ICSA Guidance on Terms of Reference
Risk Committee

Contents
If using online, click on the headings below to go to the related sections.

A  Introduction
B  Financial Reporting Council – the UK Corporate Governance Code
C  Walker Review
D  Kay Review
E  Financial Stability Board – Thematic Review on Risk Governance
F  Model Terms of Reference
A Introduction

This guidance note suggests model terms of reference for the risk committee of a company and is particularly relevant to banks and other financial institutions (BOFIs). It is also of relevance to companies in other industry sectors when a risk committee, separate from the audit committee, is considered necessary or desirable by the board. It is relevant for companies seeking to comply fully with the recommendations of the final report of the Walker review of corporate governance in UK banks and other financial industry entities (the Walker Review), published in November 2009. It draws on the experience of company secretaries and is based on best practice as applied in some of the UK’s top listed companies.

B The UK Corporate Governance Code\(^2\) (the Code)

The UK Corporate Governance Code (the Code) states that:

‘The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.’\

The Code does not make specific recommendations about the constitution and remit of the risk committee. However, with reference to the Code’s recommendations in respect of the audit, nominations and remuneration\(^4\) committees, it is considered advisable that the work undertaken by the risk committee should be described in a separate section of the company’s annual report and the committee chairman should attend the AGM to respond to any relevant questions relating to the committee’s responsibilities\(^5\). The Code recommends that the main roles and responsibilities of board committees should be set out in written terms of reference and be made ‘available’ (e.g. by including the information on a website maintained by or on behalf of the company).\(^6\) Best practice would therefore recommend formal documentation of the terms of reference for a risk committee, making a copy available where appropriate. Companies should go through a formal, documented process of considering their internal control procedures and risk management systems and, to effectively facilitate this process, it is important that the risk committee is properly constituted with a clear remit and authority delegated to it by the board as set out in a clear documented Terms of Reference (“TOR”) approved by the board.

In applying the principle in C.2 of the Code, the risk committee should refer to the FRC’s “Internal Control: Guidance to Directors” (formerly known as the Turnbull Guidance). This sets out best practice on risk management and internal control for UK listed companies.

C The Walker Review

The Walker Review recommendations require that:

---

3. The Code, Principle C.2
4. The Code, Paragraphs B.2.4, C3.8, D.2.1 and Appendix Page 34 comparison of DTR D.7.2.7 R and Code provisions – under D.2.1: a description of the work of the remuneration committee should be made available however in order to comply with DTR 7.2.7 R this information will need to be included in the corporate governance statement.
5. The Code, Paragraph, E.2.3
6. The Code, Footnote 7, Page 12
‘The board of a FTSE 100-listed bank or life insurance company should establish a board risk committee separately from the audit committee.’

The Walker Review states that the board risk committee should have responsibility for oversight and advice to the board on the current risk exposures and future risk strategy of the entity, including strategy for capital and liquidity management, and the embedding and maintenance of a supportive culture in relation to the management of risk across the company, alongside established prescriptive rules and procedures.

The Walker Review recommends that the boards of BOFIs should be served by a chief risk officer (the CRO) who should participate in the risk management and oversight process at the highest level on an enterprise-wide basis and have a status of independence from individual business units. The CRO should, alongside an internal reporting line to the chief executive officer or finance director, report to the risk committee and have direct access to the committee chairman. The CRO’s removal from office should require the prior agreement of the board and the CRO’s remuneration should be approved by the chairman of the board or the chairman of the remuneration committee.

The Walker Review states that the board risk committee should be a committee of the board comprising a majority of non-executive members and should be chaired by a non-executive director. The finance director should be a member or in attendance at meetings and the CRO should insofar as possible be present at all meetings. The board risk committee should have appropriate overlap with the audit committee, in particular involving the participation by the chairman of the audit committee.

The risk committee should also be attentive to the potential added value from seeking external input to its work as a means of taking full account of relevant experience elsewhere and challenging its analysis and assessment.

It is recognised as good practice for the company secretary, or his or her nominee, to act as secretary to the risk committee. The risk committee should have access to the services of the company secretariat on all risk committee matters. It should be the company secretary’s responsibility to assist in ensuring that the board and its committees are properly constituted and advised, and that there is clear and effective co-ordination between the board and its various committees.

The frequency with which the risk committee needs to meet will vary depending on the nature, scale and complexity of the company and the frequency of risk committee meetings may alter from time to time. As a general rule, most risk committees would be expected to meet at least quarterly.

The Walker Review includes a recommendation for a separate risk report to be included in the company’s annual report, which should:

- describe thematically the strategy of the company in a risk management context;
- include information on the key risk exposures inherent in the strategy, the associated risk appetite and tolerance;
- explain how risk appetite is assessed over time (covering both banking and trading book exposures) and the effectiveness of the risk management process over key risk exposures;
- provide high level information on the scope and outcome of the stress-testing programme; and
- report on membership of the risk committee, the frequency of meetings, whether external advice was taken

---

7 The Walker Review, Executive Summary and Recommendations, Governance of Risk, Recommendation 23, Page 19
8 The Walker Review, Recommendation 23, Page 19
9 The Walker Review, Recommendation 24 Page 19
10 The Walker Review, Recommendation 23, Page 19
11 The Walker Review, Chapter 6: Paragraph 6.15, Pages 95-96
12 The Walker Review, Recommendation 25, Page 20
and, if so, its source.\textsuperscript{13}

\section*{D Kay Review}

The final report of the Kay Review of UK Equity Markets and Long-Term Decision Making\textsuperscript{14} (the Kay Review) was published in July 2012. It is recommended that a risk committee should refer to and take note of the recommendations of the Kay Review particularly those in respect of wider shareholder consultation.

\section*{E Thematic Review on Risk Governance}

The Financial Stability Board member jurisdictions which includes G20 national supervisors and international standard setting bodies and other groupings, published their Periodic Peer Review Report on Risk Governance in February 2013\textsuperscript{15} (the Risk Governance Report). The Risk Governance Report recommends that the risk committee:

\begin{enumerate}
  \item \textit{is required to be a stand-alone committee, distinct from the audit committee;}
  \item \textit{has a chair who is an independent director and avoids “dual-hatting” with the chair of the board, or any other committee;}
  \item \textit{includes members who are independent;}
  \item \textit{includes members who have experience with regard to risk management issues and practices;}
  \item \textit{discusses all risk strategies on both an aggregated basis and by type of risk;}
  \item \textit{is required to review and approve the firm’s risk policies at least annually;}
  \item \textit{oversees that management has in place processes to ensure the firm’s adherence to the approved risk policies.}\textsuperscript{16}
\end{enumerate}

The above listed recommendations and the recommendations in relation to the risk committees’ role in appointing, assessing the performance of, and dismissing the CRO, and the broader recommendations and findings of the Risk Governance Report should be given due and careful consideration by risk committees.

\section*{F Model terms of reference}

\textit{Note: These model terms of reference are indicative of best practice and are of particular relevance for BOFIs. The model terms of reference should be used as a starting point only from which to develop terms of reference appropriate for the specific business of an individual entity. The square brackets in particular contain recommendations which are in line with best practice which may need to be amended to suit the size, complexity, business and/or circumstances of the particular organisation.}

\textsuperscript{13} The Walker Review, Recommendation 27, Page 20
\textsuperscript{14} The Kay Review of UK Equity Markets and Long-Term Decision Making, Interim Report, February 2012
\textsuperscript{15} Financial Stability Board, Thematic Review on Risk Governance, Peer Review Report, 12 February 2013, see http://www.financialstabilityboard.org/publications/r_130212.pdf
\textsuperscript{16} The Risk Governance Report, Part V, Sound Risk Governance Practices, The Risk Management Function, Pages 31-33
1. Membership

1.1 The committee shall comprise at least [three] members. The activities of the risk committee should involve participation by the chairman of the audit committee.\(^{17}\) A majority of members of the committee shall be independent non-executive directors.\(^{18}\) (Refer to the Code for guidance on circumstances likely to impact independence).\(^{19}\) Members of the committee shall be appointed by the board, on the recommendation of the nomination committee in consultation with the chairman of the risk committee.

1.2 The finance director shall be a committee member or in attendance at all meetings. The CRO shall be expected to attend at all meetings. The committee chairman shall decide, with the chief executive officer, whether the chief executive officer should be present at meetings.\(^{20}\)

1.3 Only members of the committee have the right to attend committee meetings. However, other individuals including the chairman of the board, chief executive officer, other directors, CRO, other representatives of the risk function, compliance, and internal and external audit may be invited to attend all or part of any meeting as and when deemed appropriate and necessary by the board or its risk committee.

1.4 Appointments to the committee shall be for a period of up to three years, which may be extended for further periods of up to three years, provided the director still meets the criteria for membership of the committee.

1.5 The board shall appoint the committee chairman who shall be a non-executive director.\(^{21}\) In the absence of the committee chairman and/or an appointed deputy, the remaining members present shall elect one of themselves to chair the meeting.

2. Secretary

The company secretary or his or her nominee shall act as the secretary of the committee.

3. Quorum

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

4. Frequency of meetings

The committee shall meet at least [three] times a year at appropriate times and otherwise as required.\(^{22}\)

5. Notice of meetings

5.1 Meetings of the committee shall be convened by the secretary of the committee at the request of any of its members or at the request of the CRO if he or she considers a meeting 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, all other non-executive directors and any other person required to attend, no later

---

\(^{17}\) The Walker Review, Chapter 6: Paragraph 6.15, Page 96
\(^{18}\) The Walker Review, Chapter 6: Paragraph 6.15, Page 95
\(^{19}\) The Code, Section B: Effectiveness, Code Provisions, Paragraph B.1.1, Page 11
\(^{20}\) The Walker Review, Chapter 6: Governance of Risk, Composition and role of the board risk committee, Paragraph 6.15, Page 95
\(^{21}\) The Walker Review, Chapter 6: Governance of Risk, Composition and role of the board risk committee, Paragraph 6.15, Page 95
\(^{22}\) The frequency and timing of meetings will differ according to the needs of the company. There should be as many meetings as required for the risk committee to effectively discharge its role and responsibilities and it is recommended that there should be no fewer than three meetings each year. Meetings should be organised so that attendance is maximised (for example by timetabling them to coincide with board meetings and/or other committee meetings, e.g. audit committee meetings).
than [five] working days before the date of the meeting. The agenda shall be circulated together with relevant supporting papers to committee members and to other attendees as appropriate.

6. Minutes of meetings

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

6.2 Draft minutes of committee meetings shall be circulated promptly to all members of the committee. Once approved, the minutes should be circulated to all other members of the board unless it would be inappropriate to do so in the opinion of the chairman of the risk committee.

6.3 Final signed copies of the minutes of the meetings of the risk committee should be maintained for the company’s records, in hard and soft copy where possible.

7. Annual General Meeting

The committee chairman should attend the annual general meeting to respond to questions from shareholders on the committee’s activities.

8. Duties

Note:

The list of duties below are those which all risk committees should consider. Companies may wish to add to this list. The list should be modified to accurately reflect the specific risks associated with the company’s individual business.

The committee should carry out the duties below for the parent company, major subsidiary undertakings and the group as a whole, as appropriate.

Within the duties set out below there are certain duties that could be undertaken by either the audit committee or the risk committee and there is some overlap in duties. The precise allocation of responsibilities should be detailed in the terms of reference for the audit committee and the terms of reference for the risk committee, and should be agreed by the board. It is recommended that the board should err on the side of overlapping duties on questions as critical as the capability of the executive team to manage and control risks within the agreed parameters for example.

The committee shall:

8.1 advise the board on the company’s overall risk appetite, tolerance and strategy, taking account of the current and prospective macroeconomic and financial environment and drawing on financial stability assessments such as those published by relevant industry and regulatory authorities including the Bank of England, the Prudential Regulation Authority, the Financial Conduct Authority and other authoritative sources that may be relevant for the company’s risk policies.

8.2 oversee and advise the board on the current risk exposures of the company and future risk strategy.

8.3 in relation to risk assessment and subject to overlap with the audit committee:

8.3.1 keep under review the company’s overall risk assessment processes that inform the board’s decision making, ensuring both qualitative and quantitative metrics are used;

23 The Walker Review, Chapter 6: Paragraph 6.15, Page 96
8.3.2 review regularly and approve the parameters used in these measures and the methodology adopted; and
8.3.3 set a standard for the accurate and timely monitoring of large exposures and certain risk types of critical importance.26

8.4 review the company’s capability to identify and manage new risk types [in conjunction with the audit committee].
8.5 before a decision to proceed is taken by the board, advise the board on proposed strategic transactions including acquisitions or disposals, ensuring that a due diligence appraisal of the proposition is undertaken, focussing in particular on risk aspects and implications for the risk appetite and tolerance of the company, and taking independent external advice where appropriate and available.27

8.6 review reports on any material breaches of risk limits and the adequacy of proposed action.
8.7 keep under review the effectiveness of the company’s internal financial controls and internal controls and risk management systems and review and approve the statements to be included in the annual report concerning internal controls and risk management.28

8.8 provide qualitative and quantitative advice to the remuneration committee on risk weightings to be applied to performance objectives incorporated in executive remuneration.29

8.9 review the adequacy and security of the company’s arrangements for its employees and contractors to raise concerns, in confidence, about possible wrongdoing in financial reporting or other matters. The committee shall ensure that these arrangements allow proportionate and independent investigation of such matters and appropriate follow up action.
8.10 review the company’s procedures for detecting fraud.
8.11 review the company’s procedures for the prevention of bribery.
8.12 consider and approve the remit of the risk management function and ensure it has adequate resources and appropriate access to information to enable it to perform its function effectively and in accordance with the relevant professional standards. The committee shall also ensure the function has adequate independence30 and is free from management and other restrictions.

8.13 recommend to the board the appointment and/or removal of the CRO.
8.14 review promptly all reports on the company from the CRO.
8.15 review and monitor management’s responsiveness to the findings and recommendations of the CRO.
8.16 ensure the CRO shall be given the right of unfettered direct access to the chairman of the board and to the committee31.

8.17 Work and liaise as necessary with all other board committees.

9. Reporting responsibilities

9.1 The committee chairman shall report to the board on its proceedings after each meeting on all matters within its duties and responsibilities.
9.2 The committee shall make whatever recommendations to the board it deems appropriate on any area within its remit where action or improvement is needed.
9.3 The committee shall produce a report of its activities and the company’s risk management and strategy to be included in the company’s annual report.32

9.4 The directors’ report in the annual report and accounts should set out risk management objectives and policies including in relation to financial instruments33.

10. Other matters

---

27 The Walker Review, Recommendation 26, Page 20
28 Unless this duty is carried out by the audit committee or the board as a whole.
29 The Walker Review, Chapter 6: Paragraph 6.18, Pages 96-97
30 The Walker Review, Chapter 6: Paragraph 6.21, Page 98
31 Financial Stability Board, Thematic Review on Risk Governance, Recommendation 1, iii, Page 4
32 Walker Review, Recommendation 27, Page 20
33 Sched 7 para 6 The Large and Medium-sized Companies and Groups (Accounts and Reports) Regulations 2008 (No. 410); DTR 4.1.11(6)
The committee shall:

10.1 have access to sufficient resources in order to carry out its duties, including access to the company secretariat for assistance as required;
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;
10.3 give due consideration to laws and regulations, the provisions of the Code and the requirements of the UK Listing Authority Listing, Prospectus and Disclosure and Transparency Rules and any other applicable rules, as appropriate;
10.4 oversee any investigation of activities which are within its terms of reference; and
10.5 arrange for periodic reviews of its own performance and, 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.

11. Authority

The committee is authorised:

11.1 to seek any information it requires from any employee/director of the company in order to perform its duties;
11.2 to obtain, at the company’s expense, external legal or other professional advice on any matter within its terms of reference where required; and
11.3 to request the attendance of any employee at a meeting of the committee as and when required.

This guidance note has been prepared with the assistance of a working group comprising ICSA members and Slaughter and May.