The Risk Coalition

Leading Risk Thinking

Raising the Bar

Principles-based guidance for board risk committees and risk functions in the UK Financial Services sector

THE RISK COALITION RESEARCH COMPANY

THE RISK COALITION

The Risk Coalition would like to thank the following sponsors, supporters and observers who have contributed to the production of this principles-based guidance.

Their support and inputs have been invaluable and are greatly appreciated.

Re-establishing trust, respect and confidence in financial services through greater risk governance and oversight transparency.

"We welcome the Risk Coalition's initiative to raise standards in risk oversight in UK financial services. Their approach and guidance complements the personal accountability we regard as an important regulatory objective. It is important that SMF role holders do not simply adhere to the guidance as a box-ticking exercise, but also reflect on how to ensure adequate regulatory outcomes."

Financial Conduct Authority

RISK COALITION MEMBERS

Chartered Banker
Leading financial professionalism
European Risk Management Council
Chartered Institute of Internal Auditors
ORIC INTERNATIONAL
Chartered Insurance Institute
PRMIA
INSIGHT CONSENSUS INFLUENCE
LLOYDS MARKET ASSOCIATION
airmic
IOD
ACCA
Think Ahead
RESILIENCE FIRST
CELEBRATING 140 YEARS
The London Institute of Banking & Finance
CISI
CHARTERED INSTITUTE FOR SECURITIES & INVESTMENT
CSFI
Centre for the Study of Financial Innovation

SPONSORS AND SUPPORTERS

HERMES
INVESTMENT MANAGEMENT
HOGGETT BOWERS
Institute and Faculty of Actuaries
NEDonBoard
euroclear
Permuto Consulting
winmark
NORMAN BROADBENT
Crowe
NEDA
NON-EXECUTIVE DIRECTORS' ASSOCIATION
Developing Trusted Professionals

OBSERVERS

FRC
Financial Reporting Council
LSB
Lending Standards Board
BANKING STANDARDS BOARD
irm
Leading the risk profession
THE INSTITUTE OF OPERATIONAL RISK

CONTENTS

The Risk Coalition
Leading Risk Thinking

FOREWORD

In financial services the real risk is to take no risks. We are in the business of managing financial risks. Yet for some time we have failed to manage these well. If we dealt well with threats, although we would have low-level failures, systemic impacts would be low. If we dealt well with opportunities, we would have far better reputations with our clients.

It is surprising indeed that, until the publication of *Raising the Bar*, there has been no comprehensive, principles-based guidance for financial services risk committees and risk functions. I therefore welcome and support this initiative.

The separate guidance of 'eight principles' for board risk committees and 'nine principles' for risk functions is helpful. The emphasis on first line responsibility and accountability for risk management is overdue. Hopefully, the Three Lines of Defence model benefits from extra clarity.

Though many of the principles and guidance are well-established, *Raising the Bar* attempts to provide a single, slim authoritative document, some of whose recommendations are challenging. The guidance emphasises the importance and seniority of a Chief Risk Officer (CRO) or equivalent, as well as their independence. Risk committees and CROs can and should aggregate and communicate risk information from across a business and its environment to the board. There should be one holistic view for the Board.

In so much as this guidance encourages organisations to think more deeply about risk, it has to be a good thing. Larger organisations find constant rethinking tough, often substituting 'scale of effort' for proof of professionalism. Smaller organisations fear bureaucratic sclerosis, but can and should apply proportionality to the guidance's recommendations.

So, if the opposite of danger is not taking risks, it's time to take the opportunity that *Raising the Bar* provides for financial services organisations to engage, internally and externally, in forward looking dialogue on risk governance.

Professor Michael Mainelli FCCA Chartered FCSI(Hon) FBCS
Alderman & Sheriff of the City of London
Executive Chairman, Z/Yen Group

1. Why Raising the Bar? The need for principles-based guidance

The Risk Coalition has written this guidance to meet the need for coherent, principles-based good practice guidance for board risk committees and risk functions within the UK financial services sector. In essence, this guidance provides a commonly agreed benchmark for 'what good looks like' – something that has not been available previously.

The Risk Coalition expects this guidance to lead to substantive improvements in the overall quality and effectiveness of risk management across the UK financial services sector. Consequently, we encourage organisations to consider early adoption – not as a matter of compliance, but as a matter of good business practice in line with Principle A of the UK Corporate Governance Code. In turn, this should help organisations better exploit the array of new opportunities presented by technological, environmental, socio-political and economic changes happening in the world around us.

The existence of a commonly agreed risk governance and oversight benchmark should also prove invaluable for SMF role-holders, investors, ratings agencies, s166 Skilled Persons firms, organisations performing due diligence, regulators and other stakeholders alike.

This guidance has been developed through industry, academic and regulatory consultation, and is intended to be evolutionary rather than revolutionary in nature. Elements of the guidance – such as its strong focus on accountability – may prove challenging or even contentious initially for some organisations.

The Risk Coalition believes, however, that these elements are consistent with the current regulatory 'direction of travel' as evidenced by the Senior Managers and Certification Regime.

Organisations should apply this guidance intelligently and proportionately, taking all reasonable steps to achieve the appropriate outcomes. Professional judgement should be used in deciding if and how each principle applies and over what period it should be implemented.

Where an organisation feels that an element of the guidance is not appropriate to its circumstances, the board risk committee, working in conjunction with the chief risk officer, should apply the guidance in a way that achieves appropriate outcomes.

While this guidance aims to provide a benchmark for 'what good looks like', it is key that organisations continually challenge whether application of the guidance alone is sufficient to achieve the appropriate outcomes. The Risk Coalition strongly encourages organisations to continually innovate and improve their practices, going beyond the minimum necessary wherever appropriate.

This guidance is intended to be used by organisations on an 'apply or explain' basis. The Risk Coalition encourages firms to publicly disclose the extent of their application of the guidance, including details of any implementation period where relevant.

Guidance overview

Part A of the guidance focuses on what can reasonably be expected of a mature board risk committee[1] through defining a number of key principles and supporting guidance.

Part B of the guidance follows a similar format, but focuses on the role and responsibilities of the CRO and second line risk function[2].

Each part of this guidance is intended to be standalone, although consistent with the other. Consequently, there are occasions where content may be duplicated between the parts to ensure appropriate guidance is provided to their specific audiences.

This guidance is not intended to be prescriptive but provides users with good practice principles supplemented with practical guidance on their implementation. The guidance does not reference specific types of risk as these will be different for every organisation, preferring instead to focus on good practice principles that will stand the test of time.

This guidance assumes – but does not require – that organisations operate a Three Lines of Defence model in line with current regulatory expectations and market practice[3].

While the concept of the Three Lines of Defence continues to provoke much academic and professional debate, the Risk Coalition believes the basic principle of requiring independent oversight and challenge of management risk-taking remains sound. How the principle is applied, however, may change as a result of technological or other changes in the business environment.

"Nothing like this currently exists in Europe"

Martin Stewart

Former Director,
Prudential Regulation Authority

[1] Where no dedicated board risk committee exists, the board should consider how best to apply this guidance. For example, by the board itself or through delegation to the audit/audit & risk committee.

[2] This guidance does not seek to provide advice for other second line functions, such as the compliance function.

[3] See Appendix 1 – The Three Lines of Defence for an overview of how this model should operate.

2. PART A: BOARD RISK COMMITTEE PRINCIPLES AND GUIDANCE

EIGHT BOARD RISK COMMITTEE PRINCIPLES

Principle A1

Board accountability

The board risk committee is primarily an advisory committee to the board. Its aim is to facilitate focused and informed board discussions on risk-related matters. The board retains ultimate accountability for the organisation's principal risks and for the overall effectiveness of its risk management arrangements.

Principle A2

Composition and membership

The board risk committee should be formed of independent non-executive directors and apply UK Corporate Governance Code guidance on chair, composition, succession and evaluation criteria.

Principle A3

Risk strategy and risk appetite

The board risk committee should provide the board with advice on the continued appropriateness of the board-set risk strategy and risk appetite in light of the organisation's stated purpose, values, risk culture expectations, corporate strategy and strategic objectives.

Principle A4

Principal risks and continued viability

The board risk committee should assess and advise the board on the organisation's principal and emerging risks and how these may affect the likely achievement of the organisation's strategic objectives and continued viability of its business model.

Principle A5

Risk management and internal control systems

The board risk committee should monitor and periodically advise the board on the overall effectiveness of the organisation's risk management and internal control systems.

Principle A6

Risk information and reporting

The board risk committee should assess and advise the board on the quality and appropriateness of the organisation's risk information and reporting.

Principle A7

Risk culture and remuneration

The board risk committee should consider and periodically report to the board as to whether the organisation's purpose, values and board-approved risk culture expectations are appropriately embedded in the organisation's risk strategy and risk appetite, and are reflected in observed behaviours and decisions.

Principle A8

Chief risk officer and risk function independence and objectivity

The board risk committee should safeguard the independence and objectivity, and oversee the performance, of the chief risk officer and the second line risk function.

EIGHT BOARD RISK COMMITTEE PRINCIPLES

Principle A1

Board accountability

The board risk committee is primarily an advisory committee[4] to the board. Its aim is to facilitate focused and informed board discussions on risk-related matters. The board retains ultimate accountability for the organisation's principal risks[5] and for the overall effectiveness of its risk management arrangements.

In meeting this principle, the board risk committee should:

1. Provide consolidated oversight and challenge of management's treatment and reporting of the organisation's principal and emerging risks, including those risks within the remit of other board committees.
2. Seek regular board engagement and direction on the organisation's principal and emerging risks and other key board risk committee topics. This should include escalation of contentious or strategically significant agenda items to the board for further consideration, even if within the committee's official remit.
3. Confirm that delegated risk-related responsibilities are clearly defined between board committees and that appropriate arrangements are in place to support effective co-operation, co-ordination and communication between committees when dealing with matters of common interest.
4. Where relevant, consider the benefits of, and support the committee chair in, engaging with investors and other key stakeholders on risk-related topics.
5. Where applicable, and within relevant legal and regulatory constraints, provide an appropriate mechanism for board risk committees (or committee chairs) within a group of companies to exchange relevant risk information and views on a regular basis.
6. Provide the board with a clear and concise summary of the committee's activities and matters considered, and any associated recommendations.

> *"In my view the Risk Coalition's Raising the Bar is readable, sensible, helpful, understandable and appealing.*
> *I think therefore it may have a very significant impact.*
> *It invites the reader in, doesn't over-complicate and offers something that is genuinely useful.*
>
> *This is what people, boards, organisations want.*
>
> *I consult the OECD's 22 principles for independent fiscal organisations in some of my work and find that material invaluable.*
>
> *Similarly I see great value in this new guidance focusing on risk in financial services organisations."*
>
> Dame Susan Rice DBE.
> Chair, Scottish Fiscal Commission. Chair, Banking Standards Board. Former Member of Court, Bank of England

[4] While the board risk 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 board risk committee's terms of reference.

[5] See Appendix 2 – Definition of terms for the definition of principal risks and other key terms used throughout this document.

Principle A2

Composition and membership

The board risk committee should be formed of independent non-executive directors and apply UK Corporate Governance Code guidance on chair, composition, succession and evaluation criteria.

In meeting this principle, the board risk committee should:

7. Have board-approved terms of reference which set out its responsibilities and duties clearly, guarding its non-executive status and ensuring it does not act in the capacity of an executive risk committee.
8. Periodically consider whether its planned annual cycle of activity remains appropriate to the organisation's needs, including providing sufficient time for ad hoc or deep-dive exploration of key and emerging risk-related topics and themes.
9. Where practical, ensure that board risk committee meetings are scheduled such that the committee is able to provide appropriate follow-up, resolution (including escalation if necessary) and reporting to the board on outstanding issues.
10. Ensure it has an appropriate balance of skills, diversity and relevant expertise to fulfil its remit effectively, accessing external expert risk advice and guidance as necessary.
11. Oversee a tailored continuing professional education programme for board risk committee members, and provide an environment that encourages diversity of thought and opinion when performing its work.
12. Provide a standing invitation to relevant board members and executives. The chief internal auditor and other heads of internal control functions, as well as the external auditor, should be invited to attend as necessary or appropriate.

Principle A3

Risk strategy and risk appetite

The board risk committee should provide the board with advice on the continued appropriateness of the board-set risk strategy and risk appetite in light of the organisation's stated purpose, values, risk culture expectations, corporate strategy and strategic objectives.

In meeting this principle, the board risk committee should:

13. Evaluate and advise the board as to whether the organisation's board-set risk strategy and risk appetite:
    - clearly define the organisation's overall approach to managing risks;
    - align and are consistent with the organisation's business model – including its stated purpose, values, risk culture expectations, corporate strategy and strategic objectives;
    - describe the aggregate types and extent of risk the organisation is willing to assume (or wishes to avoid) in both normal and stressed conditions in order to achieve its strategic objectives;
    - translate into a robust, board-approved risk appetite framework embedded throughout the business and designed to aid effective management decision-making, risk monitoring and reporting; and
    - help the board and executive management understand, analyse and make appropriate prioritisation decisions between competing strategic aims.
14. Periodically review and recommend for board consideration and approval, proposed material changes to the organisation's risk management framework consistent with the board-approved risk strategy and risk appetite. This should include proposed changes to risk governance, risk appetite and risk policy frameworks, and the organisation's risk universe.
15. Consider whether there is appropriate alignment between the organisation's overall product and service offering (including pricing and profitability), and the organisation's risk strategy and risk appetite.
16. Notify the board promptly of actual or likely material breaches of risk appetite and comment on the adequacy of management's response, including recommending further actions where appropriate.

> *"We believe that this guidance provides a useful framework for companies to improve their risk management approach. Companies that our membership base seeks to invest in will be strengthened by an increased focus on some of the principles described in the draft guidance."*
>
> The Investment Association

Principle A4

Principal risks and continued viability

The board risk committee should assess and advise the board on the organisation's principal and emerging risks and how these may affect the likely achievement of the organisation's strategic objectives and continued viability of its business model.

In meeting this principle, the board risk committee should:

17. Challenge whether executive management has a sound understanding of the organisation's principal and emerging risks (including emerging categories of risk), as well as the factors that drive and connect them and how they may change in the short and medium-term. The board risk committee should also consider and advise the board on the effectiveness of executive management's proposed or actual risk responses.
18. Contribute to, and periodically assess the effectiveness of, the organisation's emerging risk identification and horizon scanning processes, including its processes for reviewing, updating and approving changes to the organisation's risk universe. Challenge whether the organisation is sufficiently agile to mitigate risks and exploit opportunities presented by changes to the business environment.
19. Challenge whether executive management has assessed effectively the risks as well as the potential benefits associated with proposed material corporate actions, such as:
    - large acquisitions and disposals;
    - major change programmes; and
    - significant changes to governance arrangements or legal structure.
20. Consider whether contractual arrangements with key intra-group or outsourced service providers adequately incentivise appropriate third-party risk management behaviours, and support effective board risk committee and risk function governance and oversight.
21. Periodically assess and challenge executive management on the adequacy of operational resilience and business continuity arrangements over the provision of critical or high-profile, in-house, intra-group and outsourced services.
22. Understand, challenge and report to the board on the range of scenarios and reasonableness of key assumptions – such as the effectiveness of proposed or actual risk responses in both normal and stressed conditions – underlying management's:
    - capital, liquidity and solvency modelling;
    - business continuity, recovery, resolution and orderly wind-down planning; and
    - viability assessment.

    Review and, where appropriate, recommend for board consideration and/or approval the interim and final output of such activities.
23. Assess and advise the board on the continued viability of the organisation's business model, including the organisation's likely achievement of strategic objectives, based on an assessment of:
    - its principal and emerging risks;
    - the results of capital, liquidity and solvency modelling;
    - any actual or likely breaches of risk appetite; and
    - the organisation's overall risk profile and risk capacity.

> *"Firms need to provide more information on strategic risks to help improve public trust. Users want better understanding of emerging issues that might adversely affect a company's sustainability."*
>
> Paul George
> Executive Director, Corporate Governance & Reporting, Financial Reporting Council

Principle A5

Risk management and internal control systems

The board risk committee should monitor and periodically advise the board as to the overall effectiveness of the organisation's risk management and internal control systems.

In meeting this principle, the board risk committee should:

24. Agree the framework by which the board risk committee will monitor and periodically assess the overall effectiveness of the organisation's risk management and internal control systems.
25. Consider whether individual and collective risk and control accountabilities within the organisation[6] are clearly and adequately documented, communicated and embedded within the organisation's performance management system.
26. Challenge executive management to demonstrate that:
    - the organisation's risk appetite framework is appropriately embedded within management decision-making processes; and
    - its processes for monitoring and assessing the adequacy and effectiveness of the organisation's risk management and internal control systems are timely, robust and reliable, and that their effectiveness can be maintained in periods of stress or significant change.
27. Seek appropriate assurance on the completeness, accuracy and fairness of first line management's reporting of the organisation's:
    - principal and emerging risks (including emerging categories of risk) and their impact on the likely achievement of the organisation's strategic objectives in both the short and medium-term;
    - proposed or actual risk responses; and
    - significant incidents and near-misses, actual or likely breaches of risk appetite, overall risk profile and risk capacity.
28. In conjunction with the audit committee (as appropriate), review and advise the board of the results of independent assessments of the adequacy and effectiveness of the organisation's risk management and internal control systems, including the adequacy and the effectiveness of its risk and compliance functions[7].

> *"Recent corporate failures have highlighted the need to secure an improvement in both the reporting and assurance of going concern, viability and internal controls over financial reporting."*
>
> Dr Nigel Sleigh-Johnson
> Head of Financial Reporting and Audit Assurance, ICAEW

[6] For example, as required under the UK Senior Managers and Certification Regime.

[7] The internal audit function may provide these independent assessments. As a matter of prudence, the board risk committee should consider seeking an independent external evaluation of risk function effectiveness every three to five years as appropriate.

Risk information and reporting

Principle A6

Risk information and reporting

The board risk committee should assess and advise the board on the quality and appropriateness of the organisation's risk information and reporting.

In meeting this principle, the board risk committee should:

29. Assess the quality and appropriateness of board-level risk information and reporting from each of the lines of defence, including whether significant matters are escalated sufficiently promptly and the overall quality of supporting narrative and analysis.
30. Challenge whether first and second line board-level risk information and reporting adequately leverage risk data aggregation and analysis techniques to identify latent patterns of risk and predict emerging risk trends and themes.
31. Consider whether board-level risk information and reporting is both comprehensive and comprehensible, enabling non-executive directors to understand, probe and challenge executive management effectively.
32. Seek appropriate assurance on the quality and reliability of the organisation's risk information governance and reporting arrangements, including the adequacy and appropriateness of executive management procedures for deciding what risk-related information to present to the board and its committees.
33. Confirm that risk information reporting between group entities (where relevant) and with regulatory authorities is complete, accurate and timely.
34. Review and recommend to the board for approval any material risk information for regulatory submission or external publication.

"

We welcome the initiative and particularly support your emphasis on improving standards of accountability of the Board and its committees on risk. This guidance is consistent with the aims of the UK Corporate Governance Code."

Financial Reporting Council

Principle A7

Risk culture and remuneration

The board risk committee should consider and periodically report to the board as to whether the organisation's purpose, values and board-approved risk culture expectations are appropriately embedded in the organisation's risk strategy and risk appetite, and are reflected in observed behaviours and decisions.

In meeting this principle, the board risk committee should:

35. Assess whether the organisation's purpose, values and board-approved statement of risk culture expectations have been clearly defined and communicated throughout the organisation, and that they are properly understood by executive management. In addition, challenge whether they are reflected appropriately in the organisation's corporate strategy, strategic objectives, risk strategy and risk appetite.
36. Assess and report to the board whether the board's stated risk culture expectations have been translated appropriately into a framework of ethics, values and desired behaviours, supported with appropriate metrics and indicators, and embedded effectively throughout the organisation.
37. In conjunction with the remuneration committee:
    - consider and advise the board whether proposed incentive and remuneration plans are consistent with the board's stated risk culture expectations and whether they are likely to encourage well-controlled and transparent management risk-taking; and
    - monitor and report to the board on how incentive and remuneration arrangements appear to affect observed behaviours, decisions and influences on risk culture, and any consequent impact on the organisation's principal and emerging risks.
38. Provide a view to the remuneration committee on the overall reasonableness and likely impact on the organisation's risk profile of proposed risk-adjusted rewards for executive management and other material risk-takers.
39. In conjunction with the audit committee (as appropriate), advise the board whether the organisation's risk culture expectations and associated whistle-blowing (speak up) arrangements provide those working for and with the organisation with the appropriate support to 'do the right thing' in difficult or challenging circumstances.
40. Review and report to the board on the results of ongoing risk culture monitoring activities performed by each of the Three Lines of Defence.
41. Consider whether executive management's attitude towards and treatment of the chief risk officer, and their approach to internal control function and external audit recommendations, is supportive of a healthy risk culture.

> *"At all its meetings, the board risk committee should seek assurance of appropriate values and behaviours across the organisation and, more importantly, experience first-hand the cultures and environments in operational activities by 'walking the floor'."*
>
> Fraser White
> Chair, Insurance Internal Audit Group

Principle A8

Chief risk officer and risk function independence and objectivity

The board risk committee should safeguard the independence and objectivity, and oversee the performance, of the chief risk officer and the second line risk function.

In meeting this principle, the board risk committee should:

42. Periodically review and approve the risk function's charter, including the independence, objectivity, scope, role, responsibilities and accountabilities of the chief risk officer and the risk function.
43. Ensure that the chief risk officer has a reporting line to the board risk committee chair and an executive reporting line to the chief executive officer, and that appropriate mechanisms are in place to protect the chief risk officer's independence and objectivity.
44. Ensure the chief risk officer has unmediated access to the board chair, the board itself, the board risk committee, the external auditor and the regulatory authorities as necessary.
45. Assess whether the chief risk officer is sufficiently senior and of an appropriate mindset, standing and gravitas to challenge executive management risk-taking effectively, and that the risk function has adequate, appropriate resources (financial, people, processes and technology) to meet its charter obligations.
46. Periodically challenge and assess the continued independence and objectivity of the chief risk officer and risk function. Particular consideration should be given to the continued independence and objectivity of the chief risk officer where they have been in post for a significant period.
47. Consider whether effective arrangements are in place, particularly in a group context, to mitigate any potential conflicts of interest that might undermine the actual or perceived independence and objectivity of the chief risk officer and risk function.
48. Periodically review and approve as appropriate the principal plans and activities of the risk function, and provide the chief risk officer with appropriate direction and guidance on areas of board risk committee interest, including encouraging risk function innovation and enhancement of the organisation's risk strategy and supporting risk management framework.
49. Meet periodically with the chief risk officer in the absence of other executives to provide an opportunity for an open and non-attributable discussion of the chief risk officer's key concerns and to provide a channel of open communication between the chief risk officer and board risk committee.
50. In consultation with the chief executive officer:
    - advise the board on the appointment or removal of the chief risk officer; and
    - consider and approve the chief risk officer's annual objectives and performance, and make recommendations to the remuneration committee on the chief risk officer's remuneration (form and quantum).

> *"Perhaps we will see a shift – the 'Chief Risk Officer' becoming 'Chief Responsibility Officer' as the role matures away from managing downside risk and regulatory expectations towards supporting the boardroom in building a sustainable business model."*
>
> Alex Hindson
> Argo Group International Holdings

3. PART B – RISK FUNCTION PRINCIPLES AND GUIDANCE

NINE RISK FUNCTION PRINCIPLES

Principle B1

Independent risk oversight and challenge

The chief risk officer, supported by the risk function, is responsible for ensuring robust, independent oversight and challenge of risk-taking activities across the organisation.

Principle B2

Independent and objective perspective

The chief risk officer and members of the risk function should maintain an independent and objective perspective.

Principle B3

Risk governance

The chief risk officer should be of appropriate standing to provide effective challenge at both executive and board level.

Principle B4

Risk reporting

The chief risk officer should provide the board risk committee with appropriate assurance that executive management's reporting of risks is both complete and fairly stated.

Principle B5

Corporate strategy and objectives

The chief risk officer should ensure appropriate consideration of risk during corporate strategy, strategic objective setting and business planning discussions.

Principle B6

Risk function independence and effectiveness

The chief risk officer should ensure the independence and effectiveness of the risk function.

Principle B7

Risk culture

The risk function should monitor, assess and periodically report to executive management and the board risk committee on the organisation's risk culture.

Principle B8

Innovation and change

The risk function should support the organisation in identifying and adapting effectively to material changes or developments in the internal or external environment.

Principle B9

Group risk functions

The group chief risk officer should ensure that risk management arrangements operating across the group are appropriate and effective.

> *"This guidance has been long awaited by third line functions as it has historically been very difficult to benchmark the effectiveness of the second line function."*
>
> Fortune Chigwende
> Hermes Investment Management

NINE RISK FUNCTION PRINCIPLES

Principle B1

Independent risk oversight and challenge

The chief risk officer, supported by the risk function, is responsible for ensuring robust, independent oversight and challenge of risk-taking activities across the organisation.

51. First line management owns, and is responsible for taking and managing, the organisation's risks within risk appetite. The second line, consisting of the risk and compliance functions amongst others, is responsible for providing independent oversight and challenge of first line management risk-taking.
52. In performing their role, the chief risk officer and members of the risk function should provide first line management with advice, challenge and opinion, but should not make, approve or authorise operational or other management decisions[8].
53. In providing an opinion, the chief risk officer and members of the risk function should challenge whether first line management has adequately considered all pertinent risks, how they may positively or negatively impact the organisation, and whether appropriate risk responses have been adopted to keep within risk appetite.
54. Where the chief risk officer or members of the risk function are expected to make, approve or authorise first line management decisions as part of their role, the implications on the effectiveness of second line oversight and challenge should be assessed and shared with the board risk committee for its consideration and approval.
55. Periodically, the chief risk officer should assess whether the:
    - allocation of second line risk oversight responsibilities between the risk function and other second line functions is sufficiently clear; and
    - quality of risk oversight and challenge provided by second line functions is appropriately robust and reliable.

    Where the chief risk officer considers that second line oversight responsibilities are not sufficiently clear, or that oversight and challenge are inadequate, the chief risk officer should assess its implications and make recommendations to the board risk committee as appropriate.
56. The heads of other second line functions, such as the chief compliance officer or head of independent model validation, may report to the chief risk officer provided that appropriate conflicts of interest safeguards are put in place. The chief internal auditor must not report to the chief risk officer.

"I am supportive of everything in the guidance and believe it is essential that second line functions are in a position to provide comprehensive, holistic assurance to the board and that they have a direct reporting relationship to the board and/or its committees."

Peter Bowen
Pension Protection Fund

[8] For example, authorising lines of credit.

Principle B2

Independent and objective perspective

The chief risk officer and members of the risk function should maintain an independent and objective perspective.

57. The chief risk officer and members of the risk function should maintain an independent and objective perspective to support effective oversight and challenge of first line management risk-taking activities. This may require the risk function to independently produce or model relevant information to form an independent and objective view.
58. The chief risk officer should have a reporting line to the board risk committee chair and an executive reporting line to the chief executive officer. The chief risk officer should have unmediated access to the board chair, the board itself, the board risk committee, the external auditor and the regulatory authorities as necessary.
59. The chief risk officer should be open, transparent and empowered to speak on the organisation's behalf in all dealings with key internal and external stakeholders, such as the external auditor and regulatory authorities.
60. Appropriate organisational arrangements should be put in place, particularly in a group context, to mitigate any potential conflicts of interest that might undermine the actual or perceived independence and objectivity of the chief risk officer and risk function[9].

Principle B3

Risk governance

The chief risk officer should be of appropriate standing to provide effective challenge at both executive and board level.

61. The chief risk officer should receive a standing invitation to both the board risk committee and audit committee, and may receive a standing invitation to the board.
62. The chief risk officer should be a member of the executive committee and may be a member of the board. The chief risk officer's role is to provide independent advice, challenge and opinion while participating fully in executive committee/board discussions and collective decision-making processes.
63. Where one exists, the chief risk officer should be a member of the executive risk committee. Wherever practical, the executive risk committee should be chaired by a member of executive management rather than the chief risk officer to encourage management accountability and preserve the delineation of first and second line responsibilities.
64. Where the board risk committee, executive committee or executive risk committee makes a decision with which the chief risk officer disagrees or otherwise has concerns, the chief risk officer's objection or challenge should be fully minuted. The chief risk officer may make their views known – formally or informally – to the board risk committee chair and/or the board chair.

[9] For example, where a subsidiary entity chief risk officer has an additional reporting line to the group chief risk officer.

Principle B4

Risk reporting

The chief risk officer should provide the board risk committee with appropriate assurance that executive management's reporting of risks is both complete and fairly stated.

65. The chief risk officer should provide the board risk committee with a regular report that summarises the chief risk officer's key concerns and matters for the committee's attention, including their independent view of:
    - the organisation's principal and emerging risks (including emerging categories of risk) and their impact on the likely achievement of the organisation's strategic objectives in both the short and medium-term;
    - the appropriateness of management's proposed or actual risk responses, with recommendations for improvement where necessary;
    - any significant incidents and near-misses, actual or likely breaches of risk appetite, overall risk profile and risk capacity; and
    - any other matter that the chief risk officer feels is pertinent or necessary to facilitate full and effective board risk committee discussions.
66. Reports from the chief risk officer to the board risk committee should seek to present information in a way that is accessible to non-executive directors and enables them to understand, probe and challenge executive management effectively.
67. Where necessary, the chief risk officer should provide risk reporting to the audit committee appropriate to its needs.

Principle B5

Corporate strategy and objectives

The chief risk officer should ensure appropriate consideration of risk during corporate strategy, strategic objective setting and business planning discussions.

68. The chief risk officer should participate in executive and board-level corporate strategy, strategic objective setting and business planning discussions to ensure appropriate consideration of proposed changes to:
    - risk strategy, risk appetite, risk capacity and risk profile (including the risk universe);
    - the organisation's defined purpose, values and risk culture expectations; and
    - the way in which risk is addressed in corporate strategy implementation.
69. The chief risk officer should ensure they are aware of, and may participate in, executive and board-level discussions relating to material corporate actions and major change programmes, including significant changes to governance arrangements, legal structure or business model.

> *"This guidance is well thought out and will enable a review and evaluation of our current risk arrangements."*
>
> Justin Skinner
> Vitality

Principle B6

Risk function independence and effectiveness

The chief risk officer should ensure the independence and effectiveness of the risk function.

Risk function role and remit

70. The chief risk officer should develop and seek board risk committee approval of an appropriate risk function charter detailing the independence, objectivity, scope, role, responsibilities and accountabilities of the chief risk officer and the risk function, including the requirement for the chief risk officer and risk function to remain free of first line operational responsibilities.
71. The scope of the risk function should be unrestricted and should include consideration of any aspect of the organisation's governance, management or internal control arrangements – including free and unrestricted access to any internal or relevant third-party information, people or locations – that the chief risk officer considers pertinent to fulfilling the risk function's charter responsibilities.
72. The risk function should have a procedures guide which elaborates on the risk function charter and provides detailed guidance to members of the risk function on how they should plan, perform and report their work, including establishing appropriate quality assurance and training processes.

Risk function resourcing and expertise

73. The risk function should be adequately resourced to meet its charter obligations and the reasonable expectations of key stakeholders, including executive management, the board risk committee and the organisation's regulatory authorities. This may require access to external resources where necessary and includes access to modelling capabilities as well as technology resources such as risk data mining, aggregation and analytics capabilities.
74. Diversity of risk function staff background, experience and perspectives should be encouraged. This should be underpinned by appropriate risk management qualifications and expertise, and a sound understanding of the organisation and the context in which it operates. Risk function members should have access to, and be encouraged to participate in, relevant continuing professional education and development opportunities.
75. Members of the risk function should express their professional opinions and provide constructive challenge when observing, attending or participating in first line management (including project management) meetings, discussions and events.
76. Subject to appropriate independence safeguards, the risk function may provide expert modelling advice and support to the organisation – such as developing stresses and scenarios and advising on modelling methodologies – where necessary for both practical and efficiency purposes.
77. Where a risk function provides modelling advice and support to the organisation, appropriate arrangements should be implemented to ensure first line management is properly engaged and retains model ownership, including responsibility for key decisions such as model assumptions and scenarios, and presenting interim and final output to the board as appropriate.
78. The chief risk officer should ensure that appropriate quality assurance arrangements are implemented within the risk function. Where risk function work is co-sourced or outsourced to an external provider, the chief risk officer remains responsible for the overall quality and reliability of the work performed.

Principle B6

Risk function independence and effectiveness (continued)

The chief risk officer should ensure the independence and effectiveness of the risk function.

Risk intelligence and planning

79. The risk function should develop and implement processes to collect and analyse formal and informal risk intelligence from across the organisation, including the results of risk monitoring activities. This should include regular, structured engagement with key internal and external stakeholders as appropriate.
80. The risk function should develop a plan, based on its risk intelligence and other sources of information, to outline the independent risk assessments and risk monitoring activities it intends to undertake over the course of the following year (or other appropriate period).
81. The risk function plan should cover all sources and types of risk. It should be revised and updated in the course of the year as necessary and shared with internal audit and executive management for comment. The risk function plan, and any significant changes to it, should be submitted to the board risk committee for review and periodic approval.
82. The risk function should share details and co-ordinate planned work with other internal control functions, including the compliance and internal audit functions, to maximise the value and efficiency of second and third line assurance work. Additionally, the risk function should routinely share the results of its work, both formal and informal, with the internal audit function to facilitate their work. The chief risk officer should maintain an open and constructive relationship with the chief internal auditor and heads of other internal control functions.

Independent risk assessments and risk monitoring

83. When carrying out independent risk assessments and risk monitoring activities (including stakeholder management), members of the risk function should document details of their work sufficient to support their opinions. Relevant supporting evidence, such as meeting minutes and key documentation, should be retained in line with the organisation's document retention policy.
84. Results of independent risk assessments and risk monitoring activities, along with any associated opinions, recommendations and agreed first line management actions, should be provided to executive management. Summary results, opinions, recommendations and agreed first line management actions should be reported to the board risk committee as appropriate.
85. The risk function should routinely track and report progress against agreed first line management actions to executive management and the board risk committee.

Principle B6

Risk function independence and effectiveness (continued)

The chief risk officer should ensure the independence and effectiveness of the risk function.

Risk management framework

86. The risk function is responsible for designing, facilitating the implementation and monitoring the efficient operation of the organisation's risk management framework. Working in close collaboration with executive management and the board risk committee, the risk function should:
    - facilitate the development of a risk strategy and associated risk appetite, for both normal and stressed conditions, for consideration and approval by the board. The risk strategy and risk appetite should be consistent with the organisation's overall business model, including its purpose, values, risk culture expectations, corporate strategy and strategic objectives;
    - design and document a risk management framework consistent with the organisation's risk strategy and risk appetite and appropriate for its needs. The risk management framework should be reviewed and approved by the board and include development of any risk policies, procedures or guidance (including tools, technology and training materials) necessary to support effective risk governance and first line management's implementation and effective operation of the risk management framework; and
    - support first line management in developing, implementing, calibrating and embedding a robust, board-approved risk appetite framework and associated risk reporting.
87. The risk function should select and independently monitor a portfolio of risk appetite framework metrics and indicators to support its monitoring of the organisation's risk profile.
88. The risk function should routinely monitor the effective operation (in terms of people, processes and outcomes) of the organisation's risk management framework and make improvements where necessary.
89. Annually, the chief risk officer should provide the board risk committee with a formal analysis of the effectiveness of the organisation's – and where relevant, the group's – risk management framework, including a self-assessment of risk function effectiveness.

Principle B7

Risk culture

The risk function should monitor, assess and periodically report to executive management and the board risk committee on the organisation's risk culture.

90. The risk function should introduce processes to enable it to monitor and assess the organisation's risk culture from a range of perspectives, including across business lines, entities and geographies.

91. In performing independent risk assessments and risk monitoring activities, and providing opinions to first line management, members of the risk function should be mindful of, and where appropriate document and report, behaviours or influences on risk culture – such as board and management tone, accountability, effective communication and challenge, and (financial and non-financial) incentives – that may impact the organisation's risk profile.

92. At least annually, the risk function should provide executive management and the board risk committee with a thematic analysis of the organisation's risk culture based on the consolidated results of its risk culture monitoring and make recommendations for improvement. Where appropriate, the results of the risk function's thematic analysis may be combined with the results of risk culture monitoring performed by the first and third lines.

Principle B8

Innovation and change

The risk function should support the organisation in identifying and adapting effectively to material changes or developments in the internal or external environment.

93. The risk function should develop and facilitate the operation of an enterprise- wide risk identification and horizon scanning process, including the use of scenario planning techniques, that encourages and incorporates contributions from each of the lines of defence, executive management and the board risk committee.
94. The chief risk officer should challenge first line and executive management to analyse and assess the potential opportunities, as well as the threats, arising from the enterprise-wide risk identification and horizon scanning process. This should include how threats and opportunities might influence the organisation's business model, including its corporate and risk strategies, risk appetite, strategic objectives and sources of risk (risk universe).
95. The risk function should implement processes to support its early identification, analysis and response to proposed or actual material changes to the organisation, including consideration of how these changes might impact the risk function's operating model and its interaction with the other lines of defence.
96. The risk function should seek to enhance the efficiency and effectiveness of the organisation's risk management framework through continuous innovation and improvement, including leveraging developments in technology and risk management thinking and practice.

Principle B9

Group risk functions

The group chief risk officer should ensure that risk management arrangements operating across the group are appropriate and effective.

97. The group chief risk officer should ensure appropriate mechanisms are in place to facilitate the open, timely and transparent exchange of relevant information and views between the organisation's chief risk officers. Additionally, the group chief risk officer should work with subsidiary entity chief risk officers to ensure appropriate and effective intra-group risk escalation mechanisms are in place.
98. The group chief risk officer should monitor and regularly assess the adequacy and effectiveness of second line risk oversight arrangements within the entities for which they have consolidated risk oversight responsibility. Where the group chief risk officer has concerns over such arrangements, they should seek to raise the matter with the subsidiary entity in the first instance. The group chief risk officer may also raise the matter with the group executive committee and/or group board risk committee if their concerns are sufficiently material to the group's risk profile or reputation.
99. The group chief risk officer should assess whether adequate processes are in place across the group to facilitate the effective risk aggregation, analysis, monitoring and reporting of consolidated risks at the group level. The group chief risk officer should also assess whether adequate processes are in place to share relevant group-level risk information with subsidiary entities as appropriate.

4. APPENDIX 1
THE THREE LINES OF DEFENCE

This guidance assumes – but does not require – that organisations operate a Three Lines of Defence model. Under this model:

- **First line management is responsible for risk-taking. Management therefore owns the organisation's risks and is responsible for managing them in line with the organisation's risk strategy and risk appetite.**
- **The second line is responsible for providing robust, independent oversight and challenge of first line risk-taking, but is not responsible for managing the organisation's risks.**
- **The third line (internal audit) is responsible for providing independent assurance over the organisation's governance, risk and internal control arrangements.**

First line management should manage risks through the disciplined application of the organisation's risk management framework. The aim is to help the organisation achieve its strategic objectives while remaining within risk appetite. Consequently, first line management should be the principal source of (non-independent) risk information presented to the board risk committee.

In some organisations, first line management may use risk and control units to provide direct assurance to management that their controls are effective and risks appropriately managed. Since these risk and control units are under the control of, and report directly to, first line management, they are not considered independent and form part of the first, and not the second, line.

The same logic applies to other functions, such as HR, Legal or Financial Control, where some level of risk and control oversight is exercised. In these cases, where the definition of independence cannot be met, the risk and control oversight activity of the function should be considered part of the first line.

The second line risk function, headed by the chief risk officer, is responsible for ensuring robust, independent oversight and challenge of first line management's risk-taking activities across the organisation. This may require clear allocation of second line risk oversight responsibilities between the risk function and other second line functions, such as the compliance function.

Risk function reporting should provide the board risk committee with independent assurance that first line management's reporting of the organisation's principal and emerging risks, their impact on the likely achievement of strategic objectives, any significant incidents and near-misses, actual or likely breaches of risk appetite, as well as overall risk profile and risk capacity is complete and fairly stated.

The way in which independent second line risk oversight and challenge is exercised will vary between organisations depending on a number of factors, including first line risk management maturity and other organisational constraints. Where maturity is relatively low or other organisational constraints apply, the risk function may need to adopt a more supportive or collaborative approach to ensure appropriate risk outcomes. Where such an approach is taken, additional care should be exercised to protect the independence – real or perceived – of the chief risk officer and the risk function.

In contrast, where first line risk management maturity is relatively high, a more robust, challenging approach may be adopted.

Anticipated changes in the business environment, such as technological innovations, may influence how independent second line risk oversight and challenge is exercised in future. For example, developments such as artificial intelligence, robotics and blockchain-based technologies are likely to change how second line risk oversight and challenge are delivered, increasing speed of response and integrating challenge into the process.

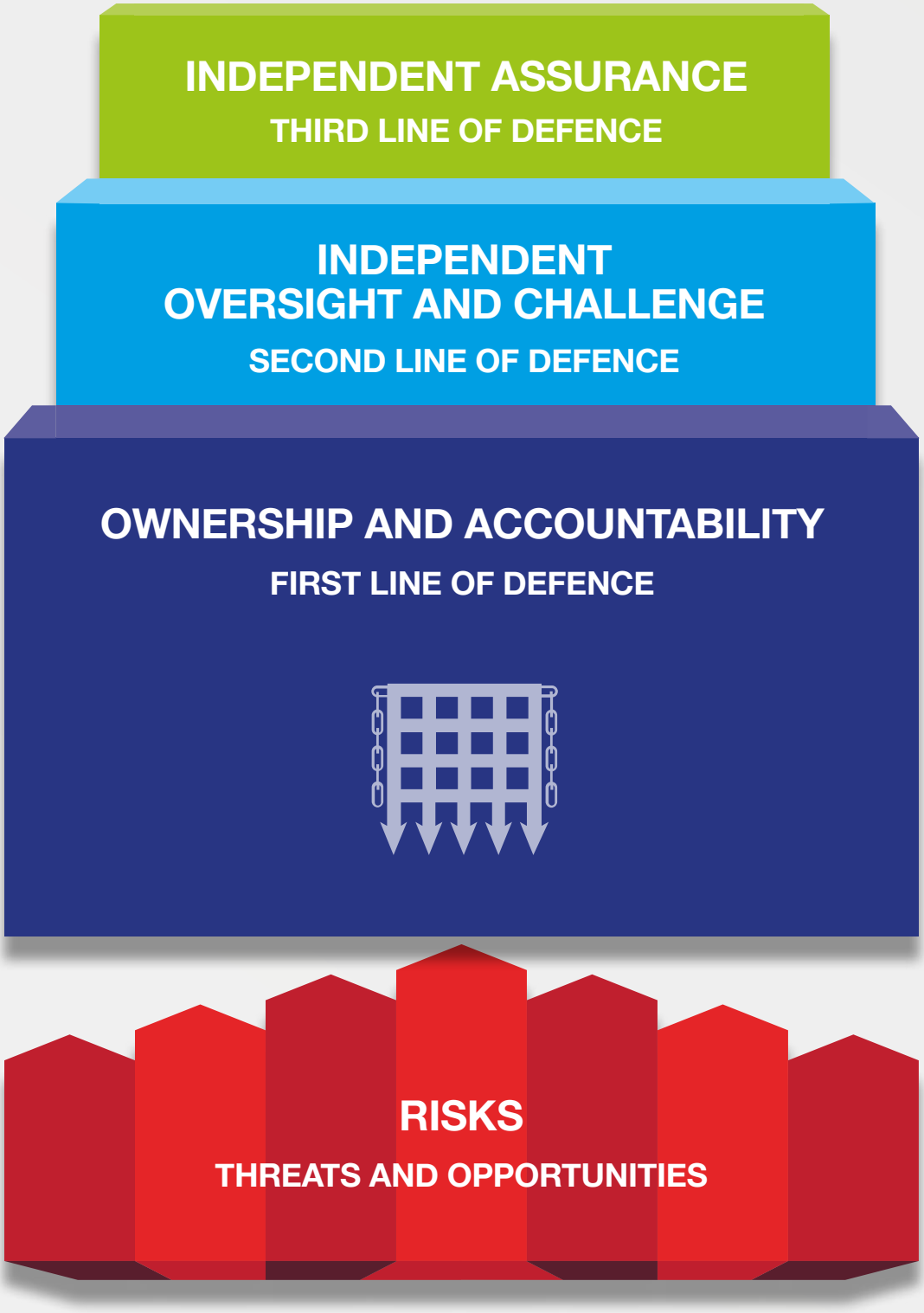
However, the basic requirement for independent risk oversight and challenge in some form will remain.

The third line internal audit function, whose primary reporting line is to the audit committee, aims to help protect the assets, reputation and sustainability of the organisation through providing independent assurance to the board audit and risk committees on the adequacy and effectiveness of the organisation's governance, risk management and internal control systems, including the effectiveness of the risk function itself.

The internal audit function should provide the board risk committee with insight on key risks, details of significant control weaknesses and audit findings. These may include any identified themes or trends that may be pertinent to, or further aid, the board risk committee's understanding of the organisation's principal and emerging risks, including their impact on the likely achievement of strategic objectives, overall risk profile and risk capacity.

The internal audit function should provide the board risk committee with a periodic assessment of the quality and reliability of first and second line risk reporting.

THE THREE LINES OF DEFENCE




risk capacity
independence
scenario analysis
risk policy framework
horizon scanning
risk universe
principal risks
executive risk committee
accountability
risk profile
oversight
risk governance framework
culture
extended enterprise risks
ERM framework
risk strategy
strategic objectives
risk appetite framework
risk appetite
stress testing
challenge

5. APPENDIX 2
DEFINITION OF TERMS

Set out below are definitions for key terms used throughout this guidance. Wherever possible we have used standard definitions[10]. 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.

Executive risk committee – An executive management level committee reporting to the executive committee. The executive risk committee supports the executive committee in fulfilling its risk management responsibilities through providing committee members with an opportunity to spend more time considering key risk matters than would otherwise be possible during executive committee meetings.

Extended enterprise risks – those risks for which the organisation remains accountable, but for which it has outsourced (some or all) responsibility for risk responses 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 chief risk officer and risk function 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 chief risk officer has a reporting line to the board risk committee chair and an executive reporting line to the chief executive officer;
- decisions on chief risk officer:
  - appointment and removal are taken by the board on the advice of the board risk committee and in consultation with the chief executive officer;
  - annual objectives and performance are taken by the board risk committee in consultation with the chief executive officer;
  - remuneration are taken by the remuneration committee in consultation with the board risk committee and the chief executive officer;
- chief risk officer and risk function staff remuneration is not linked to the financial performance of the areas of the business subject to their oversight.

Opportunity – an exploitable set of circumstances with uncertain 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 corporate strategy or strategic objectives. 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 document describing the aggregate types and extent of risk the board is willing to assume or wishes to avoid within the organisation's risk capacity to achieve its strategic objectives and deliver its business plan in both normal and stressed conditions. It should include both qualitative statements and quantitative measures expressed relative to key financial and non-financial measures, as well as addressing other more difficult to quantify risks, such as reputation, conduct and risk culture.

[10] Based on definitions provided by European Banking Authority's Guidelines on internal governance under Directive 2013/36/EU; ISO Guide 73:2009; Financial Stability Board's Principles for an Effective Risk Appetite Framework (2013); Financial Reporting Council's UK Corporate Governance Code (2018); COSO's Enterprise Risk Management – Integrating with Strategy and Performance (2017) and other sources as appropriate.

5. APPENDIX 2
DEFINITION OF TERMS

Risk appetite framework – A key, board-approved framework designed to aid effective management decision-making, risk monitoring and reporting, and through which aggregate risk appetite is translated and cascaded into meaningful, calibrated risk thresholds, limits, metrics and indicators aligned to strategic objectives, and embedded throughout the organisation.

Risk capacity – The maximum level of risk or risk type an organisation can assume, given its current level of resources, before breaching financial, operational, legal or regulatory (including conduct) constraints.

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 corporate strategy and strategic objectives.

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 profile – A composite view of the risk assumed at a particular level of the entity, or aspect of the business model, that positions management to consider the types, severity and interdependencies of risks, and how they may affect performance relative to its corporate strategy and strategic objectives.

Risk strategy – The organisation's overall approach to risk management, which should support and be consistent with the organisation's corporate strategy, strategic objectives, 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. A risk universe typically includes increasingly granular sub-categories of risk types below each of the primary risk categories.

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 objectives – Top-level objectives linked to the achievement of corporate strategy. Strategic objectives may be translated into supporting business, product, process or project objectives throughout the organisation.

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.

6. THE RISK COALITION STRUCTURE

The Risk Coalition
Leading Risk Thinking

Aspires to improve risk management, including risk governance and oversight, initially in the UK financial services sector. It is an association of not-for-profit professional bodies and membership organisations.
The Risk Coalition is governed by Terms of Reference. It instigated the Risk Guidance Initiative to develop principles-based guidance for risk committees and risk functions in the UK financial services sector.
The outcome of this work is *Raising the Bar* published in December 2019. The Risk Coalition may subsequently commission future projects or research papers.

Risk Coalition Research Company Limited (RCRC)

Administers and supports the work of the Risk Coalition, including delivery of approved projects, the first of which is *Raising the Bar*. It is a not-for-profit company, limited by guarantee and VAT registered. At present the RCRC has four directors who comprise the Core Team (see page 32).

Sponsors

Contribute significantly to the Risk Guidance Initiative either by financial or other material practical support.

Supporting organisations

Support the Risk Guidance Initiative directly and will promote this guidance both to their members and a wider audience. They have also contributed their technical expertise to the development of this guidance.

Observers

Comprise interested parties who are supportive of the Risk Coalition's work and have been involved in the development of this guidance.

Working group

Meets as required and is supported by the RCRC. It provides practitioner, professional and academic input, and reviews draft texts for intended publication. See list of participants on the inside back cover.

The Risk Coalition

Leading Risk Thinking

The Risk Coalition is an association of not-for-profit professional bodies and membership organisations committed to raising the standards of risk management in the UK. The Risk Coalition launched the Risk Guidance Initiative in 2018 to meet the need for coherent, principles-based good practice guidance for board risk committees and risk functions within the UK financial services sector. The outcome of this work is *Raising the Bar* published in December 2019.

In developing this guidance, the Risk Coalition has drawn on industry, academic and regulatory best practice and consulted widely, including with the key UK financial regulators who are supportive of all work that raises risk standards across the industry.

The Risk Coalition's objectives for this principles-based guidance are to:

- establish a common understanding of the purpose, role and activities of the board risk committee and risk function;
- provide a benchmark against which board risk committees and risk functions can be assessed objectively;
- raise the general standard of risk governance and oversight practice within UK financial services; and
- fill the gap in principles-based good practice risk guidance whilst recognising the presence of detailed regulation.

The Risk Coalition is supported by the Risk Coalition Research Company Limited, a not-for-profit company established to propose, initiate, administer and deliver Risk Coalition approved projects and initiatives.

RISK GUIDANCE INITIATIVE TEAM

The Risk Coalition would like to acknowledge and express its gratitude for the considerable pro bono efforts made towards the development and publication of this guidance by the Risk Guidance Initiative core team, without whom this initiative would not have been possible:

Core team:

- **Hanif Barma**
  (Partner, Board Alchemy)
  Coalition concept, industry/regulatory stakeholder engagement
- **Chris Burt**
  (Principal, Halex Consulting)
  Original concept and principal author
- **Bryan Foss**
  (Independent NED and Visiting Professor, Bristol Business School)
  Core team advisor and stakeholder engagement
- **Peter Neville Lewis**
  (Director, Principled Consulting)
  Research lead and stakeholder engagement

Special thanks also to:

- **Marcia Cantor-Grable**
  NED and Regulation Board, Institute and Faculty of Actuaries
- **Julia Graham**
  Deputy Chair and Technical Director, Airmic
- **Alex Hindson**
  Group CRO, Argo Group International Holdings;
  NED, ORIC International
- **Clive Martin**
  Internal Consulting Group
- **Liz Sandwith**
  Chief Professional Practice Adviser, Chartered IIA
- **Martin Stewart**
  Former Director of Supervision, Banks, Building Societies, Credit Unions, Prudential Regulation Authority
- **John Thirlwell**
  Former Director, Institute of Operational Risk
- **Carolyn Williams**
  Director of Corporate Relations, IRM
- **Marian Williams**
  Director, Financial Services – Advisory, KPMG;
  Former Director of Audit, FRC

7. Acknowledgements

The Risk Coalition would also like to acknowledge the following people who have contributed in many ways to the production of this principles-based guidance (*Raising the Bar*) through participating in Working Groups and providing critical feedback at various stages. Their support and inputs have been invaluable and are greatly appreciated.

Richard Anderson
Chair, Risk Committee, pay.uk

Dr Scarlett Brown
Co-author, Grant Thornton, Corporate Governance Review

Daniel Bruce
Partner, Crowe

Gill Clarke
Strategic Risk and Compliance Director, Hermes Investment Management

Sharon Constancon
CEO, Genius Methods; Chair, South Africa Chamber of Commerce UK

Nicola Crawford
Former Chair, Institute of Risk Management

Brandon Davies
NED and Lecturer University of Buckingham

Andrew Duff
Director, EY FS Advisory Services

Steve Fowler
Governor and Chair, Audit and Risk Committee, University of West London

Jane Fuller
Co-Director, Centre for the Study of Financial Innovation

Peter Kelk
MD, Charles Stanley Investment Management Services; Former CRO

Kathryn Kerle
Chair, Greater London Mutual

Andrew Macleod
Board Member, Cornerstone Capital (NY); Visiting Professor Kings College, London

Fraser McNeil
CRO, Coventry Building Society

John Mongelard
Technical Manager – Risk and Regulation, ICAEW

Paul Moore
Director, Moore Carter Associates

Professor Paul Moxey
London South Bank University

Liz Murrall
Chair, FRC Reporting Council; Director, Investment Association

Professor Mike Power
Professor of Accounting, London School of Economics; NED (Audit and Risk Committees) RIT Capital Partners

Richard Settle
CRO, Euroclear UK

Alan Smith
Global Head of Risk Strategy, HSBC

Richard Sykes
Former Head of GRC UK, PwC

Paul Taylor
Chair, Risk Committee, Ascot Underwriting; Former Chair, AIRMIC; Former VP, FERMA

Iain Wright
Chair, IRM; CRO, Canada Life

Paul Wright
FR Consulting; Former UK Exec Director IMF; Senior Director, Institute of International Finance

Susan Young
CRO, Randall Quilter Investment Holdings

NOTES

FEEDBACK FROM CONSULTATION EXERCISE

"

The guidance is shaping up really well to be an excellent product, which will have a good deal of impact in the financial services sector and beyond."

Olivia Dickson
Board member,
Financial Reporting Council

"

Overall, I found it a tremendously informative document that I can well believe would assist many organisations."

Kevin Bernbaum
NED,
Chorley Building Society

"

I like the Risk Coalition's positive spin on roles, focus on objectives, absence of branding as 'defence' and emphasis on the key role of the board. It should be a MUST READ for all board members, CEOs and risk specialists."

Tim Leech
Principal, Risk Oversight Solutions (Canada)

"

I view the guidance as potentially very helpful and insightful, subject to ensuring it has wide endorsement within the financial services sector, including primary regulators."

Robert Beattie
Group Director Internal Audit, Virgin Money

"

A thoughtful piece of guidance – a nice blend of principles and specifics. Going forward this will come to life via more detailed discussion and sharing of practical experiences."

Sue Kean
INED and former Group CRO, Old Mutual plc

"

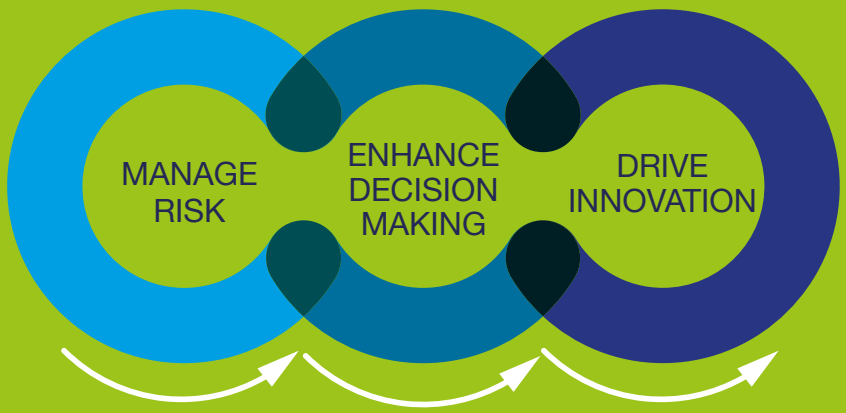
Overall I think this is a good document, and an excellent, long overdue set of guidance."

Justin Elks
MD, Crowe
ERM and Insurance

Please note that throughout this document where quotes are attributable to an individual, they do not necessarily reflect the opinion of the organisation for whom they work.

Raising the Bar

THE SMARTER 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