



Senior Management Arrangements, Systems and Controls

[Please discard this page]

3.2 Areas covered by systems and controls

Introduction

3.2.1

G
01.12.01/001

This section covers some of the main issues which a *firm* is expected to consider in establishing and maintaining the systems and controls appropriate to its business, as required by ■ SYSC 3.1.1 R.

Organisation

3.2.2

G
01.12.01/001

A *firm's* reporting lines should be clear and appropriate having regard to the nature, scale and complexity of its business. These reporting lines, together with clear management responsibilities, should be communicated as appropriate within the *firm*.

3.2.3

G
01.12.01/001

- (1) A *firm's governing body* is likely to delegate many functions and tasks for the purpose of carrying out its business. When functions or tasks are delegated, either to *employees* or to *appointed representatives*, appropriate safeguards should be put in place.
- (2) When there is delegation, a *firm* should assess whether the recipient is suitable to carry out the delegated function or task, taking into account the degree of responsibility involved.
- (3) The extent and limits of any delegation should be made clear to those concerned.
- (4) There should be arrangements to supervise delegation, and to monitor the discharge of delegates' functions or tasks.
- (5) If cause for concern arises through supervision and monitoring or otherwise, there should be appropriate follow-up action at an appropriate level of seniority within the *firm*.

3.2.4

G
01.12.01/001

- (1) The *guidance* relevant to delegation within the *firm* is also relevant to external delegation ('outsourcing'). A *firm* cannot contract out its regulatory obligations. So, for example, under *Principle 3* a *firm* should take reasonable care to supervise the discharge of outsourced functions by its contractor.
- (2) A *firm* should take steps to obtain sufficient information from its contractor to enable it to assess the impact of outsourcing on its systems and controls.

3.2.5

G
01.12.01/001

Where it is made possible and appropriate by the nature, scale and complexity of its business, a *firm* should segregate the duties of individuals and departments in such a

way as to reduce opportunities for *financial crime* or contravention of requirements and standards under the *regulatory system*. For example, the duties of front-office and back-office staff should be segregated so as to prevent a single individual initiating, processing and controlling transactions.

Compliance

3.2.6

R

01.12.01/001

A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the *regulatory system* and for countering the risk that the *firm* might be used to further *financial crime*.

3.2.7

G

01.12.01/001

- (1) Depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to have a separate compliance function. The organisation and responsibilities of a compliance function should be documented. A compliance function should be staffed by an appropriate number of competent staff who are sufficiently independent to perform their duties objectively. It should be adequately resourced and should have unrestricted access to the *firm's* relevant records as well as ultimate recourse to its *governing body*.
- (2) The *regulatory objectives* are defined in section 2 of the *Act* and include 'the reduction of *financial crime*'. This objective is more fully described in section 6 of the *Act*. This describes 'any offence involving (a) fraud or dishonesty, (b) misconduct in, or misuse of information relating to, a financial market, or (c) handling the proceeds of crime'.
- (3) The *FSA's* detailed requirements for systems and controls with respect to *money laundering* are set out in the *Money Laundering* sourcebook (*ML*).

3.2.8

R

01.01.04/003

- (1) **A firm which carries on *designated investment business* with or for *customers* 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 3.2.8 R (1) "compliance" means compliance with the *rules* in:**
 - (a) **COB (Conduct of Business);**
 - (b) **CIS (Collective Investment Schemes); and**
 - (c) **CASS (Client Assets)**

3.2.9

G

01.12.01/001

- (1) ■ SUP 10.7.8 R uses ■ SYSC 3.2.8 R to describe the *controlled function*, known as the *compliance oversight function*, of acting in the capacity of a *director* or *senior manager* to whom this function is allocated.

- (2) The *rules* referred to in ■ SYSC 3.2.8 R (2) are the minimum area of focus for the *firm's compliance oversight function*. A *firm* is free to give additional responsibilities to a person performing this function if it wishes.

Risk assessment

3.2.10



01.12.01/001

- (1) Depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to have a separate risk assessment function responsible for assessing the risks that the *firm* faces and advising the *governing body* and *senior managers* on them.
- (2) The organisation and responsibilities of a risk assessment function should be documented. The function should be adequately resourced and staffed by an appropriate number of competent staff who are sufficiently independent to perform their duties objectively.

Management information

3.2.11



01.12.01/001

- (1) A *firm's* arrangements should be such as to furnish its *governing body* with the information it needs to play its part in identifying, measuring, managing and controlling risks of regulatory concern. Three factors will be the relevance, reliability and timeliness of that information.
- (2) Risks of regulatory concern are those risks which relate to the fair treatment of the *firm's customers*, to the protection of *consumers*, to confidence in the *financial system*, and to the use of that system in connection with *financial crime*.

3.2.12



01.12.01/001

It is the responsibility of the *firm* to decide what information is required, when, and for whom, so that it can organise and control its activities and can comply with its regulatory obligations. The detail and extent of information required will depend on the nature, scale and complexity of the business.

Employees and agents

3.2.13



01.12.01/001

A *firm's* systems and controls should enable it to satisfy itself of the suitability of anyone who acts for it.

3.2.14



01.12.01/001

- (1) ■ SYSC 3.2.13 G includes assessing an individual's honesty, and competence. This assessment should normally be made at the point of recruitment. An individual's honesty need not normally be revisited unless something happens to make a fresh look appropriate.
- (2) Any assessment of an individual's suitability should take into account the level of responsibility that the individual will assume within the *firm*. The nature of this assessment will generally differ depending upon whether it takes place at the start of the individual's recruitment, at the end of the probationary period (if there is one) or subsequently.
- (3) The *FSA's* detailed requirements on *firms* with respect to the competence of individuals are in the Training and Competence sourcebook (*TC*).

- (4) The requirements on *firms* with respect to *approved persons* are in Part V of the *Act* (Performance of regulated activities) and ■ SUP 10.

Audit committee

3.2.15

G

01.12.01/001

Depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to form an audit committee. An audit committee could typically examine management's process for ensuring the appropriateness and effectiveness of systems and controls, examine the arrangements made by management to ensure compliance with requirements and standards under the *regulatory system*, oversee the functioning of the internal audit function (if applicable) and provide an interface between management and the external auditors. It should have an appropriate number of *non-executive directors* and it should have formal terms of reference.

Internal audit

3.2.16

G

01.12.01/001

Depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to delegate much of the task of monitoring the appropriateness and effectiveness of its systems and controls to an internal audit function. An internal audit function should have clear responsibilities and reporting lines to an audit committee or appropriate *senior manager*, be adequately resourced and staffed by competent individuals, be independent of the day-to-day activities of the *firm* and have appropriate access to a *firm's* records.

Business strategy

3.2.17

G

01.12.01/001

A *firm* should plan its business appropriately so that it is able to identify, measure, manage and control risks of regulatory concern (see ■ SYSC 3.2.11 G (2)). In some *firms*, depending on the nature, scale and complexity of their business, it may be appropriate to have business plans or strategy plans documented and updated on a regular basis to take account of changes in the business environment.

Remuneration policies

3.2.18

G

01.12.01/001

It is possible that *firms'* remuneration policies will from time to time lead to tensions between the ability of the *firm* to meet the requirements and standards under the *regulatory system* and the personal advantage of those who act for it. Where tensions exist, these should be appropriately managed.

Business continuity

3.2.19

G

01.12.01/001

A *firm* should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness.

Records**3.2.20****R**

01.12.01/001

- (1) A *firm* must take reasonable care to make and retain adequate records of matters and dealings (including accounting records) which are the subject of requirements and standards under the *regulatory system*.
- (2) Subject to (3) and to any other record-keeping *rule* in the *Handbook*, the records required by (1) or by such other *rule* must be capable of being reproduced in the English language on paper.
- (3) If a *firm's* records relate to business carried on from an establishment in a country or territory outside the *United Kingdom*, an official language of that country or territory may be used instead of the English language as required by (2).

3.2.21**G**

01.12.01/001

A *firm* should have appropriate systems and controls in place to fulfil the *firm's* regulatory and statutory obligations with respect to adequacy, access, periods of retention and security of records. The general principle is that records should be retained for as long as is relevant for the purposes for which they are made.

3.2.22**G**

01.12.01/001

Detailed record-keeping requirements for different types of *firm* are to be found elsewhere in the *Handbook*. Schedule 1 to the *Handbook* is a consolidated schedule of these requirements.

Appendix 1

Matters reserved to a Home State regulator (see SYSC 1.1.1 R (1)(b) and SYSC 1.1.1 R (1)(c))

1.1 Matters reserved to a Home State regulator (see SYSC 1.1.1 R (1)(b) and SYSC 1.1.1 R (1)(c))

1.1.1 G The application of ■ SYSC 2.1.3R ■ SYSC 2.2.3G and ■ SYSC 3 to an *incoming EEA firm* or *incoming Treaty firm* depends on whether responsibility for the matter in question is reserved to the *firm* ? , *s Home State regulator*. This appendix contains *guidance* designed to assist such *firms* in understanding the application of those provisions. This appendix is not concerned with the *FSA* ? , *s rights* to take enforcement action against an *incoming EEA firm* or an *incoming Treaty firm*, which are covered in the Enforcement manual (*ENF*), or with the position of a *firm* with a *top-up permission*.

01.12.01/001

1.1.2 G The *Single Market Directives* and the *Treaty* (as interpreted by the European Court of Justice) adopt broadly similar approaches to reserving responsibility to the *Home State regulator*. To summarise, the *FSA*, as *Host State regulator*, is entitled to impose requirements with respect to activities carried on within the *United Kingdom* if these can be justified in the interests of the ? ”general good?” and are imposed in a non-discriminatory way. This general proposition is subject to the following in relation to activities passported under the *Single Market Directives*:

01.12.01/001

- (1) the *Single Market Directives* expressly reserve responsibility for the prudential supervision of an *ISD investment firm*, *BCD credit institution* or passporting *insurance undertaking* to the *firm* ? , *s Home State regulator*; accordingly, the *FSA*, as *Host State regulator*, is entitled to regulate only the conduct of the *firm* ? , *s business* within the *United Kingdom*;
- (2) article 11 of the *ISD* sets out various rules of conduct which the *FSA*, as *Host State regulator*, is required to impose on an *ISD investment firm* (including a *BCD credit institution* which is an *ISD investment firm*) in relation to *core investment services* (and, where appropriate, to *non-core investment services*) provided within the *United Kingdom*;
- (3) for a *BCD credit institution*, the *FSA*, as *Host State regulator*, is jointly responsible with the *Home State regulator* under article 27 of the *Banking Consolidation Directive* for supervision of the liquidity of a *branch* in the *United Kingdom*;

- (4) for an *ISD investment firm* (including a *BCD credit institution* which is an *ISD investment firm*), the protection of clients' money and clients' assets is reserved to the *Home State regulator* under the *ISD*; and
- (5) responsibility for participation in compensation schemes for *BCD credit institutions* and *ISD investment firms* is reserved in most cases to the *Home State regulator* under the *Deposit Guarantee Directive* and the *Investor Compensation Directive*.

1.1.3


01.12.01/001

It is necessary to refer to the case law of the European Court of Justice to interpret the concept of the "general good". To summarise, to satisfy the general good test, *Host State* rules must come within a field which has not been harmonised at a Community level, satisfy the general requirements that they pursue an objective of the general good, be non-discriminatory, be objectively necessary, be proportionate to the objective pursued and not already be safeguarded by rules to which the *firm* is subject in its *Home State*.

1.1.4


01.12.01/001

The *FSA* considers that it is entitled, in the interests of the general good, to impose the requirements in ■ SYSC 2.1.3R to ■ SYSC 2.2.3G (in relation to the allocation of the function in ■ SYSC 2.1.3R(2)) and ■ SYSC 3 on an *incoming EEA firm* and an *incoming Treaty firm*; but only in so far as they relate to those categories of matter responsibility for which is not reserved to the *firm's Home State regulator*.

1.1.5


01.12.01/001

Should the *FSA* become aware of anything relating to an *incoming EEA firm* or *incoming Treaty firm* (whether or not relevant to a matter for which responsibility is reserved to the *Home State regulator*), the *FSA* may disclose it to the *Home State regulator* in accordance with any applicable directive and the applicable restrictions in Part XXIII of the *Act* (Public Record, Disclosure of Information and Co-operation).

1.1.6


01.12.01/001

This appendix represents the *FSA's* views, but a *firm* is also advised to consult the relevant European Community instrument and, where necessary, seek legal advice. The views of the European Commission in the banking and insurance sectors are contained in two Commission Interpretative Communications (Nos. 97/C209/04 and C(1999)5046).

1.1.7


01.12.01/001

■ AUTH 5 Ann 1G summarises the application of the *Handbook* to an *incoming EEA firm*. That annex indicates in broad terms, and in relation to such *firms*, those categories of matter which are reserved to a *Home State regulator* and those which the *FSA*, as *Host State regulator*, is entitled to regulate when carried on within the *United Kingdom*.

1.1.8


01.01.04/002

Examples of how the *FSA* considers that ■ SYSC 3 will apply in practice to an *incoming EEA firm* (see ■ SYSC 1.1.4G) are as follows:

- (1) The interim Prudential sourcebook (insurers) (*IPRU (INS)*) does not apply to an *insurer* which is an *incoming EEA firm*. Similarly, ■ SYSC 3 does not require such a *firm*:
 - (a) to establish systems and controls in relation to financial resources (■ SYSC 3.1.1R); or
 - (b) to establish systems and controls for compliance with that Interim Prudential sourcebook (■ SYSC 3.2.6R); or
 - (c) to make and retain records in relation to financial resources (■ SYSC 3.2.20R).

-
- (2) The Conduct of Business sourcebook applies to an *incoming EEA firm*. Similarly, ■ SYSC 3 does require such a *firm*:
- (a) to establish systems and controls in relation to those aspects of the conduct of its business covered by applicable sections of *COB* (■ SYSC 3.1.1R);
 - (b) to establish systems and controls for compliance with the applicable sections of *COB* (■ SYSC 3.2.6R); and
 - (c) to make and retain records in relation to those aspects of the conduct of its business (■ SYSC 3.2.20R).

1.1.9


01.12.01/001

See also Question 12 in ■ SYSC 2.1.6G for guidance on the application of ■ SYSC 2.1.3R(2).

