

## Chapter 6

# Compliance, internal audit and financial crime

## 6.1 Compliance

[**Note:** ESMA has also issued guidelines under article 16(3) of the ESMA Regulation covering certain aspects of the MiFID compliance function requirements. See <http://www.esma.europa.eu/content/Guidelines-certain-aspects-MiFID-compliance-function-requirements> .]

### Application to a common platform firm

6.1.-2

**G**

For a *common platform firm*:

- (1) the *MiFID Org Regulation* applies, as summarised in ■ SYSC 1 Annex 1 3.2G, ■ SYSC 1 Annex 1 3.2-AR and ■ SYSC 1 Annex 1 3.2-BR; and
- (2) the *rules and guidance* apply as set out in the table below:

Subject	Applicable rule or guidance
Adequate policy and procedures	SYSC 6.1.1R, SYSC 6.1.1AG
Compliance function	SYSC 6.1.4-AG, SYSC 6.1.7R
Internal audit	SYSC 6.2.2G
Financial crime	SYSC 6.3.1R to SYSC 6.3.11G

### Application to an MiFID optional exemption firm and to a third country firm

6.1.-1

**G**

For a *MiFID optional exemption firm* and a *third country firm*:

- (1) the *rules and guidance* in this chapter apply to them as if they were *rules* or as *guidance* in accordance with ■ SYSC 1 Annex 1 3.2CR(1); and
- (2) those articles of the *MiFID Org Regulation* in ■ SYSC 1 Annex 1 2.8AR and 3.2CR apply to them as if they were *rules* or as *guidance* in accordance with ■ SYSC 1 Annex 1 3.2CR(2).

### Adequate policy and procedures

6.1.1

**R**

A *firm* must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the *firm* including its managers, employees and *appointed representatives* (or where applicable, *tiered agents*) with its obligations under the *regulatory system* and for countering the risk that the *firm* might be used to further *financial crime*.

[**Note:** article 16(2) of *MiFID* and article 12(1)(a) of the *UCITS Directive*]

**6.1.1A** **G** The *FCA* provides *guidance* on steps that a *firm* can take to reduce the risk that it might be used to further *financial crime* in *FCG* (Financial Crime Guide: A firm's guide to countering financial crime risks) and *FCTR* (Financial Crime Thematic Reviews).

**6.1.2** **R** A *management company* must, taking into account the nature, scale and complexity of its business, and the nature and range of financial services and activities undertaken in the course of that business, establish, implement and maintain adequate policies and procedures designed to detect any risk of failure by the *firm* to comply with its obligations under the *regulatory system*, as well as associated risks, and put in place adequate measures and procedures designed to minimise such risks and to enable the *FCA* to exercise its powers effectively under the *regulatory system* and to enable any other *competent authority* to exercise its powers effectively under the *UCITS Directive*.

[**Note:** article 10(1) of the *UCITS implementing Directive*]

**6.1.2A** **G** Other *firms* should take account of the adequate policies and procedures rule (■ SYSC 6.1.2 R) as if it were *guidance* (and as if should appeared in that rule instead of must) as explained in ■ SYSC 1 Annex 1 3.3 R(1).

**Compliance function**.....

**6.1.3** **R** A *management company* must maintain a permanent and effective compliance function which operates independently and which has the following responsibilities:

- (1) to monitor and, on a regular basis, to assess the adequacy and effectiveness of the measures and procedures put in place in accordance with ■ SYSC 6.1.2 R, and the actions taken to address any deficiencies in the *firm's* compliance with its obligations; and
- (2) to advise and assist the *relevant persons* responsible for carrying out *regulated activities* to comply with the *firm's* obligations under the *regulatory system*.

[**Note:** article 10(2) of the *UCITS implementing Directive*]

**6.1.3A** **G** (1) Other *firms* should take account of the compliance function rule (■ SYSC 6.1.3 R) as if it were *guidance* (and as if should appeared in that rule instead of must) as explained in ■ SYSC 1 Annex 1 3.3 R(1).  
(2) Notwithstanding ■ SYSC 6.1.3 R, as it applies under (1), depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to have a separate compliance function. Where a *firm* has a separate compliance function the *firm* should also take into account ■ SYSC 6.1.3 R and ■ SYSC 6.1.4 R as guidance.

**6.1.4** **R** In order to enable the compliance function to discharge its responsibilities properly and independently, a *management company* must ensure that the following conditions are satisfied:

- (1) the compliance function must have the necessary authority, resources, expertise and access to all relevant information;
- (2) a compliance officer must be appointed and must be responsible for the compliance function and for any reporting as to compliance required by ■ SYSC 4.3.2 R;
- (3) the *relevant persons* involved in the compliance functions must not be involved in the performance of the services or activities they monitor;
- (4) the method of determining the remuneration of the *relevant persons* involved in the compliance function must not compromise their objectivity and must not be likely to do so.

[Note: article 10(3) of the *UCITS implementing Directive*]

- 6.1.4-A** G In setting the method of determining the *remuneration of relevant persons* involved in the compliance function:
- (1) *firms* that ■ SYSC 19A applies to will also need to comply with the *Remuneration Code*;
  - (2) *firms* that ■ SYSC 19C applies to will also need to comply with the *BIPRU Remuneration Code*;
  - (3) *firms* that ■ SYSC 19D applies to will also need to comply with the *dual-regulated firms Remuneration Code*; and
  - (4) *firms* that the remuneration part of the *PRA Rulebook* applies to will also need to comply with it.
- 6.1.4A** R (1) A *firm* which is not a *common platform firm* or *management company* and which carries on *designated investment business* with or for retail clients or professional clients must allocate to a *director* or *senior manager* the function of:
- (a) having responsibility for oversight of the *firm's* compliance; and
  - (b) reporting to the *governing body* in respect of that responsibility.
- (2) In ■ SYSC 6.1.4A R (1) compliance means compliance with the rules in:
- (a) *COBS* (Conduct of Business sourcebook);
  - (b) *COLL* (Collective Investment Schemes sourcebook);
  - (c) *CASS* (Client Assets sourcebook); and
  - (d) *ICOBS* (Insurance: Conduct of Business sourcebook).
- 6.1.4-B** G In setting the method of determining the remuneration of *relevant persons* involved in the compliance function, *full-scope UK AIFMs* will need to comply with the *AIFM Remuneration Code*.
- 6.1.4C** G A *debt management firm* and a *credit repair firm* must appoint a compliance officer to be responsible for ensuring the *firm* meets its obligations under ■ SYSC 6.1.1R for any compliance function the *firm* has and for any reporting as to compliance which may be made under ■ SYSC 4.3.2R.

- 6.1.4-C** **G** (1) This *guidance* is relevant to an *SMCR firm* required to appoint a compliance officer under ■ SYSC 6.1.4R or article 22(3) of the *MiFID Org Regulation* as applicable.
- (2) Taking account of the nature, scale and complexity of its activities, the *firm* should have appropriate procedures to ensure that the removal or any other disciplinary sanctioning of the compliance officer does not undermine the independence of the compliance function.
- (3) In the *FCA's* view, it will be appropriate, in many cases, for the removal or any other disciplinary sanctioning of the compliance officer to require the approval of a majority of the *management body*, including at least a majority of its members who do not perform any executive function in the *firm*.
- 6.1.5** **R** A *management company* need not comply with ■ SYSC 6.1.4 R (3) or ■ SYSC 6.1.4 R (4) if it is able to demonstrate that in view of the nature, scale and complexity of its business, and the nature and range of financial services and activities, the requirements under those *rules* are not proportionate and that its compliance function continues to be effective.
- [Note: article 10(3) second paragraph of the *UCITS implementing Directive*]
- 6.1.6** **G** Other *firms* should take account of the proportionality *rule* (■ SYSC 6.1.5 R) as if it were *guidance* (and as if should appeared in that *rule* instead of must) as explained in ■ SYSC 1 Annex 1 3.3R(1).
- 6.1.7** **R** (1) This *rule* applies to a *common platform firm* conducting *investment services and activities* from a *branch* in another *EEA State*.
- (2) References to the *regulatory system* in ■ SYSC 6.1.1R, ■ SYSC 6.1.2 R and ■ SYSC 6.1.3 R apply in respect of a *firm's branch* as if *regulatory system* includes a *Host State's* requirements under *MiFID* and the *MiFID Org Regulation* which are applicable to the *investment services and activities* conducted from the *firm's branch*.
- [Note: article 16 of *MiFID*]

## 6.2 Internal audit

**6.2.1** **R** A *management company* must, where appropriate and proportionate in view of the nature, scale and complexity of its business and the nature and range of its financial services and activities, undertaken in the course of that business, establish and maintain an internal audit function which is separate and independent from the other functions and activities of the *firm* and which has the following responsibilities:

- (1) to establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the *firm's* systems, internal control mechanisms and arrangements;
- (2) to issue recommendations based on the result of work carried out in accordance with (1);
- (3) to verify compliance with those recommendations;
- (4) to report in relation to internal audit matters in accordance with **■ SYSC 4.3.2 R**.

[Note: article 11 of the *UCITS implementing Directive*]

**6.2.1A** **G** Other *firms* should take account of the internal audit *rule* (**■ SYSC 6.2.1 R**) as if it were *guidance* (and as if should appeared in that *rule* instead of must) as explained in **■ SYSC 1 Annex 1 3.3 R(1)**.

**6.2.1B** **G**

- (1) This *guidance* is relevant to an *SMCR firm* required to establish and maintain an internal audit function under article 24 of the *MiFID Org Regulation*.
- (2) Taking account of the nature, scale and complexity of its activities, the *firm* should have appropriate procedures to ensure that the removal or any other disciplinary sanctioning of the head of the internal audit function does not undermine the independence of the internal audit function.
- (3) In the *FCA's* view, it will be appropriate, in many cases, for the removal or any other disciplinary sanctioning of the head of the internal audit function to require the approval of a majority of the *management body*, including at least a majority of its members who do not perform any executive function in the *firm*.

**6.2.2**

**G**

- (1) The term 'internal audit function' in ■ SYSC 6.2.1R (and ■ SYSC 4.1.11G), and for a *common platform firm* in article 24 of the *MiFID Org Regulation*, refers to the generally understood concept of internal audit within a *firm*, that is, the function of assessing adherence to and the effectiveness of internal systems and controls, procedures and policies.
- (2) For a *firm* that is not an *SMCR firm*, the internal audit function is not a *controlled function* itself, but is part of the *systems and controls function* (CF28).
- (3) For an *SMCR firm*, the internal audit function is a *PRA controlled function* (SMF5).

**6.3 Financial crime**

- 6.3.1** R A *firm* must ensure the policies and procedures established under ■ SYSC 6.1.1 R include systems and controls that:

  - (1) enable it to identify, assess, monitor and manage *money laundering* risk; and
  - (2) are comprehensive and proportionate to the nature, scale and complexity of its activities.
- 6.3.2** G "*Money laundering risk*" is the risk that a *firm* may be used to further *money laundering*. Failure by a *firm* to manage this risk effectively will increase the risk to society of crime and terrorism.
- 6.3.3** R A *firm* must carry out a regular assessment of the adequacy of these systems and controls to ensure that they continue to comply with ■ SYSC 6.3.1 R.
- 6.3.4** G A *firm* may also have separate obligations to comply with relevant legal requirements, including the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the *Money Laundering Regulations*. ■ SYSC 6.1.1 R and ■ SYSC 6.3.1 R to ■ SYSC 6.3.10 G are not relevant for the purposes of regulation 76(6) or 86(2) of the *Money Laundering Regulations*, section 330(8) of the Proceeds of Crime Act 2002 or section 21A(6) of the Terrorism Act 2000.
- 6.3.5** G The *FCA*, when considering whether a breach of its *rules* on systems and controls against *money laundering* has occurred, will have regard to whether a *firm* has followed relevant provisions in the guidance for the *United Kingdom* financial sector issued by the Joint Money Laundering Steering Group.
- 6.3.6** G In identifying its *money laundering* risk and in establishing the nature of these systems and controls, a *firm* should consider a range of factors, including:

  - (1) its customer, product and activity profiles;
  - (2) its distribution channels;
  - (3) the complexity and volume of its transactions;

- (4) its processes and systems; and
- (5) its operating environment.

**6.3.7**

**G**

A firm should ensure that the systems and controls include:

- (1) appropriate training for its employees in relation to *money laundering*;
- (2) appropriate provision of information to its *governing body* and senior management, including a report at least annually by that firm's *money laundering reporting officer (MLRO)* on the operation and effectiveness of those systems and controls;
- (3) appropriate documentation of its risk management policies and risk profile in relation to *money laundering*, including documentation of its application of those policies (see ■ SYSC 9);
- (4) appropriate measures to ensure that *money laundering* risk is taken into account in its day-to-day operation, including in relation to:
  - (a) the development of new products;
  - (b) the taking-on of new customers; and
  - (c) changes in its business profile; and
- (5) appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity.

**6.3.8**

**R**

- (1) A firm must allocate to a *director* or *senior manager* (who may also be the *money laundering reporting officer*) overall responsibility within the firm for the establishment and maintenance of effective anti-*money laundering* systems and controls.
- (2) A firm may not allocate overall responsibility under (1) to a person who is approved to perform the *other overall responsibility function*.

**The money laundering reporting officer**.....

**6.3.9**

**R**

A firm (with the exception of a *sole trader* who has no employees) must:

- (1) appoint an individual as *MLRO*, with responsibility for oversight of its compliance with the *FCA's rules* on systems and controls against *money laundering*; and
- (2) ensure that its *MLRO* has a level of authority and independence within the firm and access to resources and information sufficient to enable him to carry out that responsibility.

**6.3.10**

**G**

The job of the *MLRO* within a firm is to act as the focal point for all activity within the firm relating to anti-*money laundering*. The *FCA* expects that a firm's *MLRO* will be based in the *United Kingdom*.

---

**Financial crime guidance**

6.3.11

**G**

The *FCA* provides *guidance* on steps that a *firm* can take to reduce the risk that it might be used to further *financial crime* in *FCG* (Financial Crime Guide: A firm's guide to countering financial crime risks) and *FCTR* (Financial Crime Thematic Reviews).