Chapter 21

Risk control: additional guidance
21.1 Risk control: guidance on governance arrangements

Additional guidance on governance arrangements

(1) This chapter provides additional guidance on risk-centric governance arrangements for effective risk management. It expands upon the general organisational requirements in SYSC 2, SYSC 3, SYSC 4, SYSC 7 and FUND 3.7, and so applies to the same extent as SYSC 3.1.1 R (for insurers, managing agents and the Society), SYSC 4.1.1 R (for every other firm) and FUND 3.7 (for a full-scope UK AIFM of an authorised AIF).

(2) Firms should, taking account of their size, nature and complexity, consider whether in order to fulfil the general organisational requirements in SYSC 2, SYSC 3, SYSC 4, SYSC 7 and (for a full-scope UK AIFM of an authorised AIF) FUND 3.7 their risk control arrangements should include:

(a) appointing a Chief Risk Officer; and

(b) establishing a governing body risk committee.

The functions of a Chief Risk Officer and governing body risk committee are explained further in this section.

(3) The FCA considers that banks and insurers that are included in the FTSE 100 Index are examples of the types of firm that should structure their risk control arrangements in this way. However, this guidance will also be relevant to some similar sized firms (whether or not listed) and some smaller firms, by virtue of their risk profile or complexity.

(4) For Solvency II firms, the PRA Rulebook: Solvency II firms: Senior Insurance Management Functions makes the chief risk function a PRA controlled function.

(5) The chief risk function is having responsibility for overall management of the risk management system specified in PRA Rulebook: Solvency II firms: Conditions Governing Business, rule 3.

(6) Solvency II firms may read references to Chief Risk Officer in SYSC 21 as if it were a reference to the risk management function in the PRA Rulebook.
Chief Risk Officer

21.1.2

(1) A Chief Risk Officer should:

(a) be accountable to the firm’s governing body for oversight of firm-wide risk management;

(b) be fully independent of a firm’s individual business units;

(c) have sufficient authority, stature and resources for the effective execution of his responsibilities;

(d) have unfettered access to any parts of the firm’s business capable of having an impact on the firm’s risk profile;

(e) ensure that the data used by the firm to assess its risks are fit for purpose in terms of quality, quantity and breadth;

(f) provide oversight and challenge of the firm’s systems and controls in respect of risk management;

(g) provide oversight and validation of the firm’s external reporting of risk;

(h) ensure the adequacy of risk information, risk analysis and risk training provided to members of the firm’s governing body;

(i) report to the firm’s governing body on the firm’s risk exposures relative to its risk appetite and tolerance, and the extent to which the risks inherent in any proposed business strategy and plans are consistent with the governing body’s risk appetite and tolerance. The Chief Risk Officer should also alert the firm’s governing body to and provide challenge on, any business strategy or plans that exceed the firm’s risk appetite and tolerance;

(j) provide risk-focused advice and information into the setting and individual application of the firm’s remuneration policy (Where the Remuneration Code applies, see in particular ■ SYSC 19A.3.15 E. Where the BIPRU Remuneration Code applies, see in particular ■ SYSC 19C.3.15 E. Where the dual-regulated firms Remuneration Code applies, see in particular ■ SYSC 19D.3.16E. Where the remuneration part of the PRA Rulebook applies, see the PRA’s Supervisory Statement on Remuneration).

[Note: The PRA’s Supervisory Statement on remuneration is available on the PRA website at http://www.bankofengland.co.uk/pra/Pages/default.aspx]

(2) Firms will need to seek the FCA’s or PRA’s (as appropriate) approval for a Chief Risk Officer to perform:

(a) (for an SMCR firm that is a PRA-authorised person) the PRA’s Chief Risk Function controlled function; or

(b) (for an enhanced scope SMCR firm) the chief risk officer function.

(3) The FCA expects that where a firm is part of a group it will structure its arrangements so that a Chief Risk Officer at an appropriate level within the group will exercise functions in (1) taking into account group-wide risks.
Reporting lines of Chief Risk Officer

21.1.3 G
(1) The Chief Risk Officer should be accountable to a firm’s governing body.

(2) The FCA recognises that in addition to the Chief Risk Officer’s primary accountability to the governing body, an executive reporting line will be necessary for operational purposes. Accordingly, to the extent necessary for effective operational management, the Chief Risk Officer should report into a very senior executive level in the firm. In practice, the FCA expects this will be to the chief executive, the chief finance officer or to another executive director.

Appointment of Chief Risk Officer

21.1.4 G
(1) Firms should ensure that a Chief Risk Officer’s remuneration is subject to approval by the firm’s governing body, or an appropriate sub-committee.

(2) Firms should also ensure that the Chief Risk Officer may not be removed from that role without the approval of the firm’s governing body.

21.1.4A G
(1) This guidance is relevant to an SMCR banking firm that has appointed a chief risk officer.

(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 chief risk officer does not undermine the independence of the chief risk officer.

(3) It will be appropriate, in many cases, for the procedures in (2) to include that any approval for the removal of the chief risk officer requires the approval of a majority of the governing body, including at least a majority of its members who do not perform any executive function in the firm.

(4) Similarly, it will also be appropriate, in many cases, for any other disciplinary sanctioning of the chief risk officer to require the approval of a majority of the governing body, including at least a majority of its members who do not perform any executive function in the firm.

Governing body risk committee

21.1.5 G
(1) The FCA considers that, while the firm’s governing body is ultimately responsible for risk governance throughout the business, firms should consider establishing a governing body risk committee to provide focused support and advice on risk governance.

(2) Where a firm has established a governing body risk committee, its responsibilities will typically include:

(a) providing advice to the firm’s governing body on risk strategy, including the oversight of current risk exposures of the firm, with particular, but not exclusive, emphasis on prudential risks;
(b) development of proposals for consideration by the governing body in respect of overall risk appetite and tolerance, as well as the metrics to be used to monitor the firm’s risk management performance;

(c) oversight and challenge of the design and execution of stress and scenario testing;

(d) oversight and challenge of the day-to-day risk management and oversight arrangements of the executive;

(e) oversight and challenge of due diligence on risk issues relating to material transactions and strategic proposals that are subject to approval by the governing body;

(f) provide advice to the firm’s remuneration committee on risk weightings to be applied to performance objectives incorporated in the incentive structure for the executive;

(g) providing advice, oversight and challenge necessary to embed and maintain a supportive risk culture throughout the firm.

(3) Where a governing body risk committee is established, its chairman should be a non-executive director, and while its membership should predominantly be non-executive it may be appropriate to include senior executives such as the chief finance officer.

21.1.6 In carrying out their risk governance responsibilities, a firm’s governing body and governing body risk committee should have regard to any relevant advice from its audit committee or internal audit function concerning the effectiveness of its current control framework. In addition, they should remain alert to the possible need for expert advice and support on any risk issue, taking action to ensure that they receive such advice and support as may be necessary to meet their responsibilities effectively.