Chapter 3

Systems and controls

3

3.2 Areas covered by systems and controls

Introduction

3.2.1 G 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 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
(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* or, where applicable, its *tied agents*, 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
(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 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.

3.2.5A R [deleted]

3.2.5B G [deleted]

Systems and controls in relation to compliance, financial crime and money laundering

3.2.6 R 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*.

3.2.6A R A *firm* must ensure that these systems and controls:

(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.

3.2.6B 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.

3.2.6C R A *firm* must carry out regular assessments of the adequacy of these systems and controls to ensure that it continues to comply with ■ SYSC 3.2.6A R.

3.2.6D 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 3.2.6 R to ■ SYSC 3.2.6J 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.

3.2.6E 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 *UK* financial sector issued by the Joint Money Laundering Steering Group.

3

3.2.6F 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.

3.2.6G 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 3.2.20 R to ■ SYSC 3.2.22 G);

(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.

3.2.6H R 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.

The money laundering reporting officer

3.2.6I R A *firm* 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.

3.2.6J 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

3.2.6K 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).

The compliance function

3.2.7 G (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) [deleted]

(3) [deleted]

3.2.8 R (1) A *firm* 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 (1) "compliance" means compliance with the *firm's* obligations under the *regulatory system* in relation to which the *FCA* has responsibility.

3.2.9 G ■ SUP 10C.6.1R uses ■ SYSC 3.2.8R 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.

Conduct risk oversight (Lloyd's) function

3.2.9A R In relation to business done at Lloyd's, the *Society* must allocate to a *director* or *senior manager* the function of having responsibility for overseeing the conduct of business standards required of *managing agents* for which the *Society* has responsibility.

3

Risk assessment

3.2.10 G

(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.

(3) The term 'risk assessment function' refers to the generally understood concept of risk assessment within a *firm*, that is, the function of setting and controlling risk exposure. The risk assessment function is not an *FCA controlled function* itself, but *firms* it may fall under the *PRA* chief risk officer *controlled function*.

(4) Paragraphs (1) and (3) do not apply to a *Solvency II firm* and (2) only applies as if the term 'risk assessment function' was replaced by 'risk management function'.

(5) *Solvency II firms* are subject to requirements for an effective risk management system in PRA Rulebook: Solvency II firms: Conditions Governing Business 3.

(6) Also, PRA Rulebook: Solvency II firms: Insurance Senior Management Functions makes the chief risk function a *PRA controlled function*. The chief risk function is the function of having responsibility for overall management of the risk management system, as specified in PRA Rulebook: Solvency II firms: Conditions Governing Business 3.

(7) The *FCA* will take the requirements in (5) and (6) into account.

Management information

3.2.11 G

(1) [deleted]

(2) [deleted]

3.2.11A G

(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 effective competition and to the integrity of the *UK financial system*. Risks which are relevant to the integrity of the *UK financial system* include risks which relate to its soundness, stability and resilience and to the use of the system in connection with *financial crime*.

3.2.11B G

3

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

3.2.14 G (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) [deleted]

(4) The requirements on *firms* with respect to *approved persons* are in Part V of the *Act* (Performance of regulated activities) and ■ SUP 10C and the Senior Insurance Management Functions parts of the *PRA Rulebook*

Audit committee

3.2.15 G 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 - see ■ SYSC 3.2.16 G) 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 (1) 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.

(2) The term 'internal audit function' 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. The internal audit function is not an *FCA controlled function* itself, but for certain *firms* it may fall under the *PRA* chief risk officer *controlled function*.

(3) Paragraph (1) does not apply to *Solvency II firms*.

(4) *Solvency II firms* are subject to a requirement in PRA Rulebook: Solvency II firms: Conditions Governing Business, rule 5 to have an effective internal audit function.

(5) Also, the PRA Rulebook: Solvency II firms: Insurance Senior Management Functions makes the chief internal audit function a *PRA controlled function*. The chief internal audit function is the function of having responsibility for management of the internal audit function specified in PRA Rulebook: Solvency II firms: Conditions Governing Business, rule 5.

(6) The *FCA* will take the requirements in (4) and (5) into account.

Business strategy

3.2.17 G 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 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. See also *Solvency II Regulation* (Article 275) and *EIOPA* Guidelines on system of governance dated 28 January 2015 (EIOPA-BoS-14/253 EN) (Guidelines 9 and 10).

Business continuity

3.2.19 G A *firm*, other than a *Solvency II 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 unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness. *Solvency II firms* are subject to the business continuity requirements in PRA Rulebook: Solvency II firms: Conditions Governing Business, 2.6, and the *FCA* will take those requirements into account.

Records

3.2.20 R (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 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.

3.2.21A G ■ SYSC 28 contains *rules* and *guidance* relating to knowledge and competence record keeping requirements in relation to *insurance distribution activities* undertaken by a *firm*.

3.2.22 G 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.

Investment strategy and investment decision making

3.2.23 G (1) This *guidance* sets out the *FCA's* expectation on how a *firm* may take into account *ESG financial considerations* and *other financial considerations* and *non-financial matters* as part of its *investment* strategy and *investment* decision making, to demonstrate compliance with *Principles* 2, 3, 6 or 8.

(2) This *guidance* only applies where the *firm's investment* strategy or *investment* decision could have a material impact on a *policyholder's investment* returns and relates to a product where:

(a) the primary purpose is to provide an *investment* return; and

(b) any *investment* risk is borne by a *policyholder* who is a natural person or a *relevant policyholder*.

(3) As part of its *investment* strategy or *investment* decision making, a *firm* should take into account *ESG financial considerations* and *other financial considerations* over the period of time that the *firm* reasonably considers is needed to achieve the *investment* objective or *investment* strategy.

(4) References to *other financial considerations* in (3) may include (but are not limited to) interest rate, liquidity, concentration, exchange rate, political and counterparty risks.

(5) As part of its *investment* strategy or *investment* decision making in relation to a product, a *firm* may take into account *non-financial matters* if:

(a) the *firm* has good reason to consider that affected *policyholders* or *relevant policyholders* would generally share the views on which the *non-financial matters* are based; and

(b) taking those matters into account would not involve a risk of a significant financial detriment to any affected *investment*.

(6) (5) does not apply to a *firm's investment* strategy or *investment* decision making in relation to a product (other than in relation to a *relevant scheme* or a *pathway investment*), that has been deliberately designed by the *firm* to take into account *non-financial matters*, and *policyholders* or *relevant policyholders* make an active decision to select that product.

3.2.23 R [deleted]

3.2.24 R [deleted]

3.2.25 R [deleted]

3.2.26 R [deleted]

3.2.27 R [deleted]

3.2.28 R [deleted]

3.2.29 R [deleted]

3.2.30 R [deleted]

3.2.31 R [deleted]

3.2.32 R [deleted]

3.2.33 R [deleted]

3.2.34 R [deleted]

3.2.35 R [deleted]

3.2.36 R [deleted]