# ESMA's New Guidelines on the MiFID II Compliance Function Requirements

June 24, 2020

On 5 June 2020, the European Securities and Markets Authority (ESMA) published its final guidelines on certain aspects of the recast Markets in Financial Instruments Directive (MiFID II) compliance function requirements (the "Guidelines").

Recent years have seen regulators increasingly focus on testing the effectiveness of the compliance function of regulated firms, as well as a shift to principles-based and outcomes-led regulation, rather than prescriptive rulemaking in a push to encourage firms to instill cultural change led from the top down: a so-called "culture of compliance." This alert sets out some observations about the key aspects of the Guidelines that touch upon these themes and more as relevant to those responsible for compliance.

The Guidelines are technically applicable to MiFID firms (including credit institutions, management companies of Undertakings for Collective Investment in Transferable Securities Directive (UCITS) and Alternative Investment Fund Managers (AIFMs) carrying on MiFID services or activities). However, they are likely to inform regulatory expectations for other regulated firms, including fund managers carrying on non-MiFID services or activities. Therefore, the observations below will be of relevance to asset management firms across their business.

Whilst the Guidelines do not substantially depart from the prior iteration (see below), our observations do show incremental and nuanced differences in respect of the responsibility of the compliance function. Firms would benefit from performing a gap analysis of their current compliance framework against the Guidelines in order to assess if any changes are required to procedures, policies or internal templates.

## 1. What are the Guidelines?

The Guidelines update and supersede the guidance published by ESMA in 2012, on the basis of the compliance function requirements in the Markets in Financial Instruments Directive (MiFID) (the "2012 Guidelines").

At a high level, the organisational requirements in MiFID II require an in-scope firm (see below) to have in place robust systems and controls to mitigate risk, as well as an independent and effective compliance function to ensure regulatory compliance. The

**Contact Information**

For further information or advice, please contact one of the partners named below or your usual contact at Akin Gump.

**Helen Marshall**
Partner
helen.marshall@akingump.com
London
+44 20.7661.5378

**Ezra Zahabi**
Partner
ezra.zahabi@akingump.com
London
+44 20.7661.5367

**Suley Siddiqui**
Associate
ssiddiqui@akingump.com
London
+44 20.7661.5384

**Sahar Abas**
Trainee Solicitor
sahar.abas@akingump.com
London
+44 20.7012.9859

Guidelines are intended to provide greater clarity on these organisational requirements as they pertain to the compliance function.

The Guidelines are split into three parts:

I. Responsibility of the compliance function.
II. Organisational requirements of the compliance function.
III. Competent authority review of the compliance function.

The focus of this alert will be on the provisions concerning the responsibility of the compliance function.

## 2. Which firms are subject to the Guidelines?

The application of the Guidelines do not materially differ from the 2012 Guidelines in that it applies to firms in the European Union which are:

- Investment firms that carry on MiFID investment services or investment activities or sell or advise on structured deposits.
- Credit institutions in respect of their MiFID investment services or investment activities or when selling or advising on structured deposits.
- Management companies of UCITS in respect of their MiFID "top-up" services.
- AIFMs in respect of their MiFID "top-up" services.

## 3. How do the Guidelines differ from the 2012 Guidelines?

Although the objectives of the compliance function and the key principles underpinning the regime remain substantially the same, the Guidelines have, in places, introduced subtle and nuanced changes to the 2012 Guidelines. A summary of these is contained below.

I. Guideline 1 (compliance risk assessment) – more holistic compliance risk assessments:

A. Whilst the requirement to perform a risk assessment, identifying the level of compliance risk faced by an in-scope firm, is not new, the Guidelines provide more detail as to what compliance teams must capture in their risk assessments; in particular, when assessing compliance risks in the areas of investment services and ancillary services provided by a firm, the assessments now ought to encompass (among other things) the categories of the firm's clients, distribution channels and, where relevant, the internal organisation of the group.

II. Guideline 2 (monitoring obligations of the compliance function) – further guidance on the tools available to the compliance function as part of its monitoring tool-kit:

A. The Guidelines have elucidated a further example of a tool available to the compliance function to use as part of its tool-kit to monitor compliance risks, and that is conducting interviews with a relevant sample of the firm's clients. It is interesting that this example has specifically been drawn out, which may indicate that ESMA sees benefit in the compliance function going beyond the internal framework of a firm to fulfill its monitoring function.

III. Guideline 3 (reporting obligations of the compliance function) – compliance reporting: (i) more detail needed; (ii) greater involvement of senior management;

and (iii) organisational separation of the complaints management and compliance function (for larger/more complex firms):

A. The content of the compliance function's compliance reports to management, outlining the effectiveness of the overall control framework as well as risks facing the business, ought to contain more detail; for instance, reports must now contain information on (among other things) actions taken, details on product governance and complaints monitoring. In practice, compliance teams may have already included such information or adopted a format similar to that prescribed by the Guidelines, but it is clear that the expectation is now for more granular information to be contained in the compliance reports to management.

B. The Guidelines state that compliance reports are "suitable tools to warrant the necessary management attention." This appears to go further than the 2012 Guidelines, which outlined that such reports ought to be provided to management. The nature of this change, together with the requirement for greater levels of information in compliance reports (as above), suggest that ESMA's expectation is for management to have more visibility over compliance related risks and issues, as well as a more active role in monitoring, and engaging with, those issues.

   For authorised firms in the United Kingdom within the scope of the Guidelines, this clarification for management to have a more active role in compliance reporting may not, in practice, depart from current procedure. The Senior Managers and Certification Regime (SM&CR) was designed to ensure greater individual accountability by senior managers in respect of prescribed pools of risk; responsibility for oversight of the performance of the compliance function comprises part of a prescribed senior management responsibility that must be allocated to a senior manager; an integral part of that senior manager showing that they have met that responsibility will be to closely monitor and scrutinise compliance reports and to ensure the sufficiency of information being reported.

C. Subject to the principle of proportionality, it is suggested that firms organisationally separate the complaints management and compliance functions so as to mitigate the risk of conflicts of interest arising. This is likely to be more relevant to larger firms or those with more complex operations in light of the reference to proportionality.

IV. Guideline 4 (advisory and assistance obligations of the compliance function) – (i) further considerations as to what is meant by "compliance culture" and (ii) compliance training for management:

A. When thinking about a firm's compliance culture, management must now ensure that staff are engaged with contributing to the stability of the financial system, in addition to the existing consideration of investor protection outlined in the 2012 Guidelines.

B. The Guidelines introduce an express obligation on the compliance function to provide training to management on compliance related risks, though the remaining provisions on training remain unchanged from the 2012 Guidelines. In practice, most firms will have embedded some form of periodic training for management on compliance related issues and so perhaps the effect of this change for in-scope firms will be minimal.