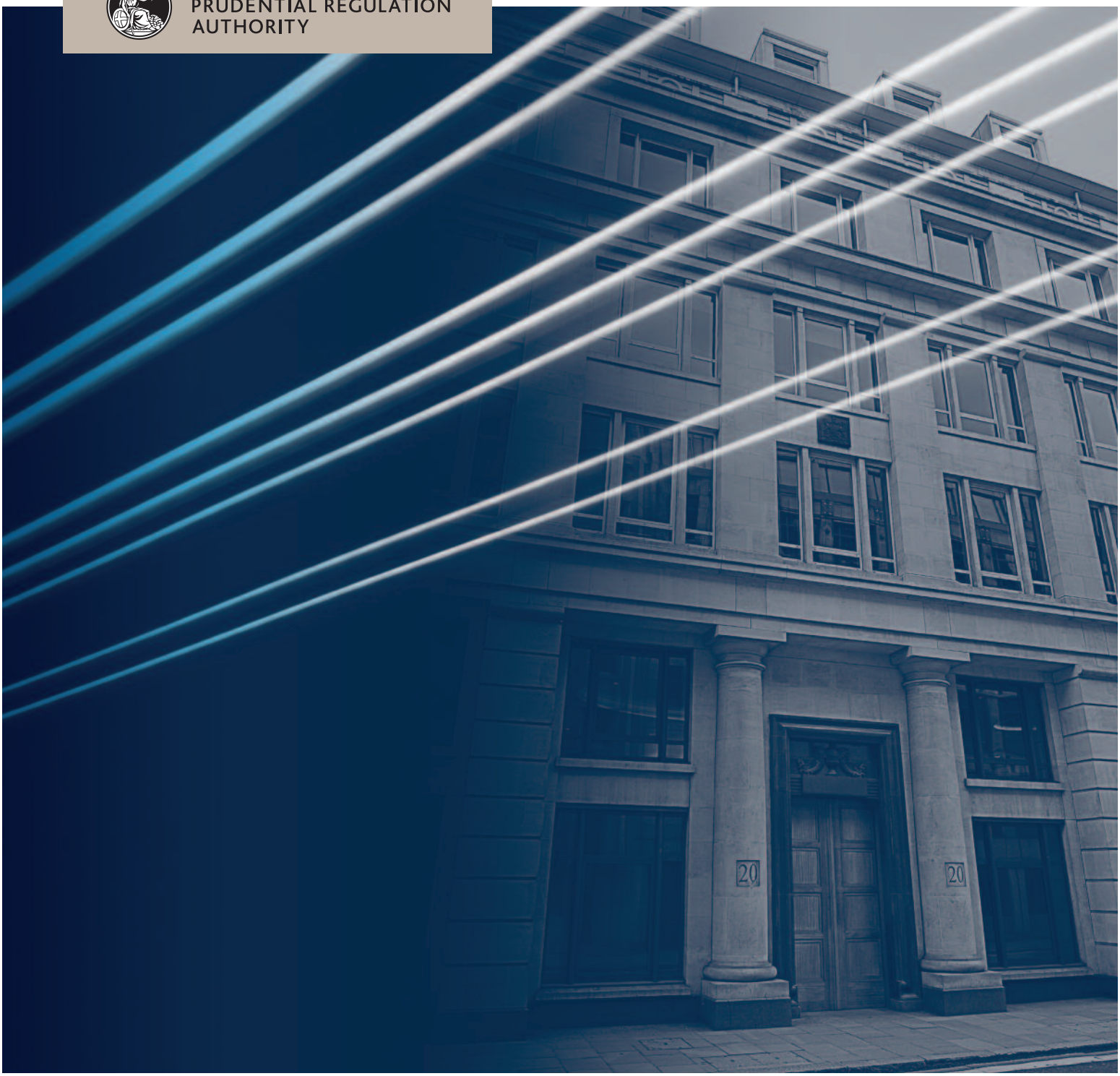
Supervisory Statement | SS21/15

Internal governance

April 2015

(Updated August 2015)



Prudential Regulation Authority
20 Moorgate
London EC2R 6DA

Prudential Regulation Authority, registered office: 8 Lothbury, London EC2R 7HH.
Registered in England and Wales No: 07854923

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Supervisory Statement | SS21/15

Internal governance

April 2015

(Updated August 2015)

1 Introduction

1.1 This supervisory statement is relevant to banks, building societies and Prudential Regulation Authority (PRA) designated investment firms. It sets out the expectations of the PRA in relation to how firms should comply with the rules in the General Organisational Requirements, Skills, Knowledge and Expertise, Compliance and Internal Audit, Risk Control, Outsourcing and Record Keeping Parts of the PRA Rulebook.

2 Internal governance

Business continuity

2.1 The PRA expects the matters dealt with in a business firm's continuity policy to include the following:

(a) resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;

(b) the recovery priorities for the firm's operations;

(c) communication arrangements for internal and external concerned parties (including the appropriate regulator, clients and the media);

(d) escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;

(e) processes to validate the integrity of information affected by the disruption; and

(f) regular testing of the business continuity policy in an appropriate and proportionate manner in accordance with Rule 2.8 in the General Organisational Requirements Part.

Audit committee

2.2 Depending on the nature, scale and complexity of its business, the PRA expects it may be appropriate for a firm to form an Audit Committee. An Audit Committee would typically examine management's process for ensuring the appropriateness and effectiveness of systems and controls.

2.3 The Audit Committee would also examine the arrangements made by management to ensure compliance with requirements and standards under the regulatory system, oversee the operations of the internal audit function (if applicable) and provide an interface between management and external auditors. It should have an appropriate number of non-executive directors and it should have formal terms of reference.

Persons who effectively direct the business

2.4 In the case of a body corporate, the PRA expects that the persons referred to in Rule 2.3 of the General Organisational Requirements Part of the PRA Rulebook should either be executive directors or persons granted executive powers by, and reporting immediately to, the governing body. In the case of a partnership, they should be active partners.

2.5 The PRA expects at least two independent minds should be applied to the formulation and implementation of the policies of a firm. Where a firm nominates two individuals to direct its business, the PRA will not regard them as both effectively directing the business where one of them makes some, albeit significant, decisions relating to only a few aspects of the business.

2.6 The two independent minds should be involved in the decision-making process on all significant decisions. Both should demonstrate the qualities and application to influence strategy, day-to-day policy and its implementation. This does not require their day-to-day involvement in the execution and implementation of policy. It does, however, require involvement in strategy and general direction, as well as knowledge of, and influence on, the way in which strategy is being implemented through day-to-day policy.

2.7 Where there are more than two individuals directing the business of a firm, the PRA does not regard it as necessary for all of these individuals to be involved in all decisions relating to the determination of strategy and general direction. However, at least two individuals should be involved in all such decisions. Both individuals' judgement should be engaged so that major errors leading to difficulties for the firm are less likely to occur.

2.8 Similarly, each individual should have sufficient experience and knowledge of the business, and the necessary personal qualities and skills, to detect and resist any imprudence, dishonesty or other irregularities by the other individual. Where a single individual, whether a chief executive, managing director or otherwise, is particularly dominant in such a firm, this will raise doubts about whether Rule 3.2 in the General Organisational Requirements Part of the PRA Rulebook is met.

Responsibility of senior personnel

2.9 In the PRA's view, the supervisory function does not include a general meeting of the shareholders of a firm, or equivalent bodies, but could involve, for example, a separate supervisory board within a two-tier board structure or the establishment of a non-executive committee of a single-tier board structure.

An individual's suitability

2.10 In the PRA's view, a firm's systems and controls should enable it to determine the suitability of anyone who acts for it. This includes assessing an individual's honesty and competence. This assessment should normally be made at the point of recruitment.

2.11 The PRA expects that any assessment of an individual's suitability takes into account the level of responsibility that the individual will assume within the firm. The nature of this assessment will generally differ depending on 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.

Segregation of functions

2.12 In the PRA's view, the effective segregation of duties is an important element in the internal controls of a firm in the prudential context. In particular, it helps to ensure that no one individual is completely free to commit a firm's assets or incur liabilities on its behalf. Segregation can also help to ensure that a firm's governing body receives objective and accurate information on financial performance, the risks faced by the firm and the adequacy of its systems.

2.13 The PRA expects a firm to ensure that no single individual has unrestricted authority to do all of the following:

(a) initiate a transaction;

(b) bind the firm;

(c) make payments; and

(d) account for it.

2.14 Where a firm is unable to ensure the complete segregation of duties (for example, because it has a limited number of staff), it should ensure that there are adequate compensating controls in place (for example, frequent review of an area by relevant senior managers).

2.15 Where a firm outsources its internal audit function, the PRA expects it to take reasonable steps to ensure that every individual involved in the performance of this service is independent from the individuals who perform its external audit. This should not prevent services from being undertaken by a firm's external auditors provided that the work is carried out under the supervision and management of the firm's own internal staff.

Compliance remuneration

2.16 In setting the method of determining the remuneration of relevant persons involved in the compliance function, in the PRA's view, firms that SYSC 19A applies to will also need to comply with the Remuneration Code.

Internal audit

2.17 The term 'internal audit function' in Internal Audit 3.1 and General Organisational Requirements 2.1 in the PRA Rulebook refers to the generally understood concept of internal audit within a firm, ie, the function of assessing adherence to and the effectiveness of internal systems and controls, procedures and policies. The internal audit function is not a controlled function itself, but it is part of the systems and controls function (CF28).

Risk control

2.18 The PRA considers that for a firm included within the scope of Internal Capital Adequacy Assessment 15, 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 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.

2.19 In setting the method of determining the remuneration of employees involved in the risk management function, in the PRA's view, firms that SYSC 19A applies to will also need to comply with the Remuneration Code.

2.20 The PRA considers the term 'risk management function' in Rules 2.5 and 2.6 in the Risk Control Part of the PRA Rulebook to refer to the generally understood concept of risk assessment within a firm, that is, the function of setting and controlling risk exposure.

2.21 In Rule 3.2 of the Risk Control Part of the PRA Rulebook, a 'CRR firm that is significant' is subject to requirements regarding the establishment of nomination and risk committees and certain restrictions on the holding of certain combinations of directorships.

2.22 For the purposes of those requirements, a firm whose size, interconnectedness, complexity and business type gives it the capacity to cause some disruption to the UK financial system (and through that to economic activity more widely) by failing or by carrying on its business in an unsafe manner.

2.23 Rule 2.1 of the General Requirements Part of the PRA Rulebook requires a firm to have effective processes to identify, manage, monitor and report risks and internal control mechanisms. Except in relation to those functions described in Rule 2.1 of the Outsourcing Part of the PRA Rulebook, where a firm relies on a third party for the performance of operational functions which are not critical or important for the performance of relevant services and activities on a continuous and satisfactory basis, the firm should take into account, (in a manner that is proportionate given the nature, scale and complexity of the outsourcing), the rules in the Internal Governance Part of the PRA Rulebook complying with that requirement.

2.24 A firm should notify the PRA when it intends to rely on a third party for the performance of operational functions that

are critical or important for the performance of relevant services and activities on a continuous and satisfactory basis.

Record keeping

2.25 Subject to any other record-keeping rule, the PRA expects records to be capable of being reproduced in the English language on paper. Where a firm is required to retain a record of a communication that was not made in the English language, it may retain it in that language. However, it should be able to provide a translation on request. 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.

2.26 In relation to the retention of records for non-Markets in Financial Instruments Directive 2004/39/EC (MiFID) business, in the PRA's view, a firm should have appropriate systems and controls in place with respect to the adequacy of, access to, and the security of its records so that the firm may fulfil its regulatory and statutory obligations. With respect to retention periods, the general principle is that records should be retained for as long as is relevant for the purposes for which they are made.

Risk control on governance arrangements

Paragraphs 2.27–2.35 were added to Chapter 2 on 3 August 2015 following CP17/15 'The PRA Rulebook: Part 3'.

2.27 The PRA expects that CRR firms should, taking account of their size, nature and complexity, consider whether their risk control arrangements should include:

- appointing a Chief Risk Officer; and
- establishing a governing body risk committee.

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 firm's 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.

Governing body risk committee

2.32 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.

2.33 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.

2.34 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.

2.35 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.