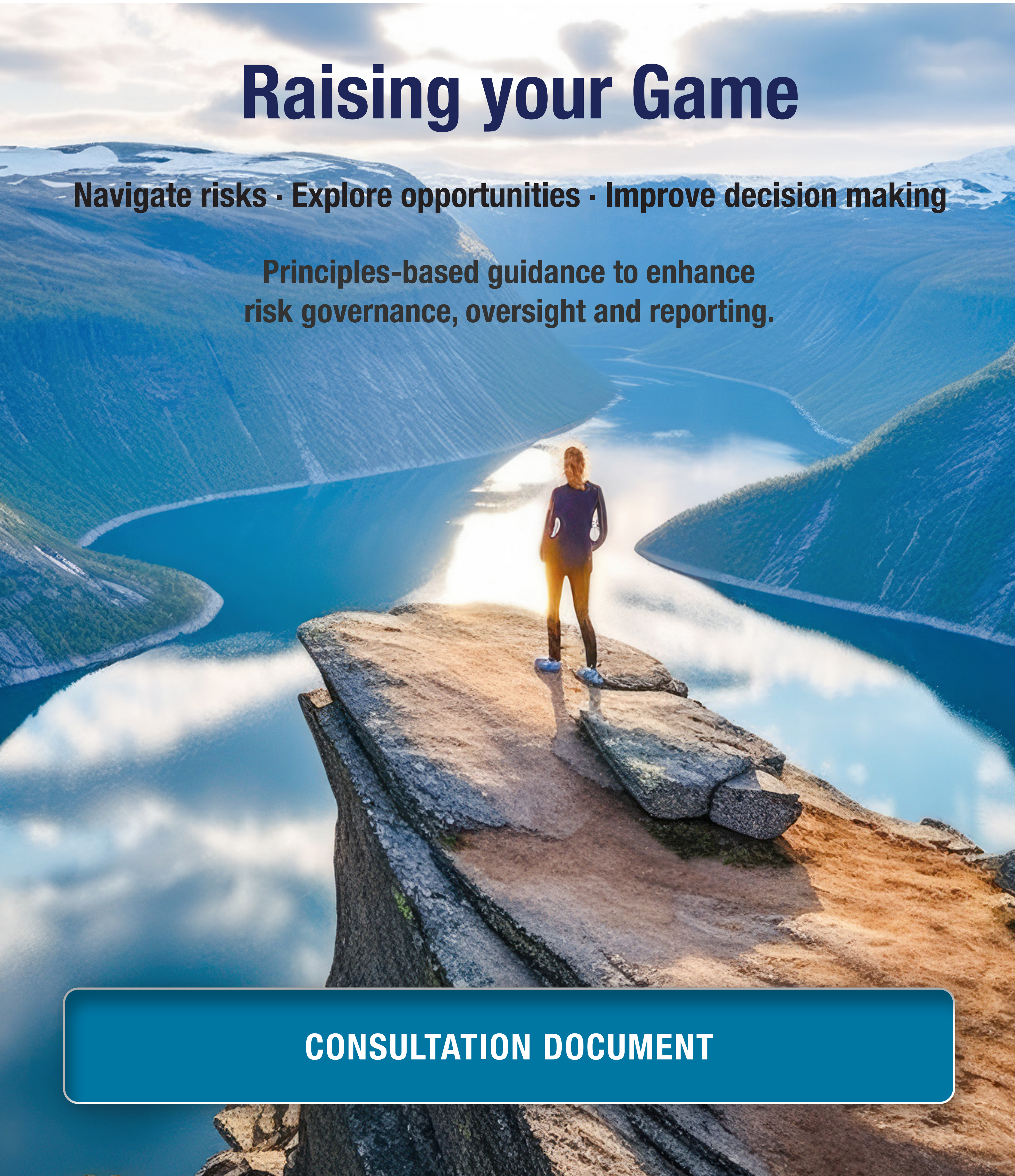
The Risk Coalition

Leading Risk Thinking



Raising your Game

Navigate risks · Explore opportunities · Improve decision making

Principles-based guidance to enhance risk governance, oversight and reporting.

CONSULTATION DOCUMENT

INTRODUCTION

Nearly five years ago, the Risk Coalition published 'Raising the Bar', its seminal guidance for board risk committees and second line risk functions in the UK financial sector.

Internationally recognised and still the gold standard for 'what good looks like' in financial sector risk governance and oversight, the Risk Coalition is soon to publish its new guidance, 'Raising your Game' - sector and jurisdiction agnostic leading practice risk governance guidance for boards and committees.

As we noted back in 2019, corporate mishaps, misbehaviour and failures remain all-too-common occurrences, with inadequate risk governance and oversight often at the heart of these issues.

Good risk management, however, is more than just about stopping bad things from happening. It is about enabling an organisation to achieve the things it wishes to achieve, through the effective management of risks. Key to this, is for organisations to have clarity of purpose and values supported by a clearly articulated strategy, strategic aims and objectives as illustrated in the strategic cascade below.

'Raising your Game' aims to help boards and committees across financial, commercial, public and not-for-profit sectors in the UK and globally, understand what good risk governance looks like. And, consequently, what steps they need to take to improve the quality and effectiveness of their organisation's risk arrangements.

The guidance is intended to be applied proportionately through application of professional judgment, and is not intended to be an exercise in compliance.

About this consultation

This document is the culmination of 18 months research and outreach by the Risk Coalition. The guidance is principles-based and does not aim to provide detailed instructions for the management of specific types of risks. Rather, the guidance provides a robust framework around which organisations can structure their risk arrangements.

The aim of this public consultation is to challenge and improve the text ahead of its planned publication in October 2024.

As such, we look forward to receiving as wide a range of views as possible and encourage you to submit your responses to our questions and any comments or suggestions you may have here, or by emailing team@riskcoalition.org.uk

The consultation closes on Monday 16th September, although we will aim to consider late responses as far as practicable.

The Risk Coalition
Leading Risk Thinking

About the Risk Coalition

The Risk Coalition is a not-for-profit, risk management think tank that aims to improve the effectiveness of risk management practice across sectors. It is supported by a network of professional bodies and membership organisations with an interest in raising standards of risk management - and corporate governance more broadly - in the UK and globally.

Support Us

As a not-for-profit, the Risk Coalition is entirely dependent on sponsorship and donations to support its public interest activities. Please contact us at team@riskcoalition.org.uk if you would like to discuss sponsoring 'Raising your Game' or any of our other planned projects.

Acknowledgements

We would like to publicly acknowledge and thank the following organisations for their valued sponsorship and support in developing 'Raising your Game':

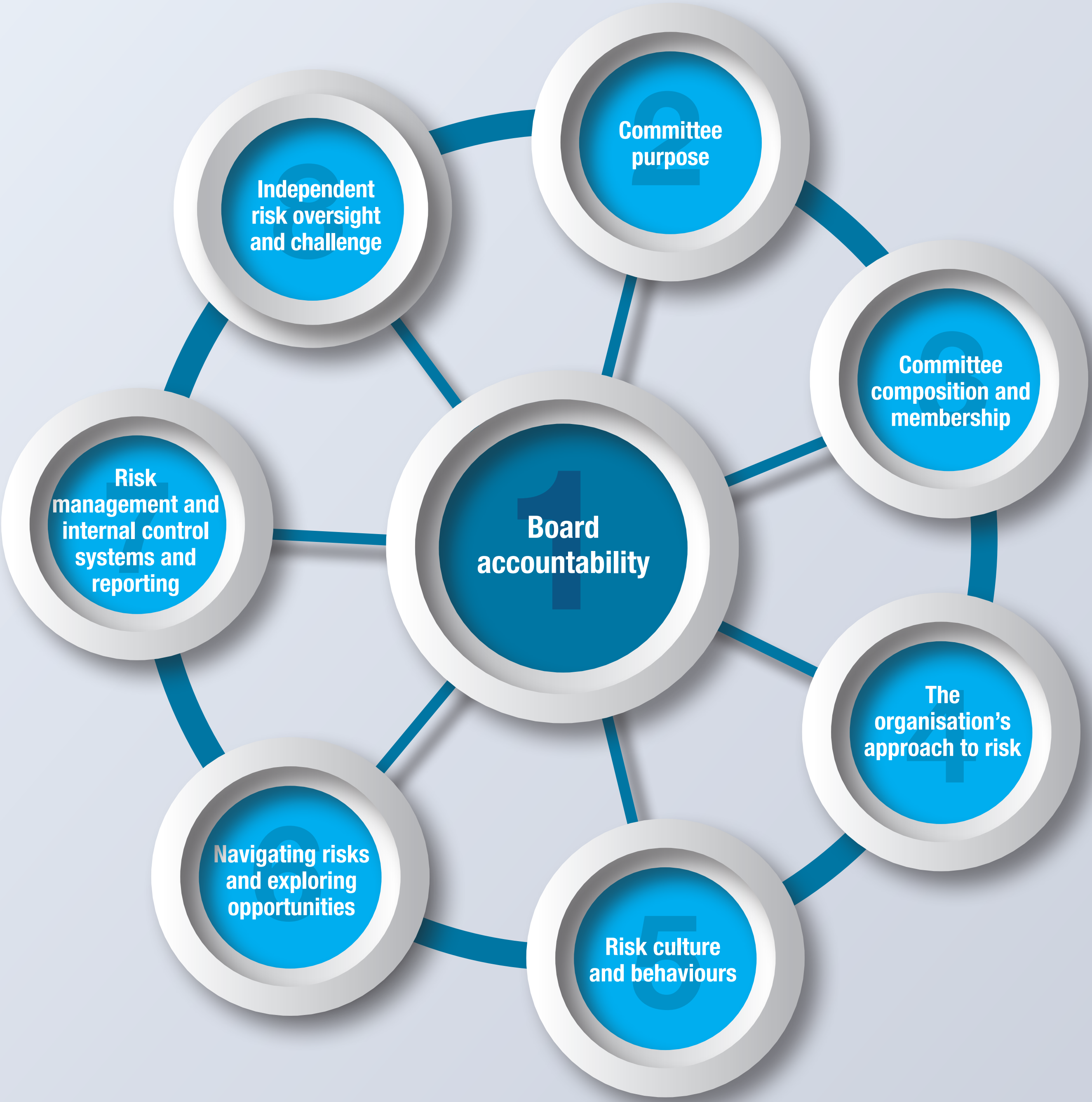
BARNETT WADDINGHAM beyond the expected

Diligent

dun & bradstreet

1 PRINCIPLES AND GUIDANCE – RISK GOVERNANCE, OVERSIGHT AND REPORTING

THE EIGHT PRINCIPLES



1

Principle 1

Board accountability

The board has ultimate accountability for the overall adequacy and effectiveness of the organisation's risk management arrangements.

In seeking to meet this principle, the board should:

1. establish a board risk policy that includes a clear articulation of the organisation's purpose, values and risk culture expectations, and defines the organisation's overall approach to - and appetite for – risk. The policy should clarify the board's expectations of the organisation's risk management arrangements, including key risk management related roles and responsibilities.
2. periodically review and approve the organisation's corporate strategy and associated strategic aims, objectives[1] and other opportunities ensuring they remain consistent with the organisation's board risk policy.
3. regularly consider whether the values and behaviours exhibited in the boardroom, by management and across the wider organisation are consistent with the organisation's stated purpose, values and risk culture expectations.
4. allocate responsibility for consolidated risk oversight to a nominated board committee ('the Committee')[2]. The board should oversee the work of the Committee, including the appropriateness of its agenda and matters considered, and endorse any recommendations or decisions made.
5. ensure that appropriate arrangements exist to support effective co-operation, co-ordination and communication between board committees when dealing with risk-related matters of common interest.
6. regularly consider whether the organisation is likely to achieve its strategic aims, objectives and other opportunities in the light of the principal and emerging risks attaching. For those strategic aims, objectives and other opportunities where concerns persist about their achievement, the board should decide on an appropriate course of action, taking into account the Committee's recommendations.
7. regularly monitor and periodically review whether the organisation's risk management arrangements meet board and other key stakeholder expectations, including supporting achievement of the organisation's strategic aims, objectives and other opportunities through the effective identification, assessment and successful navigation and/or management of risks.
8. seek regular independent assurance[3] that the organisation's risk management and internal control arrangements remain appropriate to the organisation's circumstances and are effective.

Notes

Best practice: Outcomes

In meeting this Principle a board demonstrates to all key stakeholders that it is using its best endeavours to fulfil its fiduciary duties and corporate governance requirements in terms of risk oversight.

---

1 An organisation's strategic aims and objectives should cover value creation and preservation objectives, and should also address the things the organisation chooses to do and those it is required to do, such as comply with law and regulation.

2 This could be through creation of a dedicated board risk committee, or through explicit allocation of consolidated risk oversight responsibility to the audit committee.

3 See guidance paragraph 37 for further information.

Principle 2

Committee purpose

The Committee is primarily an advisory committee[4] to the board. Its aim should be to facilitate focused and informed board discussions on risk-related matters.

In seeking to meet this principle, the Committee should:

9. through close co-ordination with the other board committees, provide consolidated oversight and challenge of management’s treatment and reporting of the organisation’s principal and emerging risks; consider how they might impact achievement of the organisation’s strategic aims, objectives and other opportunities.
10. periodically consider whether its planned cycle of activity remains appropriate to the board’s needs, including providing sufficient time for ad hoc or deep-dive exploration of key and emerging risk related topics and themes.
11. encourage and facilitate active board engagement on key risk-related topics. The Committee should consider escalation of contentious or strategically significant agenda items to the board for further consideration, even if within the Committee’s delegated decision-making authority.
12. periodically consider and recommend to the board whether the organisation should appoint an executive with independent risk oversight responsibility (a ‘risk director’)[5].
13. where practical, ensure that its meetings are scheduled such that the Committee can provide appropriate follow-up, resolution (including escalation if necessary) and reporting to the board on any outstanding questions.
14. provide a clear and concise written summary for inclusion in the board pack of the Committee’s activities and matters considered, and any associated recommendations or decisions.

Notes

Best practice: Outcomes

In meeting this Principle a Committee demonstrates that it plays a supportive and pro-active role in providing the board with the best possible risk intelligence and guidance.

---

[4] While the Committee is primarily an advisory committee to the board, it may have delegated decision-making authority in certain areas. Areas of delegated decision-making authority should be clearly defined within the Committee’s terms of reference, and all Committee decisions are subject to endorsement by the board.

[5] Different models of independent executive risk oversight exist. Some organisations may choose to appoint a dedicated risk director or chief risk officer, while others may place responsibility for independent executive risk oversight with the chief audit executive, if considered appropriate.

3

Principle 3

Committee composition and membership

The Committee should be formed of independent non-executive directors and apply relevant leading practice corporate governance guidance on composition, succession and performance evaluation criteria.

In seeking to meet this principle, the Committee should:

15. be chaired by an appropriately risk-experienced independent non-executive director and operate a collegiate culture that places value on open debate and diversity of thought and opinion.
16. have clear, board-approved terms of reference and an appropriate balance of skills, expertise and cognitive and experiential diversity. Committee members should have access to external expert risk advice and guidance as necessary.
17. encourage and facilitate subsidised Committee member participation in continuing professional development and learning opportunities[6].
18. provide a standing invitation to other board members and senior executives, including the executive with independent risk oversight responsibility (the 'risk director'), to attend Committee meetings as appropriate.

Notes

Best practice: Outcomes

In meeting this Principle a Committee demonstrates that best corporate governance practice underpins how it operates and remains up to speed.

[6] For example, through participation in industry bodies such as the Risk Coalition's Risk Committee Chairs' Forum.

4

Principle 4

The organisation's approach to risk

The Committee should provide the board with advice as to whether the organisation's approach to – and appetite for – risk, and its wider risk management arrangements, remain appropriate.

In seeking to meet this principle, the Committee should:

19. advise the board whether the organisation's approach to – and appetite for - risk as defined in the board risk policy remains appropriate to the organisation's evolving external environment and business model, while staying consistent with the organisation's purpose, values and risk culture expectations.
20. periodically review and constructively challenge management to demonstrate the effective implementation of the board risk policy, including whether the organisation's risk management arrangements:
    - are embedded within the day-to-day activities of the business and that on-going risk-focused training and education is provided at all levels;
    - clearly allocate key risk management and internal control related roles and responsibilities;
    - provide an effective means to monitor and manage the nature and extent of risks the organisation is willing to assume in seeking to achieve its strategic aims, objectives and other opportunities;
    - inform management decision-making through use of a clear decision-making framework; and
    - are consistent with the organisation's defined approach to risk and meet board and other key stakeholder expectations.
21. review and submit for board approval, proposed material changes to the organisation's:
    - board risk policy, including the organisation's approach to – and appetite for - risk; and
    - risk management framework, including risk governance and oversight arrangements.
22. ensure arrangements are in place to notify the board promptly of actual or likely material breaches of risk appetite, including significant weaknesses or failures in material controls; comment on the adequacy of management's response; recommend further actions where appropriate.

Notes

Best practice: Outcomes

In meeting this Principle a Committee demonstrates that it supports an organisation continuously reviewing its risk management arrangements, ensuring its risk policies are understood at all levels and taking appropriate actions to address any shortcomings or failures.

Principle 5

Risk culture and behaviours

The Committee should consider and periodically report to the board whether the organisation's purpose, values and risk culture expectations as defined in the board risk policy are appropriately embedded at all levels and are reflected in observed behaviours and decisions.

In seeking to meet this principle, the Committee should:

23. in conjunction with the remuneration committee, consider and advise the board whether proposed management remuneration plans, including long term incentive arrangements, are consistent with the organisation's board risk policy and likely to encourage appropriate, risk-based decision-making.
24. seek evidence (formal and informal) that management exhibits values and behaviours consistent with the organisation's board risk policy, and that these values and behaviours have been embedded effectively at all levels throughout the organisation.
25. constructively challenge whether the values and behaviours exhibited by management and the board provide those working for and with the organisation with appropriate support to 'do the right thing' in difficult or challenging circumstances.
26. continuously monitor whether management and the board's attitude towards - and treatment of - the heads of control functions[7], and the organisation's receptiveness to internal and external audit recommendations, is indicative of a healthy risk culture.

Notes

Best practice: Outcomes

In meeting this Principle a Committee demonstrates that the culture of the organisation is regarded as paramount by the board and that its values positively influence employee behaviours at all levels and ongoing business success.

[7] Heads of control functions typically include the executive with independent risk oversight responsibility, the chief compliance officer and the chief audit executive.

6

Principle 6

Navigating risks and exploring opportunities

The Committee should assess and advise the board on the likely achievement of the organisation's strategic aims, objectives and other opportunities in the light of the principal and emerging risks attaching.

In seeking to meet this principle, the Committee should:

27. constructively challenge management to demonstrate that they have identified, understand and are able to successfully navigate and/or manage those risks that may materially impact achievement of the organisation's strategic aims, objectives and other opportunities in the short-, medium- and long-term.

28. using a variety of means, contribute to and periodically assess the effectiveness of the organisation's emerging risk and opportunity identification and horizon scanning processes[8].

29. using all relevant sources of information and independent assurance available to it, regularly assess and advise the board whether the organisation appears likely to achieve its strategic aims, objectives and other opportunities in the light of the principal and emerging risks attaching.

    For those strategic aims, objectives and other opportunities where concerns persist about their achievement, the Committee should recommend to the board whether the organisation should:

    - take additional steps to increase certainty of achievement;
    - revise the relevant strategic aim; and/or
    - accept the reduced certainty of achieving the strategic aim.

30. assess whether executive management has identified and appropriately considered the material risks, as well as the potential opportunities, associated with proposed major projects, contracts and corporate actions.

31. periodically consider whether contractual and independent assurance arrangements in place over the provision of key intra-group or outsourced services provide sufficient confidence that material risks associated with the service provision are identified, assessed and managed effectively.

32. periodically explore and challenge management on the operational and financial resilience and on-going sustainability of the organisation's business model. This should include overseeing the selection and testing of a range of severe but plausible stress testing scenarios, as well as challenging management on the results of the analyses.

Notes

Best practice: Outcomes

In meeting this Principle a Committee demonstrates that it supports an organisation in taking the necessary steps to ensure it meets its objectives by identifying and mitigating associated risks and exploring fresh opportunities.

[8] In particular, the Committee should guard against positivity bias in management's estimations of risk likelihood, as well as probing potential interdependencies and linkages between risks through the use of scenario analysis and other methods.

Principle 7

Risk management and internal control systems and reporting

The Committee should routinely monitor and periodically review and advise the board on the effectiveness of the organisation's risk management and internal control arrangements, including the quality and completeness of key risk-related information.

In seeking to meet this principle, the Committee should:

33. constructively challenge management to demonstrate that:
    - the organisation's risk management arrangements meet board and other key stakeholder expectations, and support achievement of the organisation's strategic aims, objectives and other opportunities; and
    - it has robust processes in place to routinely monitor and periodically review the adequacy and effectiveness of the organisation's risk management and internal control arrangements, including the preparation, analysis and timely reporting of key risk and control-related information.
34. consider whether board-level risk and control-related reporting is both comprehensive and comprehensible, enabling non-executive directors to understand, probe and constructively challenge management effectively.
35. seek independent assurance that management's reporting of key risk and control-related information, including the likely achievement of the organisation's strategic aims, objectives and other opportunities, is complete, accurate and fairly presented.
36. review and recommend to the board for approval any material risk and control-related information for regulatory submission or external publication.
37. commission and oversee a programme of independent assurance activity to assess the adequacy and effectiveness of the organisation's risk management and internal control arrangements[16].

Notes

Best practice: Outcomes

In meeting this Principle a Committee demonstrates that an organisation has a well co-ordinated approach to the management and reporting of risk-related information and the quality of its supporting controls.

[9] The internal audit function may provide these independent assessments. As a matter of good practice, the Committee should commission an independent external review of the organisation's risk management and internal control arrangements every three to five years as appropriate.

8

Principle 8

Independent risk oversight and challenge

Where relevant, the Committee should safeguard the independence and objectivity of the executive with independent risk oversight responsibility (the 'risk director').

In seeking to meet this principle, the Committee should:

38. sponsor the development and board approval of a formal charter, consistent with the board risk policy, that defines the independence, objectivity, role and responsibilities of the risk director and the risk advisory function.
39. provide the risk director with direction and guidance on key areas of Committee interest, including periodically reviewing and approving the risk director's short-, medium- and long-term activity plans for the risk advisory function.
40. ensure that the risk director has a reporting line to the Committee chair, with an executive reporting line to the chief executive officer. The risk director should have unmediated access to the board chair, the board itself, the Committee, the external auditor and relevant regulatory authorities as appropriate.
41. assess whether the risk director is sufficiently senior and of an appropriate mindset, standing and gravitas to constructively challenge management risk-taking and decision-making effectively, and that the risk advisory function has adequate, appropriate resources (financial, people, processes and technology) to meet its charter obligations.
42. periodically challenge and assess the continued independence and objectivity of the risk director, particularly where their reporting lines are not consistent with this guidance, or where they have been in post for a significant period.
43. meet periodically with the risk director in the absence of other executives to provide an opportunity for an open and non-attributable discussion of any significant concerns the risk director may have.
44. in consultation with the chief executive officer, advise the board on the appointment or removal of the risk director, and the appropriateness of the risk director's remuneration arrangements.

Notes

Best practice: Outcomes

In meeting this Principle a Committee demonstrates that an organisation has a mature approach to risk oversight through appointing and supporting a dedicated senior executive with a clearly defined role and appropriate resources.

2 DEFINITION OF TERMS

Set out below are definitions for key terms used throughout this guidance. Wherever possible we have used standard definitions. In some cases, however, it has been necessary to develop definitions using several sources.

Accountability – In the context of this guidance, accountability for an action cannot be delegated but responsibility for performing it can.

Challenge – Use of carefully targeted questions to explore completeness of understanding and reasonableness of views, ideas and assumptions.

Executive management – Includes members of the executive committee and their direct reports.

Extended enterprise risks – those risks for which the organisation remains accountable, but for which it has outsourced (some or all) responsibility for management of risks to a third party, typically through an outsourcing arrangement or joint venture.

Horizon scanning – A process by which an organisation seeks to identify, assess and analyse new or emerging risks and opportunities, including emerging categories of risk, thereby enabling timely management action.

Independence – A risk director may be considered independent if:

- the risk function is organisationally separate from, and its staff do not perform any operational tasks within, areas of the business subject to its oversight;
- the risk director has a non-executive reporting line to the chair of the Committee and an executive reporting line to the Chief Executive Officer;
- decisions on risk director appointment, removal and remuneration are taken by the board on the advice of the Committee and Chief Executive Officer.

Opportunity – an exploitable set of circumstances with uncertain but potentially positive outcomes requiring commitment of resources and involving exposure to risk.

Oversight – Monitoring, assessment and reporting of risk-taking activities.

Principal risks – The most significant or key risks facing an organisation, including those that may threaten the organisation's business model, future performance, solvency or liquidity and reputation. Principal risks may include all types of risk including, inter alia:

- existing and emerging risks, internal and external risks, financial and non-financial risks, in-house and extended enterprise risks;
- categories or types of risk as defined in an organisation's risk universe; and
- risk scenarios in which combinations of risks or risk types may crystallise.

Risk – The possibility that events will occur that affect the likely achievement of an organisation's strategic aim, objectives or other opportunities. Commonly considered as negative events (downside risk), there may be occasions where risks may be exploited to an organisation's advantage (upside risk).

Risk appetite – A board-approved statement describing the aggregate types and extent of risk the board is willing to assume or wishes to avoid to achieve its strategic aims, objectives and other opportunities.

Risk culture – The combination of an organisation's desired ethics, values, behaviours and understanding about risk, both positive and negative, that influences decision-making and risk-taking.

Risk culture expectations – A board-approved statement setting out board expectations relating to key risk culture influences such as board and management tone, accountability, effective communication and challenge, and financial and non-financial incentives.

Risk governance – The activity of providing governance oversight of an organisation's risk management arrangements and risk-taking activities.

Risk governance framework – The framework of governance fora (board, executive and non-executive committees), defined roles and responsibilities, terms of reference, policies, procedures and guidance through which risk governance is exercised.

(Enterprise) risk management framework – An enterprise-wide framework for the robust, consistent and disciplined management of risk with the aim of facilitating the achievement of the organisation's strategic aims, objectives and other opportunities.

Risk policy framework – The framework of risk-focused board-approved policies that define and set the board's risk management expectations of the organisation.

Risk strategy – The organisation's overall approach to risk management, which should support and be consistent with the organisation's strategic aims, objectives and other opportunities, purpose, values and risk culture expectations.

Risk universe – Sometimes described as risk categories or a risk library, a risk universe is a representation of an organisation's key sources or categories of risk.

Scenario analysis – A process for selecting and analysing one or more scenarios to understand how they might positively or negatively impact the organisation, including assessing the effectiveness of possible risk responses.

Strategic aims and objectives – Top-level aims and objectives linked to the achievement of corporate strategy.

Stress testing – A process for selecting and analysing one or more changes to key variables and assumptions underlying a model (or scenario) to understand how the changes might positively or negatively impact the organisation, including assessing the effectiveness of possible risk responses.

3 RISK COALITION TEAM

Chris Burt

Co-founder and Executive Chair, the Risk Coalition

Principal author of the Risk Coalition's 'Raising the Bar' and 'Raising your Game' leading practice risk guidance.

Chris is a CGI accredited board reviewer and Principal at Halex Consulting, a leading boutique governance consultancy specialising in independent board evaluations and risk management advisory services. He is also a co-founder and Executive Chair of the Risk Coalition, a not-for-profit, risk management think tank that aims to improve the effectiveness of risk management practice in the UK and globally.

Chris is the principal author of the Risk Coalition's internationally acclaimed 'Raising the Bar' leading practice guidance for financial sector board risk committees, and the Risk Coalition's soon to be published 'Raising your Game', leading practice cross-sector guidance. He also Chairs the Risk Coalition's Risk Committee Chairs and CROs forums, and Halex Consulting's own CoSec Forum for company secretaries and governance professionals.

Chris speaks regularly on risk and governance-related topics.

Professor Bryan Foss

Co-founder and board member, the Risk Coalition.

Bryan is an experienced board member with an active financial services authorisation and chair role. He mentors board members in listed, public sector, institutional finance backed and other organisations, having held SID, INED and numerous committee chair roles himself. Bryan's prior experience included international executive roles within IBM, managing business and technical relationships with some of the largest FS clients across emerging and mature economies. Bryan also led international export development assessments for the UK government and made early investments in high growth startups.

His qualifications include Chartered Director (IoD), Chartered Engineer (IT), also finance, FS regulation (CISI) and marketing (FCIM). Bryan holds a Visiting Professor role with Bristol Business School, lectures on Henley Business School board programmes and held an eight-year senior advisory role with the Financial Reporting Council alongside his co-founder role with the Risk Coalition.

Peter Neville Lewis

Co-founder and board member, the Risk Coalition

Principal author of the Risk Coalition's 'The Extra G' leading practice geo-political risk guidance and contributing author, project sponsor and working group lead, 'Raising your Game'.

Peter is the founder of Principled Consulting and a co-founder of the Risk Coalition. He is also principal author of the Risk Coalition's, 'The Extra G', leading practice guidance on geo-political risk.

With over 30 years' practical delivery at Managing Director level, Peter specialises in advising boards and senior executive teams on principled leadership, values-based decision making, conduct risk and, more recently, geo-political risk.

Peter's longstanding connections within the City and various political, academic and economic institutions, together with his wide range of cultural interests provide clients with a rich source of intellect, expertise and pragmatism. He is also an Honorary Research Fellow at Brunel University London.

Having trained at RMA Sandhurst, Peter left the Army to work in the City and in the early 70's he established a wholesale business which was successfully sold to a Public Company in 1986. From 1988 up to 2001, Peter held various senior roles and non-executive positions with an emphasis on Sales and Marketing, including setting up a Sales Office in Bangkok for a US Multinational FMCG business covering South East Asia.

Peter's current focus is on providing clients with advice and guidance on culture audits, ethical leadership, business conduct and values-based decision-making.

Hanif Barma

Co-founder and board member, the Risk Coalition

Hanif is an experienced non-executive director and the founding partner of Board Alchemy, a specialist governance consultancy. Board Alchemy undertakes board and committee effectiveness reviews for clients across a range of sectors. We also assess the effectiveness of internal audit and risk teams and we also support clients by helping to develop board and organisational culture. We have an unassuming style, and let our work and relationships speak for themselves.

4 ACKNOWLEDGEMENTS

The Risk Coalition would like to acknowledge the following people who have contributed to the production of this consultation document through working group participation, reviewing draft texts and providing critical feedback. We greatly appreciate their advice, guidance and continued support.

Working group members

James Beasley
Head of Board Advisory EMEA,
NASDAQ

Richard Brasher
Vice President Sustainability, LKQ Corporation

Carolyn Clarke
Founding Partner,
Brave Within LLP
NED, Elcogen
Council, Chartered IIA

Peter Elam
Group Head Risk Management,
Business Assurance,
Anglo American plc
Former President,
Chartered IIA

Julia Graham
Chief Executive, AIRMIC

Gavin Hayes
Head of Policy and Public Affairs,
Chartered Institute of IIA

Patrick Healy
Founder, Merlance Consulting

Melanie Hind
Audit NED, KPMG UK
Chair of Audit Committee,
Talbot Underwriting
INED, OneFamily

Kathryn Kerle
Chair Audit & Risk Committee:
- Planet Smart City
- Newcleo
- Microbiology Association

Michael Lucas
Founding Partner,
Brave Within LLP
Former Head of Risk,
Centrica Consumer

Jeremy Small
Company Secretary,
WE Soda Ltd

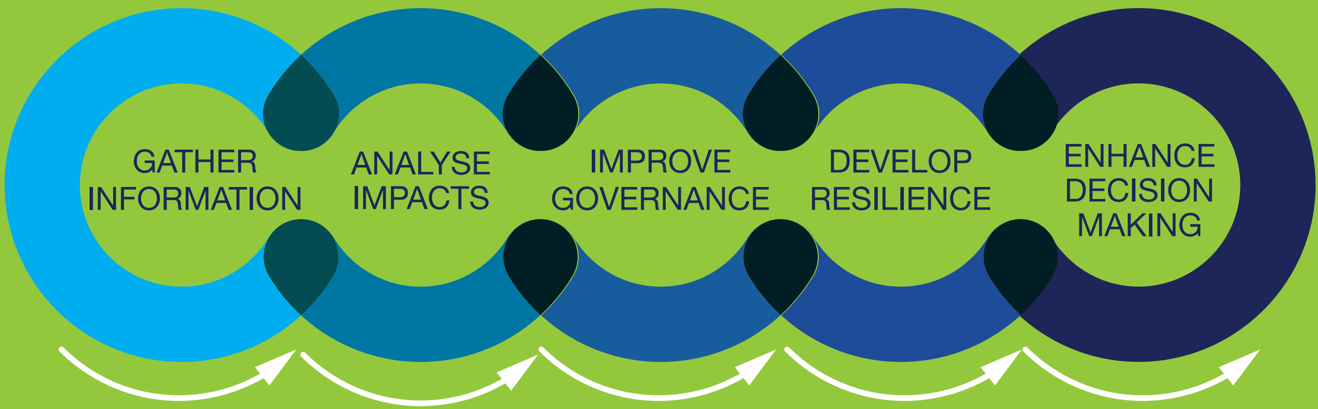
Keith Smith
Chair of BSI Committee RM1/4
Founder, RiskCovered Ltd

Sir James Wates CBE
Chair, Vestey Holdings Ltd
Chair, Institute of Family Business UK
Former Chair, Wates Group
NED, Argent LLP

David Wilson
Global Director,
Risk and Compliance
Carbon Disclosure Project

Raising your Game

THE SMART WAY TO:



The Risk Coalition

Leading Risk Thinking

enquiries@riskcoalition.org.uk

+44 (0)20 3823 6569

riskcoalition.org.uk

86-90 Paul Street
London.
EC2A 4NE