icsa
The Chartered
Governance
Institute

ICSA member resource.
Downloaded by
on 24 September 2020.

Terms of reference for the risk committee

Guidance note

The Chartered
Governance Institute

June 2020

Terms of reference for the risk committee

ICSA member resource.
Downloaded by
on 24 September 2020.

Contents

Introduction 3

The UK Corporate Governance Code 5

Notes on the terms of reference 6

Outline terms of reference 7

Acknowledgement
This guidance note has been prepared with the assistance of a working group comprising members of The Chartered Governance Institute and Slaughter and May.

If you have any feedback on the content of these resources, or additional questions that you'd like to discuss, please contact The Chartered Governance Institute information centre: **020 7612 7035** | **informationcentre@icsa.org.uk**

© The Chartered Governance Institute, 2020

The information given in this report is provided in good faith with the intention of furthering the understanding of the subject matter. While we believe the information to be accurate at the time of publication, The Chartered Governance Institute and its staff cannot, however, accept any liability for any loss or damage occasioned by any person or organisation acting or refraining from action as a result of any views expressed therein. If the reader has any specific doubts or concerns about the subject matter they are advised to seek legal advice based on the circumstances of their own situation.

Terms of reference for the risk committee

ICSA member resource.
Downloaded by
on 24 September 2020.

Introduction

This guidance note proposes outline terms of reference for the risk committee of a company seeking to comply fully with the requirements of the UK Corporate Governance Code published in July 2018 (the Code) and reflects the FRC Guidance on Risk Management, Internal Controls and Related Financial and Business Reporting (FRC Guidance) published in September 2014. It is particularly relevant to significant banks and insurance firms that are required to have a separate board risk committee under the rules of the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA). It is also of relevance to other financial institutions and companies in other industry sectors where the board considers that a risk committee, separate from the audit committee, is considered necessary or desirable. This is a matter for each company and its board to determine.

This guidance note draws on the experience of company secretaries and is based on good practice as carried out in some of the UK's largest listed companies. The Code and FRC Guidance are available at www.frc.org.uk.

The outline terms of reference are intended as a guide for companies to adapt to their needs where the board decides it is necessary or desirable to have a separate risk committee. The risks associated with the operational activities of each company will be specific to the organisation. It is therefore essential that the duties of the risk committee are tailored to the needs of the company using a variety of reference sources and specific regulation. The duties need to be agreed in close collaboration with the senior management team, in particular the Chief Risk Officer (CRO) if the company has one.

In addition:

- Companies with additional primary listing(s) may need to amend the terms of reference in light of additional requirements in the relevant country, in particular the US Sarbanes-Oxley Act 2002.

- Some responsibilities that are relevant to certain companies or sectors only are shown in square brackets.

Terms of reference for the risk committee

ICSA member resource.
Downloaded by
on 24 September 2020.

The guidance notes on terms of reference for all board committees should be read together when allocating responsibilities to the committees. It is important to recognise the links and overlap between the responsibilities of board committees and consequently the need for each board committee to have full knowledge of the deliberations of other committees through reports to the board and, if possible, by appointing at least one member of a committee to each of the other committees.

Some or all of the duties undertaken by a risk committee could be undertaken by either the audit committee or by the board itself. It is important to ensure that duties are not allocated to more than one committee and that there are no gaps. The precise allocation of responsibilities should be detailed in the terms of reference for the risk committee and the audit committee, and should be agreed by the board.

ICSA member resource.
Downloaded by
on 24 September 2020.

The UK Corporate Governance Code

The Code states that:

'The board should […] establish a framework of prudent and effective controls, which enable risk to be assessed and managed [and] the board should carry out a robust assessment of the company's emerging and principal risks.'[1]

The Code recognises that companies may establish a separate board risk committee to review the company's internal control and risk management systems, or this function may be carried out by the board itself.[2] Banks and insurance companies are subject to the regulatory requirements of the PRA and the FCA, and may be required to have a separate board risk committee to carry out these and other risk functions. Where the board determines to establish a separate risk committee, it is essential that the risk committee is properly constituted with a clear remit and identified authority.

As with most aspects of corporate governance, the company must be seen to be doing all these things in a fair and thorough manner. The Code does not make specific recommendations on the risk committee, however this guidance reflects many of the Code's recommendations in respect of other board committees. The responsibilities of the risk committee and the authority delegated to it by the board should be set out in terms of reference and published on the company website.[3]

Where one is established, the risk committee should report to the board on the nature and content of discussion, on recommendations, and on actions to be taken, and adequate time should be made available for discussion when necessary.[4]

1 Code Principle C and Code Provision 28
2 Code Provision 25. See also FRC Guidance on Board Effectiveness 2018 paragraphs 120-122
3 FRC Guidance on Board Effectiveness 2018 paragraph 63
4 FRC Guidance on Board Effectiveness 2018 paragraph 62

ICSA member resource.
Downloaded by
on 24 September 2020.

Notes on the terms of reference

The outline terms of reference are indicative of good practice and are of particular relevance to regulated companies such as banks and insurance companies. The outline terms of reference should be used as a starting point only from which to develop terms of reference appropriate for the specific risks associated with the business of an individual entity.

The company secretary is responsible for helping the board and its committees to function effectively.[5] The company secretary (or their nominee) should act as secretary to the committee. The committee should also have access to the services of the company secretariat on all risk committee matters, including assisting the chair in planning the committee's work, drawing up meeting agendas, maintenance of minutes, drafting of material about its activities for the annual report, collection and distribution of information and provision of any necessary practical support. The company secretary should ensure that the risk committee receives information and papers in a timely manner to enable full and proper consideration to be given to the issues.

The frequency with which the risk committee needs to meet will vary depending on the nature, scale and complexity of the business of a company and external regulatory requirements, which may change from time to time.

5 FRC Guidance on Board Effectiveness 2018 paragraph 79

ICSA member resource.
Downloaded by
on 24 September 2020.

Outline terms of reference

Note: square brackets contain recommendations which are good practice, or alternative wording which will need to be tailored to suit the circumstances of the particular organisation or excluded where not relevant to the company.

1. Membership

1.1 The committee shall comprise at least [three] members, all of whom shall be independent non-executive directors. [The committee shall include at least one member of the audit committee and/or remuneration committee and/or include one non-executive director specifically responsible for risk.] [Members shall have appropriate knowledge, skills and expertise to fully understand risk appetite and strategy/members as a whole shall have relevant risk expertise.] [The committee as a whole shall have competence relevant to the sector in which the company operates.]

1.2 Members of the committee shall be appointed by the board on the recommendation of the nomination committee and in consultation with the chair of the risk committee. Appointments shall be for a period of up to three years which may be extended for up to two additional three-year periods, provided the director still meets the criteria for membership of the committee.

1.3 Only members of the committee have the right to attend committee meetings. However, the finance director and any CRO shall be expected to attend meetings of the committee on a regular basis and other individuals may be invited to attend all or part of any meeting as and when appropriate.

1.4 The board shall appoint the committee chair. In the absence of the committee chair and/or an appointed deputy at a committee meeting, the remaining members present shall elect one of themselves to chair the meeting.

ICSA member resource.
Downloaded by
on 24 September 2020.

2. Secretary

The company secretary, or their nominee, shall act as the secretary of the committee and will ensure that the committee receives information and papers in a timely manner to enable full and proper consideration to be given to issues.

3. Quorum

The quorum necessary for the transaction of business shall be [two] members.

4. Frequency of meetings

The committee shall meet at least [four] times a year at appropriate times and otherwise as required.

5. Notice of meetings

5.1 Meetings of the committee shall be called by the secretary of the committee at the request of the committee chair or any of its members, [or at the request of the CRO (or other head of risk) if they consider it necessary].

5.2 Unless otherwise agreed, notice of each meeting confirming the venue, time and date of the meeting, together with an agenda of items to be discussed, shall be forwarded to each member of the committee and any other person required to attend no later than [five] working days before the date of the meeting. Supporting papers shall be sent to committee members and to other attendees, as appropriate, at the same time.

6. Minutes of meetings

6.1 The secretary shall minute the proceedings and decisions of all committee meetings, including recording the names of those present and in attendance.

ICSA member resource.
Downloaded by
on 24 September 2020.

6.2 Draft minutes of committee meetings shall be circulated to all members of the committee. Once approved, minutes should be circulated to all members of the board unless, exceptionally, it would be inappropriate to do so.[6]

7. Engagement with shareholders

7.1 The committee chair should attend the annual general meeting to answer any shareholder questions on the committee's activities.[7] In addition the committee chair should seek engagement with shareholders on significant matters related to the committee's areas of responsibility.[8]

8. Duties

Note: The duties set out below are those which all risk committees should consider. Companies may wish to add to these duties to reflect specific risks associated with the company's individual business.

The committee should have oversight of the group as a whole and, unless required otherwise by regulation, carry out the duties below for the parent company, major subsidiary undertakings and the group as a whole, as appropriate.

8.1 Risk appetite, tolerance and strategy

The committee shall:

8.1.1 Advise the board on the company's overall risk appetite, tolerance and strategy, and the principal and emerging risks the company is willing to take in order to achieve its long-term strategic objectives.[9]

6 FRC Guidance on Board Effectiveness 2018 paragraph 65
7 FRC Guidance on Board Effectiveness 2018 paragraph 38
8 Code Provision 3
9 Code Principle O. See also FRC Guidance paragraph 24 and Appendix C

Terms of reference for the risk committee

ICSA member resource.
Downloaded by
on 24 September 2020.

The risk committee should seek assurance on the risks the company identifies as those to which the business may be exposed. The risks will be specific to the company's circumstances but are likely to include many of the following:

- Threats to the business model or future performance
- Operational risk
- Transactional risk
- Capital
- Insolvency
- Market risk
- Liquidity
- Counterparty risk
- Conduct risk
- Material litigation
- Reputational risk
- Environmental, Social and Governance (ESG) issues
- Ethical codes
- IT operations, including cyber risk
- Health and safety
- Pandemic risk
- Business continuity plans
- Duties under the Companies Act 2006

Other risks specific to the company's sector and its operations need to be identified and may, for example, include:

- Regulatory and legal risks
- Investment risk
- Insurance risk
- Credit limits
- Regulatory stress testing
- Risk exposures and limits
- Asset impairments
- Risk trends, concentrations and correlations
- Research and development
- Manufacturing and supply chains
- Terrorism
- Major accident

ICSA member resource.
Downloaded by
on 24 September 2020.

8.1.2 Advise the board on the likelihood and the impact of principal risks materialising, and the management and mitigation of principal risks to reduce the likelihood of their incidence or their impact.[10]

8.1.3 Advise the board on the risk aspects of proposed changes to strategy and strategic transactions including acquisitions or disposals, ensuring that a due diligence appraisal of the proposition is undertaken, focussing in particular on implications for the risk appetite, tolerance and strategy of the company, and taking independent external advice where appropriate and available.[11]

8.2 Narrative reporting

The committee shall carry out the following duties to assist the board in fulfilling its reporting responsibilities in the annual report.

8.2.1 Monitor and review the effectiveness of the company's risk management and internal control systems.[12]

8.2.2 Review the company's procedures to manage or mitigate principal risks and to identify emerging risks, to assist in the board's assessment of principal and emerging risks.[13]

8.2.3 Review and assess the company's risk appetite and associated stress testing.

8.2.4 Evaluate the company's principal risks, to be taken into account by the board when assessing the company's prospects.[14]

8.2.5 Review and approve the statements to be included in the annual report concerning internal controls and risk management.

10 FRC Guidance paragraph 35
11 FRC Guidance section 3
12 See Code Provision 29
13 See Code Provision 28
14 The viability statement. See Code Provision 31

ICSA member resource.
Downloaded by
on 24 September 2020.

8.3 Internal controls and risk management systems[15]

The committee shall oversee and seek suitable assurance regarding:

8.3.1 The risk exposures of the company, including risk to the company's business model, and solvency and liquidity risks.

8.3.2 The adequacy and effectiveness of the company's processes and procedures to manage risk and the internal control framework, including the design, implementation and effectiveness of those systems.[16]

8.3.3 The ability of the company's risk management and internal control systems to identify the risks facing the company and enable a robust assessment of principal risks.

8.3.4 The company's capability to identify and manage new and emerging risks.

8.3.5 The effectiveness and relative costs and benefit of particular controls.

8.3.6 The effectiveness of management's processes for monitoring and reviewing the effectiveness of risk management and internal control systems and ensuring corrective action is taken when necessary.

8.3.7 The company's ability to reduce the likelihood of principal risks materialising and the impact on the business of risks that do materialise.

8.3.8 The appropriateness of the company's values and culture and reward systems for managing risk and internal controls, and the extent to which the culture and values are embedded at all levels of the company.

8.3.9 The CRO's (or head of risk's) right of direct access to the chairman of the board and to the committee.

15 See FRC Guidance sections 2 and 4 and Appendix C
16 Code Principle O. See also FRC Guidance paragraph 24 and Appendix C

ICSA member resource.
Downloaded by
on 24 September 2020.

9. Reporting responsibilities

9.1 The committee chair shall report formally to the board on its proceedings after each meeting on all matters within its duties and responsibilities.

9.2 The committee shall provide advice to the remuneration committee on any risk weightings to be applied to performance objectives incorporated in the incentive structure for executive remuneration and make recommendations to the remuneration committee on clawback provisions.

9.3 The committee shall make whatever recommendations to the board it deems appropriate on any area within its remit where action or improvement is needed.

9.4 The committee shall compile a report of its activities to be included in the company's annual report, describing the work of the committee.[17]

10. Other matters

The committee shall:

10.1 Have access to sufficient resources in order to carry out its duties, including access to the company secretariat for advice and assistance as required.[18]

10.2 Be provided with appropriate and timely training, both in the form of an induction programme for new members and on an ongoing basis for all members.[19]

10.3 Give due consideration to all relevant laws and regulations, the provisions of the Code and published guidance, the requirements of the FCA's Listing Rules, Prospectus Regulation Rules and Disclosure Guidance and Transparency Rules sourcebook and any other applicable rules, as appropriate.

10.4 Oversee any investigation of activities which are within its terms of reference.

17 As required by the Code for other board committees
18 Code Provision 16 and FRC Guidance on Board Effectiveness 2018 paragraphs 79-85
19 FRC Guidance on Board Effectiveness 2018 paragraph 81

ICSA member resource.
Downloaded by
on 24 September 2020.

10.5 Work and liaise as necessary with all other board committees ensuring interaction between committees and with the board is reviewed regularly, taking particular account of the impact of risk management and internal controls on the work of other committees.[20]

10.6 Ensure that a periodic evaluation of the committee's performance is carried out.

10.7 At least annually, review its constitution and terms of reference to ensure it is operating at maximum effectiveness and recommend any changes it considers necessary to the board for approval.[21]

11. Authority

The committee is authorised to:

11.1 Request the attendance of any employee at a meeting of the committee and/or seek any information it requires from any employee of the company in order to perform its duties.

11.2 Delegate any matter or matters to another committee or person(s) as it deems appropriate.

11.3 Obtain, at the company's expense, independent legal or other professional advice on any matter within its terms of reference if it believes it necessary to do so.[22]

20 FRC Guidance on Board Effectiveness 2018 paragraph 65, FRC Guidance section 3 and FRC Guidance on Audit Committees 2016 paragraph 43
21 FRC Guidance on Board Effectiveness 2018 paragraph 63
22 FRC Guidance on Board Effectiveness 2018 paragraph 83

icsa

The Chartered
Governance
Institute

ICSA member resource.
Downloaded by
on 24 September 2020.

The Chartered Governance Institute is the qualifying and membership body for governance with over 125 years' experience of educating and supporting governance professionals. With a Royal Charter purpose of leading 'effective and efficient governance and administration of commerce, industry and public affairs', we provide professional development, guidance and thought leadership, and work with regulators and policy makers to champion high standards.

The Chartered Governance Institute
Saffron House
6–10 Kirby Street
London EC1N 8TS

June 2020

The Chartered
Governance Institute