BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Supervisory Statement | SS21/15

Internal governance

April 2015

The proposed changes below should be made to the SS21/15 'Internal governance'. Underlining indicates new text and striking through indicates deleted text.

Risk control

2.18 The PRA considers that for a firm included within the scope of Internal Capital Adequacy Assessment 15, ~~SYSC 20 (Reverse stress testing)~~ the strategies, policies and procedures for identifying, taking up, managing, monitoring and mitigating the risks to which the firm is, or might be, exposed include conducting reverse stress testing. A firm that falls outside the scope of Internal Capital Adequacy Assessment 15 ~~SYSC 20~~ should consider conducting reverse stress tests on its business plan as well. This would further senior personnel's understanding of the firm's vulnerabilities and would help them design measures to prevent or mitigate the risk of business failure.

…

Risk control on governance arrangements

2.27 All CRR firms are obliged to appoint a chief risk officer, in addition CRR firms that are significant are obliged to have a risk committee and should read this supervisory statement in conjunction with the rules in the Risk Control Part of the Rulebook.

Chief Risk Officer

2.28 The PRA expects that a Chief Risk Officer should:

- ensure that the data used by the firm to assess its risks are fit for purpose in terms of quality, quantity and breadth;
- provide oversight and challenge of the firms systems and controls in respect of risk management;
- provide oversight and validation of the firm's external reporting of risk;
- ensure the adequacy of risk information, risk analysis and risk training provided to members of the firm's governing body;
- 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; and
- provide risk-focused advice and information into the setting and individual application of the firm's remuneration policy.

2.29 The PRA 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 2.28 taking into account group-wide risks.

2.30 The Chief Risk Officer should be accountable to a firm's governing body.

2.31 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.

2.32 The appropriate regulator recognises that in addition to the Chief Risk Officers 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 appropriate regulator expects this will be to the chief executive, the chief finance officer or to another executive director.

Governing body risk committee

2.33 The PRA considers that while the firm's governing body is ultimately responsible for risk governance throughout the business, firms that are not significant CRR firms should consider establishing a governing body risk committee to provide focused support and advice on risk governance.

2.34 The PRA expects that a governing body risk committee's responsibilities will typically include:

- 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;
- 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;
- oversight and challenge of the design and execution of stress and scenario testing;
- oversight and challenge of the day-to-day risk management and oversight arrangements of the executive;
- 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;
- providing advice to the firm's remuneration committee on risk weightings to be applied to performance objectives incorporated in the incentive structure for the executive; and
- providing advice, oversight and challenge necessary to embed and maintain a supportive risk culture throughout the firm.

2.35 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.

2.36 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.