Investment firms, fund management companies, AIF managers

The FIN-FSA's thematic evaluation of the organisation of the compliance function in supervised entities

The Financial Supervisory Authority (FIN-FSA) has conducted an evaluation of the organisation and quality of the compliance function of investment firms, fund management companies and alternative investment fund (AIF) managers. The compliance function is responsible for ensuring compliance with legal provisions and internal policies and constitutes an integral part of supervised entities' internal governance and control.

In its thematic evaluation, the FIN-FSA observed shortcomings in the organisation of the compliance function in a majority of supervised entities. The following observations and shortcomings were identified:

- The board of directors' measures to set up a compliance function were not adequate.
- A person in charge of the compliance function had not been appointed.
- The function had been combined with other supervisory tasks without taking sufficient measures to ensure the independence of the compliance function.
- The thematic evaluation was unable to ascertain the sufficiency of staff resources.
- No risk assessment related to regulatory non-compliance had been conducted, or the risk assessment had not been updated.
- Shortcomings were identified in the outsourcing agreements of supervised entities that had outsourced the compliance function to another company of the same group.

In 2016, the FIN-FSA conducted, for purposes of a thematic evaluation, a survey among supervised entities on the organisation and resources of the compliance function. The survey was returned by 96 supervised entities – all the investment firms, fund management companies and AIF managers with appropriate authorisation at the time. No meetings with supervised entities were arranged for the thematic evaluation, which was based on written documentation only.

The aim of the thematic evaluation was to establish how the compliance function and its tasks are set up, whether the independence of the function is ensured and whether sufficient quantitative and qualitative resources have been set aside for the function. In the thematic evaluation, special attention was focused on the regulatory compliance of outsourced functions.

Provisions on the compliance function of supervised entities are laid down in EU regulations and national legislation applicable to each type of supervised entity. Compliance function requirements for investment firms, and for fund management companies and AIF managers providing investment services, are also laid down in the FIN-FSA's standard 1.3 *Internal governance and organisation of activities* and the FIN-FSA's regulations and guidelines 12/2012 on certain aspects of the compliance function requirements arising from the Markets in Financial Instruments Directive (MiFID)[1]. In

[1] Not available in English. It incorporates ESMA/2012/388 Guidelines into the local regulatory framework.

addition, regulatory provisions on the compliance function of fund management companies are laid down in the FIN-FSA's regulations and guidelines 3/2011 *Organisation and code of conduct of investment fund activities*.

The compliance function provisions of various directives are broadly consistent, with the same key principles being applied to all the supervised entities covered by this thematic evaluation. Although there are compliance guidelines in place for investment firms only, the FIN-FSA takes the view that all the supervised entities covered by this thematic evaluation should aim at putting in place a compliance function that meets the standards of the FIN-FSA's regulations and guidelines 12/2012.

General aspects of the organisation of the compliance function

The practical organisation of the compliance function depends on a number of factors, such as the size of the supervised entity, the services provided and the structure of the supervised entity. A supervised entity may set up the function in many different ways but must ensure that the compliance function performs its tasks on a permanent basis. The function may be organised in a number of ways; it may e.g. be established as a separate unit or be run by one individual person. The staff of the compliance function may be subordinate to the compliance officer, or be employed elsewhere in the organisation and report to the compliance officer.

In setting up the compliance function, supervised entities must take into account the nature, scale and complexity of the business, in keeping with the principle of proportionality, while ensuring that the effectiveness of the function is not compromised, i.e. that the function has sufficient quantitative and qualitative human and other resources and the appropriate powers. When taking advantage of the principle of proportionality, the supervised entity must document the reasons for this and re-examine this on a regular basis. The principle of proportionality works in both ways: as the supervised entity's business grows or becomes more complex, the resources of the compliance function must be increased in response.

Permanence of the compliance function

The compliance function must be permanent and the supervised entity must therefore ensure that the tasks of the function are performed on an ongoing basis. Every company with appropriate authorisation must have a designated compliance officer in its service. The supervised entity should have in place a compliance policy adopted by the board of directors, which also defines issues ensuring the permanence of the compliance function, including the tasks of the function, the regularity of the tasks and stand-in arrangements.

The thematic evaluation found that as many as 22% of the supervised entities had not designated a compliance officer for the entity from among their own staff. Some of these supervised entities had appointed an employee of a parent or sister company as compliance officer, while some had not designated a compliance officer at all.

Compliance policy

According to the findings of the thematic evaluation, nearly all the supervised entities had a compliance policy in place, but only roughly half of them had defined all the regulatory issues required in the policy. A written description of the stand-in arrangements was missing from the

compliance policies of 35% of the supervised entities, while 55% of the supervised entities had failed to update and outline the schedule of their supervision programme.

Mostly, compliance policies lacked a definition of the expertise of compliance staff and a statement as to who can appoint and dismiss the compliance officer. The compliance policy should also define e.g. the position of the compliance function relative to other functions and the powers, tasks and competence of the compliance staff.

Role of the board of directors

The supervised entity's board of directors must, on an annual basis, control that the compliance policy is up to date and the compliance function effectively organised, and that the risks related to regulatory non-compliance are contained.

The thematic evaluation found that a majority of the board of directors had failed to perform these tasks: 35% had not evaluated the timelines of the compliance policy in the past year, 60% had not evaluated the effectiveness of the function, and 45% had not assessed the risks related to regulatory non-compliance to establish if they are contained.

The board of directors' attitude to the organisation of the compliance function and compliance tasks is reflected in the compliance culture of the company as a whole. It is the duty of the board of directors to foster such practices in the supervised entity as support the position of the compliance function and, by their own example, encourage staff not only to comply with legislation to the letter but also to evaluate whether the practices in place are appropriate and reasonable.

Independence of the compliance function

The compliance function must enjoy a position of independence in the supervised entity. The supervised entity should set up the compliance function so as to ensure that the compliance officer and other compliance staff perform their tasks independently of the other business and senior management. Compliance staff have an obligation to perform their tasks objectively.

Position of the compliance function in the supervised entity

To ensure the independence of the compliance function, the compliance policy should indicate who can appoint and dismiss the compliance officer. The compliance policy should also address any conflicts of interest arising from other tasks or responsibilities of compliance staff. If the supervised entity decides to diverge from the recommendations of the compliance report, such divergence should be documented.

The thematic evaluation found that 40% of supervised entities had not addressed possible conflicts of interest in the compliance policy or corresponding documentation. Similarly, 40% of supervised entities had failed to indicate who can appoint and dismiss the compliance officer.

Combining the compliance function with other supervisory measures

The supervised entity may combine the compliance function with other supervisory functions, but there must be documented reasons for such combination of functions, and this should not compromise the independence of the compliance function. Especially major supervised entities or

entities with a complex or complicated business should avoid combining the compliance function with other supervisory functions. Any conflicts of interest inherent in the combination of functions should be identified and minimised.

Of the 96 supervised entities covered by the evaluation, 65% had chosen not to combine the compliance function with other supervisory functions, although the compliance officer and other compliance staff might also have been entrusted tasks other than compliance tasks. Some supervised entities had combined the compliance function with the risk management or internal audit function, or both. Supervised entities that had combined the compliance function with other supervisory functions were mostly minor companies that were running the compliance function themselves, rather than outsourcing it.

The thematic evaluation established that 42% of the supervised entities that had combined the compliance function with other supervisory functions had not defined conflicts of interests in their compliance policy.

If, in keeping with the principle of proportionality, the supervised entity has come to the conclusion that the compliance officer should also take part in the tasks of the function monitored, such combination of tasks should be subject to periodic review. It cannot, however, be considered appropriate to combine the compliance function with the internal audit function, given that the internal audit function also reviews the compliance function.

In some supervised entities, a member of the board of directors acts as the compliance officer. It is possible for a board member to act as a compliance officer in minor supervised entities, provided that he or she is not at the same time responsible for the entity's business or a business area. It must also be ensured that the individual has enough time to spare for the performance of compliance tasks.

Resources of the compliance function

Appropriate qualitative and quantitative human resources must be allocated to the compliance function, taking into account the nature and scale of the supervised entity's business.

Competence of the compliance staff

The compliance staff must demonstrate appropriate expertise and experience to ensure the reliable performance of the compliance tasks. The compliance staff should be familiar with at least the EU and national law governing the supervised entity's business, and related regulations and guidelines. Staff should receive training on a regular basis to ensure maintenance of competence.

The compliance officer should demonstrate a high level of expertise and sufficient knowledge of the supervised entity's business. He or she should also possess the professional experience required for assessing the risks related to the compliance function.

The thematic evaluation sought to establish the quantity and quality of the experience of compliance officers and other compliance staff, and their training. The observation made was that roughly half of the compliance officers had more than five years of professional experience in handling compliance tasks, while one in five persons had 2–5 years of professional experience. Four in five compliance

officers had an academic degree in economics or law, while 10% had obtained a degree in General Securities qualification (of level 1 or 2).

According to the FIN-FSA's assessment, compliance staff demonstrated sufficient expertise and experience in proportion to the size and operations of the company, in two-thirds of supervised entities. However, for a third of supervised entities, the competence of compliance staff could not be sufficiently ascertained. The compliance staff should demonstrate both expertise and experience, and one cannot replace the other. The resources cannot be found sufficient e.g. in a context where lack of experience is combined with e.g. complexity of business or constant changes in business.

Quantitative resources of the compliance function

The thematic evaluation found that a third of supervised entities had allocated less than 5% of total staff to the compliance function. Although this figure does not directly imply that there is a shortage of resources, it, nevertheless, can be taken as a basis for comparisons of compliance resources across companies. This figure was above 10% for every second supervised entity, and 20% for one in five supervised entities.

The sufficiency of compliance staff resources should also be assessed in terms of the experience of compliance staff. Compliance staff resources should respond flexibly to changes in circumstances affecting the business or applicable regulations or other equivalent compliance risk.

According to the FIN-FSA's assessment, the compliance function was sufficiently resourced in proportion to the business and size of the entity, in roughly half of the supervised entities, whereas the FIN-FSA was unable to ascertain that the function was sufficiently resourced in nearly half of the supervised entities. In some supervised entities, there was a notable lack of compliance staff resources.

Tasks of the compliance function

Risk assessment and supervision programme

It is the duty of the compliance function to assist the supervised entity's board of directors in the management of risks related to regulatory non-compliance. The compliance policy should define the procedures for risk assessment. The supervised entity should use the risk assessment as a basis for defining the aims of the compliance function and deciding on the measures (supervision programme) to be adopted to monitor the sufficiency of the practices designed to ensure regulatory compliance.

The compliance function should conduct regular assessments of the risks related to regulatory non-compliance to ensure that the focus of supervisory measures and advisory activities remains appropriate.

The thematic evaluation found that nearly half of the supervised entities had not prepared any risk assessment at all since 2014, or had not updated it. Some of these companies did not either have in place a compliance policy laying down the procedures for risk assessment.

The review of the supervision programmes prepared by supervised entities found that only roughly 20% of supervised entities had in place a supervision programme as required by the regulations. In the case of one in three supervised entities, the supervision programme did not comply with the

applicable regulations, or was completely missing. The shortcomings in the supervision programmes were related e.g. to how risk assessments were reflected in supervisory priorities, or how broad the coverage of various business areas was. Shortcomings were also identified in the determination of appropriate supervisory tools and methodologies and in the regularity of updates of the supervision programme.

A third of supervised entities reported that they had prepared compliance reports with no observed deviations, while two-thirds reported that compliance reports always included observed deviations. The FIN-FSA takes the view that also compliance reports including no observed deviations should always be listed as one element of the risk assessment.

Reporting and advisory obligation

The compliance function must also report on its activities and the observations made to the supervised entity's board of directors at least on an annual basis. Another task of the compliance function is to advise and assist the supervised entity's board of directors and other staff in the fulfilment of their obligations.

As regards the reporting task of the compliance function, the thematic evaluation found that the reporting policies of nearly all the supervised entities were in line with regulatory requirements, i.e. they indicated the method of reporting, contents of the report, reporting frequency and recipients of the report.

The fulfilment of the advisory obligation was assessed by reviewing whether the compliance function participates in the preparation of internal guidelines, the approval process for new instruments, the customer complaints process and provision of guidance to potential tied agents.

A majority of the supervised entities had fulfilled their advisory obligation to satisfaction with respect to the areas covered by the thematic evaluation. 80–90% of supervised entities reported that the compliance function participates in the preparation of internal guidelines, the approval process for new instruments, the customer complaints process and/or provision of guidance to tied agents. The same supervised entities reported that the staff had been trained in issues related to regulatory compliance during the past year. Two-thirds of supervised entities also maintained a training register to keep track of training needs.

As regards the advisory obligation, the thematic evaluation also explored whether the compliance officer attends meetings of the board of directors or any other regular meetings of the supervised entity. Roughly 10% of compliance officers do not attend board meetings or any other company meetings, while 35% of supervised entities reported that the compliance officer attends board meetings. Other meetings include business meetings or risk control meetings, which are attended by most of the compliance officers who do not attend board meetings.

Outsourcing of the compliance function

The tasks of the compliance function may be outsourced either in part or in full. Regardless of the outsourcing arrangement, the supervised entity remains responsible for fulfilment of all the compliance function requirements. Moreover, there are additional requirements to be met by supervised entities that outsource the compliance function, such as evaluation of the service provider and conclusion of an outsourcing agreement.

The supervised entity should ensure the sufficiency of the resources and expertise, as well as financial operating capacity, of the entity providing the outsourced service. The supervised entity should have in place procedures for monitoring and assessing the performance of service providers running the outsourced activity.

The outsourcing agreement should define at least the compliance tasks to be outsourced, the powers and information rights of the service provider and details of its reporting to the supervised entity. In addition, the resources available to the service provider should be defined, and the method of regular contact with the service provider agreed.

Of the 96 supervised entities covered by the thematic evaluation, 40% had outsourced the compliance tasks in full, and a good 10% in part. This means that a little under half of the supervised entities had not outsourced any compliance tasks. The thematic evaluation did not suggest any correlation between the type of authorisation held by the supervised entity, its size or staff size, and the outsourcing approach, i.e. whether the compliance tasks were outsourced in full, in part, or not at all.

By contrast, the thematic evaluation found that the outsourcing of compliance tasks to a company of the same group was reflected in a deficient organisation of the function. Supervised entities that had outsourced compliance tasks to an external service provider had exercised more care when setting up the function. Around 60% of supervised entities with an outsourced compliance function had outsourced the tasks to another company of the same group. Eight companies were engaged as external service providers.

The thematic evaluation found that supervised entities that had outsourced the compliance tasks to another company of the same group had not, in their outsourcing agreements, agreed in sufficient detail on the powers, tasks and information rights of the compliance officer, the reporting procedures or ways of keeping himself or herself up to date. Shortcomings in the outsourcing agreements were identified in roughly 70% of these supervised entities. However, the outsourcing agreements of nearly all the supervised entities that had entered into an outsourcing agreement with an external service provider were found to comply with the requirements.

Supervised entities that had outsourced the compliance tasks were found to lack a compliance officer more often than other supervised entities. While 22% of all supervised entities had not appointed a compliance officer from among their own staff, the corresponding figure for supervised entities that had outsourced the compliance tasks was 40%. However, responsibility for the compliance function and for monitoring the outsourced services rests with each individual supervised entity itself.

Concluding remarks

The FIN-FSA requires that this supervisory letter be taken up for review at a meeting of the supervised entity’s board of directors. The minutes of the board meeting must indicate what conclusions the board has made, and what possible corrective action the board has decided to take, on account of the supervisory letter. A copy of the minutes of the board meeting must be submitted to the FIN-FSA by 15 December 2017.

The FIN-FSA requests that supervised entities, at the same time, indicate their designated compliance officer. Supervised entities that have combined the internal audit and compliance functions, must re-examine this combination and submit the findings to the FIN-FSA in the same connection.

The FIN-FSA also takes the view that supervised entities should always submit a fit and proper notification for the compliance officer in the same way as for members of the board of directors[2].

[2] See the FIN-FSA's standard RA 1.4 on the reporting of fitness and propriety to the Financial Supervision Authority, and the Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU, currently under preparation.