The Risk Guidance Initiative

Board risk committee and risk function principles and guidance

Purpose

1. This guidance has been developed by the Risk Coalition to provide UK financial services organisations, their boards, non-executive committees and executive management teams with pragmatic, industry-consensus good practice guidance on risk governance and practise. Moreover, the Risk Coalition believes that the principles defined within this guidance are sufficiently fundamental that non-FS organisations would also benefit from their application.

2. Part A of the guidance focuses on what can reasonably be expected of a mature board risk committee 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 chief risk officer and second line risk function.

3. The guidance has been written to be ‘risk agnostic’, providing users with guidance on what needs to be done, rather than how it should be done. So, for example, the guidance does not reference specific types of risk as these will be different for every organisation, preferring, instead, to focus on basic good practice principles that will stand the test of time.

4. The guidance is intended to be applicable to all UK regulated financial services organisations, whether a group, subsidiary or stand-alone entity and is consistent with key regulatory requirements and good practice guidance, such as the UK Corporate Governance Code (the Code).

5. The guidance assumes that organisations operate a three lines of defence model in line with current regulatory expectations1. Whilst the concept of the three lines of defence continues to be the subject of much academic and professional debate, the Risk Coalition believes the basic principle of requiring independent oversight and challenge of management’s risk-taking remains sound, although how the principle is applied may change as a result of technological or other changes in the business environment.

6. The guidance has been developed through industry consultation and consensus and is intended to be evolutionary in nature, going beyond current common practice. Nonetheless, the Risk Coalition anticipates that full implementation of the guidance will prove appropriately challenging, even for the largest organisations.

7. Whilst this guidance aims to define ‘what good looks like’ for board risk committees and risk functions, it is key that organisations and their regulators continually challenge whether application of this guidance is sufficient. The Risk Coalition strongly encourages organisations to innovate, going beyond the minimum necessary wherever possible.

8. The Risk Coalition expects that larger, more mature organisations will wish to fully implement the guidance relatively quickly. Smaller or less mature organisations are expected to apply the guidance intelligently and proportionately and are encouraged to use professional judgement in deciding how each principle applies to the firm and over what period it should be implemented.

9. The Risk Coalition encourages firms to disclose their application of the guidance in their annual report.

---

1 See Appendix 1 for guidance on how the three lines of defence should typically be applied within a financial services organisation.
Part A - Board risk committee principles and guidance

**Principle A1 - Board accountability:**

*The board risk committee is an advisory committee to the board with the aim of facilitating focused and informed board discussions on risk matters. The board retains ultimate accountability for the adequacy and effectiveness of the organisation’s risk management arrangements.*

*The board risk committee should:*

10. Provide consolidated oversight and reporting to the board on the organisation’s principal risks, including those within the remit of other board committees, such as the audit, remuneration and nomination committees. For clarity, this includes consideration of all enterprise risks - whether internal or external, financial or non-financial, in-house or extended enterprise.

11. Confirm that responsibility for oversight of each principal risk is clearly allocated to a specific board committee, without undermining the board risk committee’s consolidated risk oversight responsibility, and that arrangements are in place to ensure an efficient and effective exchange of information and views amongst the relevant committees.

12. Where applicable, provide an appropriate mechanism for board risk committees (or committee chairs) within a group of companies to periodically exchange relevant information and views.

13. Provide the board with a clear and concise summary of the matters the board risk committee has considered and any associated recommendations.

**Principle A2 - Composition & membership:**

*The board risk committee should be formed of independent non-executive directors and apply chair, membership, competence and performance evaluation criteria as outlined in the UK Corporate Governance Code for other board committees.*

*The board risk committee should:*

14. Have board-approved terms of reference which set out its responsibilities and activities clearly.

15. Periodically consider whether its planned annual cycle of activity remains appropriate, including providing sufficient time for exploration of key and emerging risk-related topics and themes.

16. Regularly consider whether it possesses the appropriate balance of skills and relevant expertise to fulfil its remit successfully. The board risk committee should have access to external expert risk advice and guidance as necessary.

17. Implement 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.

18. Guard its non-executive status carefully and should not act (fully or partially) in the capacity of an executive risk committee.

19. Provide a standing invitation to key board members (where not a board risk committee member) and relevant executives. Other standing invitees should include the chief risk officer, chief internal auditor and external auditor.

**Principle A3 - Risk strategy & 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 the light of the organisation’s corporate strategy and objectives.*

*The board risk committee should:*

20. Constructively challenge whether the organisation’s corporate strategy is sufficiently clearly defined, aligned to a resilient and sustainable business model and effectively communicated to all levels.
21. Assess whether the organisation has an appropriate framework of prioritised, well-defined objectives covering, as a minimum, categories for strategic, operational, financial, conduct & compliance, ESG\(^2\) and viability objectives that have been embedded throughout the organisation.

22. Evaluate whether the organisation has a clearly defined and understandable board-set risk strategy and risk appetite statement that align and are consistent with the organisation’s corporate strategy and objectives. Together, the risk strategy and risk appetite statement should:

- clearly define the organisation’s overall approach to managing risks;
- describe the aggregate types and extent of risk the organisation is willing to assume (or wishes to avoid) in both normal and stressed conditions;
- translate into a robust, board-approved risk appetite framework of calibrated risk thresholds, limits and metrics aligned to objectives, that have been cascaded and embedded throughout the organisation; and
- help the board and executive management understand, analyse and make appropriate prioritisation decisions between competing objectives.

23. Consider whether there is appropriate alignment between the organisation’s product and service offering (including pricing and profitability) and the organisation’s risk strategy and risk appetite.

24. Notify the board of actual or forecast material breaches of risk appetite and comment on management’s response, including recommending further actions where appropriate.

**Principle A4 - Principal risks and continued viability:**

*The board risk committee should assess and advise the board on the organisation’s principal current and emerging risks, including those associated with the organisation’s corporate strategy and objectives, and the continued viability of its business model.*

The board risk committee should

25. Constructively challenge whether executive management has a sound understanding of the organisation’s principal current and emerging risks – including those associated with the organisation’s corporate strategy and objectives, and the continued viability of its business model – and how they may impact (or benefit) the organisation, as well as the factors that drive and connect them and how they may change in the short and medium term.

26. Contribute to, and assess the effectiveness of, the organisation’s emerging risk identification and horizon scanning processes. Constructively challenge whether the organisation is sufficiently agile to mitigate risks and exploit opportunities presented by business environment changes and technology innovations.

27. Consider whether contractual arrangements with key intra-group or outsourced service providers enable effective first and second line risk oversight and adequately incentivise appropriate third-party risk management behaviours.

28. Monitor, and constructively 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.

29. Assess and advise the board on the likely achievement of objectives based on an assessment of the organisation’s principal current and emerging risks and overall residual risk profile.

\(^2\) Environmental, social & governance (ESG). In some organisations the concept of corporate & social responsibility is used instead.
30. Understand and constructively challenge the range of scenarios and reasonableness of key assumptions – such as the effectiveness of current and planned risk mitigations in both normal and stressed conditions - underlying management’s capital, liquidity and solvency modelling, and business continuity, recovery, restructuring and orderly wind-down planning (where relevant).

31. Critically review and, where appropriate, recommend for board approval the final output of capital, liquidity and solvency modelling, as well as business continuity, recovery, restructuring and orderly wind-down plans.

**Principle A5 – Risk culture & remuneration:**

*In liaison with the remuneration committee (where appropriate), the board risk committee should consider and periodically report to the board whether the organisation’s purpose and board-approved risk culture expectations are appropriately reflected in observed ethics, values and behaviours.*

*The board risk committee should*

32. Consider whether the organisation has a clearly defined purpose and board-approved statement of risk culture expectations covering key risk culture influences such as tone from the top, accountability, effective communication and challenge, and (financial and non-financial) incentives.

33. Assess whether the organisation’s purpose and risk culture expectations are properly understood by executive management and reflected in the organisation’s corporate strategy, objectives, risk strategy and risk appetite, as well as executive and management remuneration arrangements.

34. Assess whether the board’s stated risk culture expectations have been appropriately translated into a framework of ethics, values and desired behaviours and effectively embedded throughout all levels of the organisation with associated metrics and indicators.

35. Consider whether proposed executive and management remuneration plans are consistent with the board’s stated risk culture principles and whether they are likely to encourage prudent, transparent management risk-taking.

36. Monitor and report to the board on how executive and management remuneration arrangements appear to affect observed behaviours and influences on risk culture and any consequent impact on the organisation’s principal risks.

37. Advise the board whether the organisation’s risk culture expectations and associated whistle-blowing (speak up) arrangements provide those working within the organisation with the appropriate support to ‘do the right thing’ in difficult or challenging circumstances.

38. Review and report to the board on the results of on-going risk culture monitoring activities performed by each of the three lines of defence.

39. Consider whether executive management’s attitude towards, and treatment of, internal control function and external audit recommendations is indicative of a healthy risk culture.

**Principle A6 - Risk management and internal control systems:**

*In liaison with the audit committee (where appropriate), the board risk committee should assess the results of on-going monitoring and periodic reviews of the effectiveness of the organisation’s risk management and internal control systems, including the adequacy and quality of independent assurance over the organisation’s risk arrangements.*

*The board risk committee should*

40. Review and recommend to the board for approval, proposed material changes to the organisation’s risk management framework, including its risk governance and risk appetite frameworks.
41. Constructively challenge whether the organisation is taking sufficient advantage of new technologies and ways of working to enhance the adequacy and effectiveness of its risk management arrangements.

42. Consider whether individual and collective risk and control accountabilities within the organisation are clearly and adequately documented, communicated and applied appropriately.

43. Constructively challenge executive management to demonstrate that its processes for monitoring and assessing the adequacy and effectiveness of the organisation’s risk management and internal control systems - including near miss and lessons learned analysis and reporting – is both robust and reliable.

44. Seek independent second line risk function assurance that first line management’s identification, assessment, analysis (both qualitative and quantitative), monitoring and reporting of the organisation’s principal current and emerging risks, and their likely impact on the organisation’s objectives - both in isolation and in combination - as well as overall residual risk profile and risk capacity is complete, accurate and fairly stated.

45. Consider and report to the board the results of periodic independent assessments of the design, implementation and operation of the organisation’s risk management and internal control systems, including the effectiveness of its risk management, compliance and internal audit functions.

**Principle A7 - Risk information and reporting:**

The board risk committee should review the adequacy, appropriateness, reliability and timeliness of board-level risk information, including risk information for external publication. The board risk committee should also assess the quality and reliability of information governance arrangements including over risk data collection, aggregation, analysis and reporting.

The board risk committee should

46. Consider the adequacy, appropriateness, reliability and timeliness of board-level risk reporting from each of the lines of defence, including the prompt escalation of relevant risk appetite framework information and supporting analysis/narrative.

47. Seek independent assurance that risk information reporting within the organisation (including between group entities) and with supervisory authorities is complete, accurate and timely, and that information governance arrangements over risk data collection, aggregation, analysis and reporting are robust and reliable.

48. Review and recommend to the board for approval all risk information for regulatory submission or external publication.

**Principle A8 - Chief risk officer and risk function independence:**

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

The board risk committee should

49. Periodically review and approve the risk function’s charter, including the independence, scope, role, responsibilities and accountabilities of the chief risk officer and the risk function. Particular consideration should be given to the continued objectivity and independence of the chief risk officer where they have been in post for more than seven years.

---

3 Internal audit may provide independent assessments of an organisation’s risk management and internal control systems. As a matter of prudence, it is recommended that an independent external evaluation of risk function effectiveness is performed at least once every five years.

4 Where an organisation does not have a chief risk officer or second line risk function, the board risk committee should periodically consider whether this remains appropriate.
50. Understand 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.

51. Ensure that the chief risk officer is sufficiently senior and appropriately positioned to challenge effectively executive management risk-taking, and that the risk function has adequate, appropriate resources (people, processes and technology) to meet its charter obligations.

52. Have access to the minutes of executive committee and executive risk committee discussions.

53. Ensure that appropriate arrangements are in place, particularly in a group context, to mitigate any potential conflicts of interest that might undermine the actual or perceived independence of the chief risk officer and risk function. (For example, where a subsidiary entity chief risk officer has an additional reporting line to the group chief risk officer.)

54. Ensure that the chief risk officer has a direct report to the board risk committee chair and has unmediated access to the board chair, the board itself, the board risk committee, the external auditor and the supervisory authorities as necessary.

55. 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.

56. Appoint or remove the chief risk officer in consultation with the chief executive officer.

57. In consultation with the chief executive officer, 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).
Part B – Risk function principles and guidance

Principle B1 - Risk oversight - The chief risk officer is responsible for ensuring robust, independent oversight and challenge of risk-taking activities across the organisation.

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

59. It is acceptable for the heads of other independent second line functions, such as the chief compliance officer or head of independent model validation, to report to the chief risk officer provided that appropriate conflicts of interests safeguards are put in place. For example, when reviewing compliance arrangements within the risk function or validating models owned or operated by the risk function.

60. It is not acceptable for the chief internal auditor (or equivalent) to report to the chief risk officer.

61. The chief risk officer should periodically share a summary of independent second line risk oversight responsibilities with the board risk committee for its consideration and approval.

62. The chief risk officer should identify instances where the three lines of defence model is not followed – for example, where the second line provides operational support to first line management. In each instance, the variation to the model should be documented, its implications assessed and the findings presented to the board risk committee for consideration and approval as necessary.

Principle B2 - Independent perspective - The chief risk officer should seek to maintain an independent perspective.

63. Wherever possible, the chief risk officer should seek to develop an independent perspective to support effective challenge of first line management risk-taking activities. This may require the chief risk officer to leverage risk function resources to independently produce relevant information, as well have having free and unrestricted access to any internal or relevant third-party information, people or locations deemed necessary to form an independent view.

64. Executive management and the board should seek to protect the independence of the chief risk officer and risk function through implementation of a three lines of defence model, including ensuring the chief risk officer and risk function remain free of operational responsibilities.

65. The chief risk officer should report directly to the board risk committee chair with a secondary (administrative) reporting line to the chief executive officer if required. The chief risk officer should also have unmediated access to the board chair, the board itself, the board risk committee, the external auditor and the supervisory authorities as necessary.

66. The chief risk officer should always seek to be open and transparent in any dealings with executive management, the board risk committee and supervisory authorities.

67. 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 of the chief risk officer and risk function. For example, where a subsidiary entity chief risk officer has an additional reporting line to the group chief risk officer.
Principle B3 - Risk governance – The chief risk officer should be appropriately positioned to provide effective challenge at executive management and board risk committee level

68. The chief risk officer should receive a standing invitation to attend both the board risk committee and audit committee where they should actively engage in committee discussions, providing an independent, expert view as appropriate.

69. The chief risk officer should be of equivalent standing and seniority as members of the executive committee and should routinely attend and may be a member of the executive committee, subject to appropriate independence safeguards being in place.

70. Where the chief risk officer is a member of the executive committee, the chief risk officer retains collective responsibility for executive committee decisions with the other executive committee members.

71. Where one exists, the chief risk officer should be a member of, but should not chair, the executive risk committee - the purpose being to enable appropriate second line challenge whilst reinforcing first line management responsibility and accountability for taking and managing risks in line with the organisation’s risk appetite.

72. The chief risk officer should not form part of any standard approval process for operational decisions—such as approval of lines of credit - or separately approve or otherwise endorse or ‘sign-off’ key management decisions. The chief risk officer should instead seek to constructively challenge first line management whether all pertinent risks and their potential impact on objectives and risk appetite, as well as overall risk capacity and risk profile, have been appropriately considered and addressed in first line management’s decision-making process.

73. Where, after full and frank discussion at the board risk committee, executive committee or executive risk committee, a decision is made to which the chief risk officer objects or is not otherwise comfortable, the chief risk officer’s objection or reason for discomfort should be clearly and fully minuted. The chief risk officer may reasonably choose to make their objection or discomfort known - formally or informally - to the board risk committee chair and/or the board chair.

74. Organisations may choose to give the chief risk officer the right of veto over management decisions taken at levels below that of the executive committee or executive risk committee.

Principle B4 - Risk reporting – The chief risk officer should provide the board risk committee with independent assurance that first line management’s reporting of risks is both complete and fairly stated.

75. The chief risk officer should provide the board risk committee with their independent view of the organisation’s principal current and emerging risks and their likely impact on the organisation’s objectives - in both the short and medium term - on a regular basis, as well as any other matter that the chief risk officer feels is pertinent or necessary to facilitate full and effective board risk committee discussions.

76. The chief risk officer should provide the board risk committee with appropriate assurance that first line management’s reporting of the organisation’s principal risks (including new and emerging risks), overall residual risk profile (including any actual or forecast breaches of risk appetite) and risk capacity is complete and fairly stated.

77. Chief risk officer reports 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. The chief risk officer should also routinely provide formal reporting to the audit committee appropriate to its needs.
Principle B5 - Corporate strategy - The chief risk officer should actively participate in corporate strategy and objective discussions at the executive and board level.

78. The chief risk officer should attend and actively participate in executive and board-level discussions relating to the development and setting of the organisation’s corporate strategy and objectives. The chief risk officer should seek to ensure that discussions adequately consider the implications of changes to corporate strategy and objectives on:

- risk strategy, risk appetite, risk capacity and risk profile; and
- the organisation’s defined purpose, values and desired risk culture.

79. The chief risk officer should ensure they are aware of, and may choose to participate in, executive and board-level discussions relating to material corporate actions and significant changes to governance arrangements or legal structure with the aim of ensuring that relevant risks are appropriately considered.

Principle B6 - Risk function – the chief risk officer should ensure the independence and effectiveness of the risk function

80. The chief risk officer should develop and seek board risk committee approval of an appropriate risk function charter detailing the independence, role, responsibility, scope and authority of the chief risk officer and the risk function.

81. 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 that the chief risk officer, in consultation with the board risk committee chair, considers pertinent to fulfilling the risk function’s charter responsibilities.

82. The risk function should have a risk function manual 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 processes.

83. In discharging its independent risk oversight and challenge responsibilities, the risk function should:

- establish, monitor, maintain, facilitate and assess the effective operation of the organisation’s risk management framework;
- ensure the organisation has access to adequate risk management resources, including tools and technology;
- provide risk education and training at all levels within the organisation where helpful or necessary;
- constructively challenge management and advise the board risk committee on the identification, assessment, analysis, mitigation and reporting of risks – including new and emerging risks;
- act as an independent risk ‘sounding board’ for executive management and the board risk committee; and
- lead and share risk thinking within the organisation.

84. The risk function should be sufficiently resourced to meet its charter obligations and the reasonable expectations of key stakeholders, including executive management, the board risk committee and the
organisation’s supervisory authorities. Where the chief risk officer considers resources are insufficient for its purposes, the matter should be raised with executive management in the first instance with further escalation to the board risk committee if necessary.

85. The risk function should be appropriately and adequately staffed. Diversity of background, experience and perspectives should be encouraged, underpinned by an appropriate level of risk management expertise and understanding of the organisation.

86. 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.

87. The risk function should have access to appropriate technology resources to support its charter obligations and stakeholder expectations, including access to risk data aggregation and analytics capabilities.

88. Where a risk function provides modelling 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, scenarios and final output.

89. The risk function should have access to external risk management resources to supplement internal capabilities or capacity constraints where needed. Where risk function work is co-sourced or outsourced to an external provider, the chief risk officer remains responsible for the overall quality of the work performed.

90. The chief risk officer should ensure that appropriate quality assurance arrangements are implemented within the risk function.

91. Risk function members should have access to, and be encouraged to participate in, relevant continuous education and development opportunities. The chief risk officer should give consideration to further professionalising the risk function through providing access to externally recognised risk management qualifications where appropriate.

**Principle B7 - Planning – the risk function should develop and implement a plan of independent risk assessment and risk monitoring activities**

92. The chief risk officer, supported by senior members of the risk function, should develop and implement regular, structured engagement with key stakeholders from across the organisation and externally where appropriate.

93. The risk function should develop a plan, drawing on both formal and informal sources of information, outlining the independent risk assessments and risk monitoring activities it intends to undertake over the course of the following year (or other appropriate period).

94. The risk function plan should cover all sources and types of risk and be revised and updated in the course of the year as necessary and shared with executive management for comment and submitted to the board risk committee for review and approval periodically.

95. The risk function should share details and co-ordinate planned work with the compliance and internal audit functions to minimise the impact of second- and third-line assurance work on the organisation. 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.

96. When carrying out independent risk assessments and risk monitoring activities (including stakeholder management), members of the risk function should document their work and retain appropriate supporting evidence – such as meeting minutes and key documentation - sufficient to support their opinions.
97. Results of independent risk assessments and risk monitoring activities, along with any associated recommendations and agreed first line management actions, should be formally documented in a report, memo or other appropriate means to executive management. Summary results, recommendations and agreed first line management actions should be shared with the board risk committee as appropriate.

98. The risk function should routinely track and report progress against agreed first line management actions to executive management and the board risk committee.

**Principle B8 - Risk management framework – the risk function should design and facilitate the implementation and efficient operation of a robust risk management framework**

99. The risk function is responsible for designing and facilitating the implementation and efficient operation of the organisation’s risk management framework (incorporating its risk governance and risk appetite frameworks). Working in close collaboration with executive management and the board risk committee, the risk function should:

- propose a risk strategy and associated risk appetite statement, for both normal and stressed conditions, for consideration and approval by the board. The proposed risk strategy and risk appetite statement should be consistent with the organisation’s corporate strategy, objectives, purpose, values and risk culture;

- design and document a risk management framework consistent with the organisation’s risk strategy and appetite and appropriate for its needs. This should include development of relevant policies, procedures, guidance, tools, templates 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 of risk thresholds, limits and metrics\(^5\), aligned to objectives, that have been cascaded and embedded throughout the organisation.

100. The risk function should develop and monitor a portfolio of risk appetite framework metrics, in addition to those used by first line management, to support its independent monitoring of the organisation’s risk profile.

101. The risk function should routinely monitor the effective operation (in terms of process and outcomes) of the organisation’s risk management framework and suggest improvements where necessary.

102. Annually, the chief risk officer should provide the board risk committee with a formal analysis of the adequacy and effectiveness of the organisation’s - and where relevant, the group’s - risk management arrangements, including risk function effectiveness.

**Principle B9 - Risk culture – the risk function should monitor, assess and periodically report to executive management and the board risk committee on the health of the organisation’s risk culture**

---

\(^5\) Including metrics relating to the organisation’s risk culture.
103. The risk function should introduce processes to enable it to monitor and assess the organisation’s risk culture from a range of perspectives, including top-down, bottom-up and horizontally across business lines, entities and geographies.

104. In performing independent risk assessments and risk monitoring activities, members of the risk function should be mindful of, and where appropriate document and report, behaviours or influences on risk culture – such as tone from the top, accountability, effective communication and challenge, and (financial and non-financial) incentives - that may impact the organisation’s risk profile.

105. 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 risk culture monitoring and make recommendations for improvement.

Principle B10 - Innovation and change – the risk function should support the organisation to identify and adapt effectively to material changes or developments in the internal or external environment

106. The risk function should develop and facilitate operation of an enterprise-wide risk identification and horizon scanning process that encourages and incorporates contributions from each of the lines of defence, executive management and the board risk committee.

107. The chief risk officer should constructively challenge first line management to analyse and assess the potential benefits, as well as the threats, associated with the outputs of the enterprise-wide risk identification and horizon scanning process and to consider the implications for the organisation’s corporate strategy, objectives and business model.

108. The risk function should implement processes to support its own early identification, analysis and response to proposed or actual material changes within 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.

109. 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 B11 - Group risk functions – the group chief risk officer should ensure that risk management arrangements operating across the group are appropriate and effective

110. The group chief risk officer should ensure appropriate mechanisms are in place to facilitate the open 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.

111. The group chief risk officer should monitor and regularly assess the adequacy and effectiveness of independent risk oversight arrangements within the regulated 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 local entity board risk committee in the first instance. The group chief risk officer may also raise the matter with the group board risk committee if their concerns are sufficiently material to the group’s residual risk profile or reputation.
APPENDIX 1 - The three lines of defence

112. The guidance assumes that organisations operate a three lines of defence model. Under this model, first line management owns the organisation’s risks and is responsible for risk-taking. First line management is therefore responsible for identifying, assessing, managing, monitoring and reporting the organisation’s risks in line with the organisation’s risk strategy and risk appetite. The second line is responsible for providing independent oversight and challenge of first line risk-taking.

113. First line management should manage risks through the disciplined application of the organisation’s risk management framework, incorporating its risk governance and risk appetite frameworks. The purpose being to help the organisation achieve its 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.

114. 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 and report directly to first line management, they are not considered independent and form part of the first, and not the second, line.

115. 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 independent cannot be met, the risk and control oversight activity of the function is considered part of the first line.

116. The chief risk officer, as head of the second line risk function, 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.

117. The way in which independent second line risk oversight and challenge is exercised will vary between organisations depending on first line risk management maturity. Where maturity is relatively low, the risk function may need to adopt a more supportive or collaborative approach to ensure appropriate risk outcomes. In contrast, where first line risk management maturity is relatively high, a more robust challenging approach may be adopted. Under the former approach, additional care should be exercised to protect the independence – real or perceived - of the chief risk officer and the risk function.

118. Changes in the business environment or technological innovations may also influence how second line risk oversight and challenge is exercised. For example, recent developments such as artificial intelligence and adoption of Blockchain based technologies are likely to influence how independent second line risk oversight and challenge is delivered, increasing speed of response and integrating challenge into the process. The basic requirement for some sort of independent risk oversight and challenge will, however, remain.

119. Risk function reporting should provide the board risk committee with independent assurance that first line management’s reporting of the organisation’s principal risks (including new and emerging risks), overall residual risk profile and risk capacity is complete and fairly stated. The chief risk officer should also give their view on the likely achievement of objectives in the context of the organisation’s principal risks and risk appetite.

120. The third line internal audit function 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.

121. The internal audit function should provide the board risk committee with insight on key risks, details of significant control weaknesses and audit finding themes or trends that may be pertinent to, or further aid, the board risk committee’s understanding of the organisation’s principal risks, overall residual risk profile and risk capacity.

122. At least annually, the internal audit function should assess, based on an analysis of its work in the year, the overall adequacy and effectiveness of the organisation’s risk management framework, including its risk governance and risk appetite frameworks.
123. Internal audit function reporting to the board risk committee should include a periodic assessment of the quality and reliability of first- and second-line risk reporting.

124. The board risk committee should encourage the external auditor to express their views on the organisation’s principal risks and whether they consider the information presented to the board risk committee by each of the three lines of defence is consistent with their own views.
APPENDIX 2 - Glossary of terms

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

Enterprise risks – All risks facing an organisation, whether internal or external, financial or non-financial, in-house or extended enterprise.

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 (ExCo). The executive risk committee supports the ExCo 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 ExCo meetings.

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

Independence – an independent second line function is considered independent if:

• it is organisationally separate from, and its staff do not perform any operational tasks within, areas of the business subject to its oversight;

• the head of the independent second line function has a direct reporting line to an appropriate independent non-executive director and decisions on hiring, firing, performance and remuneration are taken by the responsible board committee. (The head of the independent second line function may report to a person that reports to an appropriate independent non-executive director.); and

• remuneration of independent second line function staff is not linked solely to the financial performance of the areas of the business subject to their oversight but may be linked to a broad range of financial and non-financial organisational objectives provided this will not compromise their objectivity.

Inherent (gross or pre-control) risk – The risk remaining before risk treatment. OR The exposure before management actions have been taken to mitigate the likelihood or impact (or combination thereof) of a risk.

Objectives – May apply at different levels, such as strategic, organisation-wide, project, product or process.

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.

Residual (net or post-control) risk – The risk remaining after risk treatment. OR The remaining exposure after management actions have been taken to mitigate the likelihood or impact (or combination thereof) of a risk.

Risk - The effect of uncertainty on objectives. OR The possibility that events will occur and affect the achievement of an organisation’s strategy or objectives. Commonly considered as a negative event (downside risk), there may be occasions where risks may be exploited to an organisation’s advantage (upside risk).

Risk appetite – amount and type of risk that an organisation is willing to pursue or retain. OR The aggregate types and extent of risk the board is willing to assume within its risk capacity to achieve its objectives and deliver its business plan in both normal and stressed conditions.

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

Risk appetite statement – A board-approved document describing the aggregate types and extent of risk the organisation is willing to assume (or wishes to avoid) in order to achieve its 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 risks.

**Risk capacity** - The maximum level of risk 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 influence management decisions.

**Risk culture influences** – Defined by the Financial Stability Board as comprising tone from the top, clarity of accountabilities, effective communication and challenge, and (financial and non-financial) incentives.

(Enterprise) **risk management framework** – The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. OR The combination of an organisation’s risk strategy and risk appetite; risk governance arrangements; risk policies, frameworks and procedures; risks in execution (identification, assessment, analysis, mitigation, monitoring & reporting); risk data & technology and risk culture.

**Risk profile** - Description of any set of risks. OR 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 strategy and business objectives.

**Risk strategy** - The organisation’s overall approach to managing risks which should be consistent with the organisation’s corporate strategy, objectives, purpose, values and risk culture. For example, some organisations may seek to align risk profile with risk appetite, whereas other organisations may seek to minimise risk profile below risk appetite.

**Stakeholder** – A person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.