primarily as a desk-based review, based on the completed CSA questionnaires, supporting documentation and targeted follow-up questions. Where necessary, additional explanations and documentation were requested. For a number of fund managers, further clarification was obtained through brief discussions by telephone or in writing.

Legal framework

The legal framework for the compliance function and the internal audit function for AIF managers is set out in Articles 61 and 62 of Delegated Regulation (EU) No 231/2013. For managers of a UCITS, this is laid down in Articles 30(6) and 31c of the Decree on the Supervision of the Conduct of Business of Financial Undertakings under the Financial Supervision Act (BGfo) and in Chapter 2, in particular Section 3, of Directive 2010/43/EU. This report is based on the situation as it applied during the implementation of the CSA and applies at the time of publication.

The areas of attention in this report are a practical interpretation of existing standards for the compliance and internal audit functions.