Report on the organisation of outsourced compliance function in fund management companies, alternative investment fund managers and investment firms

Content

Writers

Heidi Tähtinen / heidi.tahtinen(at)finanssivalvonta.fi or tel. +358 9 183 5314

Hannele Alanen / hannele.alanen(at)finanssivalvonta.fi or tel. +358 9 183 5292

1 Background, purpose and key findings of the report

Background and purpose

The Financial Supervisory Authority (FIN-FSA) has assessed the organisation and quality of the outsourced compliance function of investment firms, fund management companies and alternative investment fund managers. The purpose of the report was to ascertain how the outsourced compliance function and its tasks are organised, whether sufficient quantitative and qualitative resources have been allocated to the function, and how the outsourced function is monitored. The background to the report is an observation made by the FIN-FSA in its supervision about the prevalence of the outsourcing of the compliance function[1].

The report is based on the FIN-FSA's annual survey for authorised entities[2] in spring 2022 and a separate survey sent in summer 2022, which was answered by those authorised investment firms, fund management companies and alternative investment fund managers that had outsourced the compliance function outside the company or group, either completely or partially. The FIN-FSA last investigated the organisation of the compliance function of these supervised entities in a thematic review in 2017.[3]

A total of 28 supervised entities responded to the survey. Although the report focuses on outsourcing outside the company or group, the FIN-FSA's views on the organisation of the compliance function are largely applicable to outsourcing within the group as well as to situations where the compliance function has not been outsourced.

Key findings and shortcomings

On the grounds of the report FIN-FSA considers that the quality of outsourced compliance function has not been sufficient. The FIN-FSA found in its report that all supervised entities that participated in the survey had shortcomings in the organisation of the outsourced compliance function.

The most significant findings and shortcomings were:

1. *Shortcomings in the time allocation, resourcing, competence and organisation of the compliance function*
   - Outsourced compliance officers do not have sufficient time and competence to perform their tasks, as compliance has not performed all of its tasks sufficiently.
   - Outsourced compliance is not sufficiently reachable or present in the daily operations of the supervised entities when performing its task. Most of the supervision is done as desk-based exercises.
   - The compliance function is particularly intermixed with legal tasks. Compliance also often has other tasks in the supervised entity.
   - The share of the partially outsourced compliance function remaining with the supervised entity is not sufficiently clearly defined.

[1] *The Financial Supervisory Authority's annual survey 2022: 31/38 fund management companies have outsourced the compliance function inside or outside the group. 30/44 of the investment firms have outsourced the function inside or outside the group.*
[2] *Authorised alternative investment fund managers, fund management companies and investment firms*
[3] *https://www.finanssivalvonta.fi/en/publications-and-press-releases/supervision-releases/2017/the-fin-fsa-has-assessed-the-organisation-and-quality-of-the-compliance-function-of-investment-firms-fund-management-companies-and-alternative-fund-managers/*

- Outsourced compliance is not sufficiently present at board meetings where the activities of the compliance function are presented (e.g. risk assessment, monitoring programme, reporting).
- There are shortcomings in the competence of those responsible for compliance.

2. *The compliance function does not perform all of its tasks as required by regulations*
   - There are many shortcomings in the content of compliance reporting.
   - Compliance activities consist mainly of regulatory reviews for the board of directors and participation in the updating of guidelines. Revenue and monitoring tasks performed by compliance are either completely or partially absent.

3. *There is room for improvement in the activities of supervised entities' boards of directors*
   - The boards of supervised entities do not sufficiently assess the resourcing and efficiency of the compliance function.
   - The boards do not have sufficient competence to assess or question the sufficiency and appropriateness of the function.

Good practices

Good practices in the organisation of the compliance function, as observed by the FIN-FSA in the report or in ongoing supervision:

- The supervised entity has its own compliance function so that the compliance can remain permanent in nature and play an active role in the entity's day-to-day operations.
- The person handling the outsourced compliance function has a deputy in the company providing the service so that the continuity of the function can be secured.
- The supervised entity has separated the acquisition of legal and compliance services.
- The board of directors has sufficient competence and understanding of compliance activity.
- Compliance reports and participates to the meetings of the board of directors quarterly.
- The questions, comments and conclusions of board members for the compliance officer on issues discussed are entered in the minutes of the board.

Regulations

The compliance function of supervised entities is regulated in EU regulations and national legislation for each type of supervised entity.

Regulations on investment firms and fund management companies and alternative investment fund managers providing investment services:

- Investment Services Act 747/2012
- Commission Delegated Regulation (EU) 2017/565, particularly Articles 22, 25, 26 and 31
- The FIN-FSA's Regulations and guidelines 7/2018
- Guidelines on certain aspects of the MiFID II compliance function requirements (ESMA35-36-1952), hereinafter ESMA Guidelines
- Guidelines on internal governance under Directive (EU) 2019/2034 (EBA/GL/2021/14)

Regulations on fund management companies:

- Act on Common Funds 213/2019
- Commission Directive 2010/43/EU, particularly Article 10

Regulations on alternative investment fund managers:
- Act on Alternative Investment Fund Managers (162/2014)
- Commission Delegated Regulation (EU) 231/2013, particularly Article 61

The principles of the various statutes concerning supervised entities are similar. Although there are guideline-level regulations only for investment firms, all supervised entities should, where applicable, aim for a level in accordance with the above-mentioned guidelines for investment firms when organising the compliance function. In addition, ESMA has addressed the organisation of the compliance function in its Brexit opinions concerning fund management companies, alternative investment fund managers and investment firms.[4]

2 Outsourcing the compliance function

General conditions for outsourcing

The compliance function, i.e. the function responsible for ensuring compliance with regulations and internal operating principles, is a key part of supervised entities' reliable governance and internal control. A strong, independent and sufficiently resourced compliance function is in the common interest of both the company and the supervisory authority. An appropriate compliance function serves to ensure and strengthen a responsible and reliable operating environment for companies' management, employees and customers alike.

The supervised entity can outsource the tasks of the compliance function either completely or partially. In that event, the supervised entity must make sure that all the requirements for the compliance function and the general conditions set for outsourcing are fulfilled. In addition, the supervised entity must ensure that the compliance function remains permanent in nature. Outsourcing must not hinder the entity's internal control.

The supervised entity must ensure the sufficiency of resources and professional competence as well as the financial capacity of the party handling the outsourced function. A written agreement on the outsourcing of the function must be made, stating the tasks of the compliance function to be outsourced, the powers of the service provider, rights to access to information, and reporting.

The senior management of the supervised entity is responsible for the ongoing monitoring, supervision and evaluation of the outsourced tasks as well as the management of outsourcing-related risks. Even though senior management is responsible for organising and monitoring the effectiveness of activities related to compliance with requirements, the compliance function should perform its tasks independently of senior management and the entity's other units.

Person responsible for compliance in the supervised entity

Each authorised entity must have a designated person responsible for compliance, even when the entity has outsourced the compliance function. This also applies to situations where outsourcing takes place within a group. The FIN-FSA considers that a person responsible for an independent monitoring function

[4] *Opinion concerning investment firms: esma35-43-762_opinion_to_support_supervisory_convergence_in_the_area_of_investment_firms_in_the_context_of_the_united_kingdom_withdrawing_from_the_european_union.pdf (europa.eu). Opinion concerning management companies and alternative investment fund managers: esma34-45-344_opinion_to_support_supervisory_convergence_in_the_area_of_investment_management_in_the_context_of_the_united_kingdom_withdrawing_from_the_european_union.pdf (europa.eu)*

must not be in dependent relationship with the entity's business operations. For this reason, the person supervising the outsourced compliance function cannot be from business operations, as business operations cannot give instructions to the compliance function or otherwise influence the performance of the tasks of the persons involved. Therefore the chief executive officer could not act as the person responsible for the compliance function. In addition, conflicts of interest related to the tasks of the person designated as compliance officer must be primarily avoided. If conflicts of interest cannot be avoided, they must be appropriately assessed and monitored.

The person responsible for monitoring outsourcing is required to have expertise and competence in the compliance function as well as genuinely sufficient resources, so that they can effectively monitor and assess the outsourced function. This cannot therefore merely be a nominal role. The person responsible for compliance should also maintain their understanding and competence with regard to the tasks and areas of responsibility of the compliance function by receiving regular training.

It is not credible for the supervised entity's person responsible for compliance to act as the deputy for outsourced compliance if they do not have sufficient competence or resources to perform the task. In addition, the supervised entity must have the key competence with regard to the outsourced function, so that the function can, if necessary, be taken back to be performed by the entity, unless the entity already has sufficient readiness to transfer the function to another service provider.

In its investigation, the FIN-FSA found that supervised entities lack key competence with regard to the compliance function and its tasks. In many entities, the role of person responsible for compliance is only nominal, and they do not have sufficient competence to perform their tasks.

Outsourcing the compliance function within a group

If the supervised entity belongs to a group, each authorised entity of the group has an independent responsibility for the compliance function. Even if the supervised entity outsources compliance function tasks to another entity belonging to the group, each entity itself should ensure that risk related to complying with requirements is still monitored in the entity in question. Outsourcing the compliance function within a group therefore does not reduce the responsibility of the senior management of the individual entities belonging to the group. In addition, each authorised entity must have a designated person responsible for compliance, as stated in the previous section.

An outsourcing agreement must also be prepared when an entity outsources the compliance function to another entity of the same group. The powers, tasks, and rights of access to information of the party handling the compliance function as well as the reporting procedures must be stated in the agreement.

3 Compliance function resources

Criteria

Sufficient resources must be allocated to the compliance function. When ensuring the sufficiency of resources, the supervised entity should take into account the nature, scope and complexity of its operations. If the entity's business expands or changes significantly/materially, the entity must ensure that the compliance function is also expanded, if this is necessary taking into account the altered risk in the entity with regard to complying with requirements.

The compliance function must be independent of business operations. The compliance function may, however, participate in business development in the ways described in sections 40 and 41 of the ESMA guidelines. Even then, the compliance function must maintain its independent status.

FIN-FSA's findings

All of the supervised entities that participated in the FIN-FSA's investigation had outsourced the compliance function either completely or partially outside the entity or group. Slightly more than half of the supervised entities who responded to the survey stated that they had completely outsourced the compliance function.

In the supervised entities that had partially outsourced the compliance function, the nature and scope of the outsourced compliance tasks varied from ad-hoc advice to very extensive sets of tasks. Based on the survey and submitted material, it remained unclear to the FIN-FSA, with regard to some entities, how the portion of the partially outsourced compliance function remaining in the entity itself is organised, i.e. which compliance tasks are performed in the entity and by whom.

At the time of the survey, the outsourcing of supervised entities' compliance function was mainly focused on six service providers. The service providers are law firms in which the outsourced compliance function is handled by designated persons. In some service providers, the task is handled by only one person. Individual service providers generally provide a compliance service to 3–7 supervised entities.

More than half of the supervised entities had agreed with the service provider on a minimum number of hours to be used for to handling the compliance function. A few entities had agreed on a maximum number of hours to be used. Five entities had not agreed anything with the service provider with regard to the working time to be used for the function. With a few exceptions, the minimum number of hours agreed with the service provider was low, on average less than six hours per month. For those who had outsourced the function completely, the average agreed minimum number of compliance hours is less than 7 hours per month. The extent of outsourcing (completely or partially) was found to have no significance for the working hours agreed.

According to the survey, service providers used an average of 11 hours per month per company for handling the outsourced compliance function. There is significant variation, however, in the working hours allocated to individual entities: a minimum of around 2 hours per month and a maximum of around 120 hours per month are used for handling the outsourced task. The FIN-FSA found that the hours used for the compliance function differed significantly depending on the supervised entity and the service provider.

A third of the supervised entities reported that the outsourced compliance function used less than one working day per month for handling its tasks. The extent of outsourcing (completely or partially) was found to have no particular significance for the working hours used: in a number of cases, partially outsourced compliance spent more time on handling tasks than completely outsourced compliance.

Based on the survey, the time allocated to the various tasks of the person handling the compliance function varies greatly from entity to entity. Most of the working time of outsourced compliance is used on advice (on average, 38% of working time). Outsourced compliance uses an average of 11% of working time on reviews and 17% on monitoring. A third of the supervised entities have reported that outsourced compliance does not use any time at all on reviews. Outsourced compliance uses an average of 5% of its working time on training.

Based on the survey, around half of the responding supervised entities reported that the person handling the outsourced compliance function also has other tasks in the supervised entity. The other, non-compliance function tasks, were mainly related to legal advice or other legal services, administrative matters, internal audit or, for example, acting as board secretary.

If the compliance function is outsourced to a larger service provider than a one-person company, the designated compliance officer is typically supported by a compliance team whose members also act as the compliance officer's deputies. If a deputy is appointed from within the supervised entity, the person in question is typically, according to the entity's reports, the entity's chief financial officer or administrative director, chief risk officer or chief executive officer.

FIN-FSA's view

Taking into account the working hours used by the outsourced compliance function for its tasks, the FIN-FSA was unable to verify in all respects the sufficiency of the resources of the outsourced compliance function or whether the compliance function is, in fact, organised as required by regulations. This applies, in particular, to those supervised entities where the compliance function has been outsourced completely. Many of the supervised entities that responded to the survey stated that compliance does not use any working time at all for supervision or reviews; the time is mainly used for advice, regulation monitoring, and preparing and updating work guidelines or operating principles.

The FIN-FSA emphasises that compliance does not fulfil its regulatory obligations if it does not carry out any monitoring or review measures. It is the responsibility of the entity's board of directors to ensure that the compliance function handles sufficiently all of its regulatory tasks. The board is neglecting its supervisory duties if it does not address shortcomings in the operation of the compliance function.

The above-mentioned finding is also supported by the fact that, based on compliance reports, the compliance function in a number of supervised entities had not been able to carry out monitoring measures to the agreed schedule. The FIN-FSA has grounds to suspect that such service providers are unable to effectively and properly handle the outsourced compliance function of several entities at the same time.

Applying the principle of proportionality does not mean that some tasks of compliance can be left entirely undone. It means that not every company's compliance has to perform its tasks at the same extent and at the same intensity.

The FIN-FSA considers it good practice for the person handling the outsourced compliance function to have a deputy in the company from which the outsourced service is provided. If the service provider has only one employee, the supervised entity should verify in even more detail the company's internal responsibility and deputy arrangements, in terms of both the person's responsible for compliance competence and use of time. The supervised entity must have the readiness to organise the compliance function in a reliable way also when the outsourced service provider is temporarily prevented from performing its task.

The FIN-FSA emphasises the need to maintain the compliance function's independence from the supervised entity's business operations, when an entity assigns other tasks to the compliance function. The FIN-FSA therefore recommends that supervised entities clearly separate legal and compliance tasks from each other and, if necessary, acquire the services in question from different service providers. If an entity uses the proportionality principle when combining different functions, it should document why this is justified.

4 Operating principles of the compliance function

Criteria

The responsibilities, competencies and powers of the compliance function must be defined in the operating principles of the compliance function or in other codes of conduct or internal guidelines that take into account the scope and nature of the supervised entity's operations. The board of directors of the supervised entity must regularly reassess and confirm the operating principles.

The operational principles should include information about the compliance function's monitoring programme and reporting obligations as well as an risk-based approach to monitoring activities. The operating principles should define arrangements aimed at ensuring that the responsibilities of the compliance function are handled on a continuous basis. These should include, for example, deputy arrangements, and procedures in case the compliance function outsourcing arrangements are terminated. The supervised entity must define and document the appointment and dismissal of the person responsible for compliance. In addition, the competence and experience required of the persons handling compliance activities should be defined.

The operating principles must specify that the persons handling the compliance function have access to the information that is material to their tasks as well access rights to all relevant databases or records, reports prepared from internal or external audits, and other reports prepared for senior management or supervisory functions.

In addition, the operating principles should clearly state how the compliance function's tasks are divided when the function is partially outsourced. In that case, a description must be prepared specifically for each task and responsibility. The operating principles or the entity's conflict of interest policy must take into account possible conflicts of interest related to compliance activities.

FIN-FSA's findings

The FIN-FSA found a number of shortcomings in the content of operating principles, for example with regard to competence, definition of tasks, responsibilities and powers, and reporting:

- A third of the supervised entities had not defined in their operating principles the deputy arrangements in the absence of the actual compliance officer.
- Around half of the supervised entities had not defined properly or not at all in their operating principles who appoints and dismisses the person responsible for the compliance function and the compliance officer. Some of the supervised entities had defined only the appointment, but not the dismissal. Some had defined only the appointment and dismissal of the person responsible for compliance.
- Two-thirds of the supervised entities had not defined properly or not at all in their operating principles the return of tasks after the termination of the outsourcing of the compliance function.
- Some of the supervised entities had not taken into account in their operating principles possible conflicts of interest in the event of the compliance officer/compliance function handling other tasks inside or outside the entity. Most of the supervised entities had taken into account in their operating principles only the entity's internal conflicts of interest, but not at all the entity's external conflicts of interest regarding the compliance function.

- Most of the supervised entities had defined narrowly or not defined at all the competence required of the outsourced compliance officer and entity's person responsible for compliance.
- In the case of several supervised entities that have partially outsourced their compliance function, it was unclear to the FIN-FSA how the compliance tasks have been divided between the entity's internal compliance function and the outsourced compliance function.

FIN-FSA's view

The FIN-FSA urges supervised entities to ensure that their operating principles meet the regulations. Entities are urged to focus on the following points in particular:

- The appointment and dismissal of the compliance officer and person responsible for compliance as well as deputy arrangements must be defined and documented.
- The entity must define the return or transfer to a new service provider of compliance tasks at the termination of outsourcing.
- The personnel of the supervised entity responsible for supervising compliance with requirements must have the knowledge, competence and expertise required for the tasks assigned to them. The entity must define what kind of competence and experience is required of the compliance officer and person responsible for compliance.
- The handling of the tasks of the compliance function between each party must be specified when the function is partially outsourced. The specification must cover all of the tasks that fall under the compliance function according to regulations.
- The powers of those handling the compliance function must be defined more extensively and in more detail than at present.
- The frequency and content of compliance reporting should be defined in more detail.

The FIN-FSA considers that supervised entities have not sufficiently taken into account conflict of interest situations related to the organisation of the outsourced function. The FIN-FSA urges entities to pay particular attention to conflicts of interest related to time use of outsourced compliance and prioritisation of different work tasks as well as the procedures required for handling them. It is recommended that conflict of interest situations and their management procedures be included in the regular reporting of internal control.

5 Tasks of the compliance function

Criteria

The compliance function assists the board of directors of the supervised entity in managing risks related to non-compliance with regulations. An important element of the tasks of the compliance function is executing monitoring measures in accordance with a prepared monitoring programme and as necessary. Compliance must also participate in the supervision of complaints handling and in the training and advising the supervised entity's personnel.

The compliance function must prepare a risk assessment, which is used to create a compliance work programme and a risk-based monitoring programme that specifies the monitoring and advisory priorities. The risk assessment must be reviewed and updated regularly. ESMA's guidelines (paragraphs 19–26) provide more detailed instructions on what aspects should be taken into account in the preparation of the monitoring programme. The guidelines emphasise that all monitoring measures performed by compliance cannot be solely desk-based.

The compliance function must support operational business units in organising appropriate training. The focus of the training must be all personnel directly or indirectly involved in carrying out activities in accordance with the entity's authorisation. Training must be organised regularly and as necessary. Training must cover material changes, for example in legislation.

The compliance function must report to the supervised entity's senior management both regularly and as necessary. ESMA's guidelines (paragraphs 27–31) list issues that should be covered in compliance reports.

FIN-FSA's findings

Based on the supervised entities' responses, the FIN-FSA was left with the impression that not all entities and outsourced compliance officers know what the tasks and obligations of compliance are.

The FIN-FSA found that, in some supervised entities, reviewing and monitoring are only covered by updating internal guidelines. This cannot be considered to be sufficient. Based on the responses, compliance uses most time on advice.

Risk assessment

Five supervised entities completely lacked a risk assessment. In some entities, compliance risks are part of the assessment of operational risks. Some entities have difficulty separating compliance risks and operational risks. In the risk assessments they submitted to the FIN-FSA, five entities only listed risks without specifying the probability of the risks or their mutual significance.

Risk-based monitoring programme

Five supervised entities had not drawn up a risk-based monitoring programme at all. The most common justification for this was the limited nature of the entities' operations.

Numerous shortcomings were found in supervised entities' monitoring programmes. In the case of several entities, review plans were unclear. For example, it was stated in one monitoring programme that compliance must make two reviews, but their subject matter and method of implementation remained undefined. Furthermore, there were entities whose monitoring programme recorded no reviews at all, or too few of them had been planned taking into account the quality and scope of the entity's business operations. For some entities, the reviews selected did not correspond to the priorities according to the entity's risk assessment. In addition, it was noticeable that outsourced compliance performed the same review/reviews for all its entities. Monitoring programmes also often lacked an assessment of training needs.

In many supervised entities, the board of directors had not approved the monitoring programme until halfway through the year to which the monitoring programme applied. At longest, the monitoring programme was only approved 11 months after the start of the year. Four of the supervised entities that participated in the survey stated that their board of directors does not approve annually the risk-based monitoring programme for compliance. With regard to some entities, the FIN-FSA remained unclear as to whether the entity's board of directors has approved a monitoring programme at all.

Training

At several supervised entities, the most recent training organised by the compliance function was held in 2021 or more than a year had passed between the two most recent training events. In some entities, training does not cover all personnel; only, for example, the board of directors or tied agents. Moreover, in some entities, training has only consisted of regulatory reviews held by compliance.

Compliance reports

In the FIN-FSA's view, the standard of the supervised entities' compliance reports was mostly poor. Nearly all entities had significant shortcomings in the content of their compliance reports. Many reports only described the measures taken, but did not highlight the observations made by the compliance function or the assessments made of the observations. The reviews performed and the observations made in them were absent from the compliance reports of several entities.

It remained unclear to the FIN-FSA how the supervised entities' internal compliance function reports to the board of directors when the function has been partially outsourced. The FIN-FSA found that in a number of entities the compliance reports only covered the outsourced compliance function. These reports therefore did not take any position at all on the compliance tasks that the entities had not outsourced.

FIN-FSA's view

The FIN-FSA emphasises that monitoring and reviews cannot be merely desk-based; compliance must also monitor the entity's operations through on-site inspections at the entity's operating premises. The compliance function must be involved in commenting on and preparing guidelines, but that alone does not cover the monitoring obligation.

Taking into account outsourced compliance service providers' acting as the compliance of several different supervised entities as well as the time they use in handling the tasks of individual entities, it is clear that outsourced compliance is not present in the day-to-day operations of the entities and therefore cannot adequately monitor the compliance of the entities' operations with regulations.

Based on the survey, compliance uses most time for advice, which is an important part of compliance work. The FIN-FSA considers, however, that companies must not, by prioritising advice, neglect the handling of the other tasks assigned to the compliance function.

The FIN-FSA considers that, in most cases, companies and the compliance function do not have sufficient competence to identify and assess the compliance risks of each supervised entity.

Risk assessment

All supervised entities must prepare a risk assessment of the compliance function. Regulations do not allow any deviation from this. Without a risk assessment, it is impossible for entities to prepare monitoring and work programmes for the compliance function. The special characteristics of each entity must be taken into account when preparing the risk assessment. The compliance risk assessment may be combined with the operational risk assessment, but the entities must then be able to distinguish the differences between these risks.

The FIN-FSA considers it insufficient for the risk assessment to merely list risks. Furthermore, entities must assess the probability and mutual significance of risks.

Risk-based monitoring programme

All supervised entities must have a risk-based monitoring programme that defines which are the review targets for the coming year and when and how the reviews will be performed. The monitoring programme should also include an assessment of training needs. The FIN-FSA considers that the board of directors should approve the monitoring programme before it enters into effect.

The FIN-FSA emphasises that reviews and monitoring measures should be selected according to a risk-based assessment and the entity's individual needs. The FIN-FSA does not consider it credible that outsourced compliance would be able on an annual basis to thoroughly review the entire operations of a supervised entity.

Training

The compliance function must attend to the training of personnel. Training must be regular but, if necessary, compliance must also be prepared to organise additional training. In planning training, the risk areas defined in the risk assessment must be taken into account. Training should be organised for all relevant personnel, not only for a small part of the workforce. The FIN-FSA considers that, in order to fulfil the training obligation, it is not sufficient merely to organise regulatory reviews for the board of directors.

Compliance reports

The FIN-FSA emphasises that compliance reports should cover the entire compliance function. The requirements set out in ESMA's guidelines should be taken into account in the preparation of the reports. The reports should take a concrete position on the supervised entity's issues and highlight the observations made by the compliance function. The compliance reports must include the reviews carried out as well as the observations made in them and any follow-up measures.

The compliance function must report to the senior management of the supervised entity on its activities and the observations it has made at least annually. The FIN-FSA recommends that, in addition to this annual summary, the compliance function reports to the board of directors at least quarterly. In addition, the compliance function must have the opportunity to otherwise bring any shortcomings it observes to the attention of the board.

6 Board of directors' role in organising internal control

Criteria

The board of directors bears responsibility for ensuring that the supervised entity has adequate, reliable and effective internal control functions relative to the quality and scope of its operations. The board must monitor the effectiveness of operations and, if necessary, take measures to correct observed shortcomings. In addition, the board must assess, at least annually, the effectiveness and suitability of the outsourced function in relation to the entity's business.

It is the board's task to approve and re-evaluate the operating principles of the compliance function. The board should approve annually the compliance function's risk-based monitoring programme. In addition, the board must discuss the reports prepared by the compliance function.

FIN-FSA's findings

The FIN-FSA found that several of the supervised entities that participated in the survey had not, according to submitted board minutes, discussed matters related to the compliance function at all in 2021 or in early 2022. Most of the boards of the supervised entities receive each year for their information a monitoring programme and compliance report prepared by the compliance function. Only six entities reported that the board of directors had discussed internal audit monitoring reports related to the compliance function.

It is challenging to assess the actions of boards of directors, however, as supervised entities' ways of recording board minutes vary. In the case of most entities, the board minutes do not show with certainty what matters the board has discussed, whether the compliance issues brought to the board have sparked discussion, what conclusions have been reached, or whether the board has, for example, called into question issues presented by the business or control functions. Although the reason can be partly attributed to the practices that guide the preparation of meeting notes and minutes, the entries missing from the minutes lead to the conclusion that boards do not discuss compliance issues in their meetings and address questions, comments or assessments to the executive management or compliance. In addition, the FIN-FSA found that outsourced compliance in a number of entities does not participate in board meetings when the compliance monitoring programme, reports or observations are discussed there.

Apart from individual supervised entities, it did not appear from the board minutes submitted to the FIN-FSA that the boards of directors regularly assess the sufficiency of compliance function resources or the effectiveness of monitoring measures. According to the survey, during the previous year, only a few supervised entities had assessed the resourcing and effectiveness of the compliance function taking into account the quality and scope of the entity's operations.

FIN-FSA's view

The FIN-FSA considers that outsourced compliance should participate in the meetings of boards of directors when the compliance monitoring programme, compliance reports or other materials produced by compliance are discussed there, so that the compliance officer can present the said documents and, if necessary, answer the board's questions. The FIN-FSA recommends that the questions, comments and conclusions of board members are entered in more detail in board minutes or their appendices.

The observed shortcomings may also be due to the fact that boards of directors do not have the competence necessary to assess and challenge the actions of internal control functions. Boards, moreover, have not necessarily embraced their task of challenging executive management. The FIN-FSA recommends that the boards of supervised entities require regularly from executive management a report on the basis of which the board can assess the effectiveness and resourcing of independent control functions. In addition, the board should assess, at least annually, the effectiveness and suitability of the outsourced function in relation to the entity's business. In that case, outsourced compliance should not be present at the board meeting. The board should also consult annually with the compliance function and other representatives of the internal control functions without the presence of executive management.

7 Fit & proper obligation

The Fit & Proper assessment applies to both the outsourced compliance officer and the supervised entity's own person responsible for compliance as the persons responsible for key functions of the entity. Before selecting a person for a position, the supervised entity must assess whether the person in question meets the Fit & Proper requirements set by regulations (also in terms of professional competence). These requirements must be clearly set out to support the decision-making of the organisation making the selection. It is an obligation of the supervised entity to obtain all the necessary information and clarifications from the person in question. In addition, the supervised entity must assess the significance of matters that may only come to light as a result of the FIN-FSA's investigations. The task of the FIN-FSA is to verify the appropriateness of the assessment made by the supervised entity.

The FIN-FSA must be notified of new appointments and changes, and of the Fit & Proper assessments related to them. The FIN-FSA recommends that the Fit & Proper notification is submitted to the FIN-FSA in good time prior to the appointment decision. The notification must, however, always be made without delay after an appointment decision or change of tasks, if nothing else is required in the regulations or in the FIN-FSA's regulations and guidelines based on them.