Risk Governance Checklist

It is good governance for any organisation to ensure that all directors and senior executives have a shared understanding of risk, which is the effect of uncertainty on an organisation achieving its strategic objectives and maintaining its long-term sustainability and reputation. This checklist incorporates the key elements of risk governance, which includes the board itself, compliance risk and organisational culture along with risk management.

NOTE: This checklist is only meant as a guide to establishing good practice risk governance. The presence or absence of many of the topics in the questions below will be dependent on the maturity and lifecycle of the organisation – for example, a small organisation will be unlikely to have an internal audit function.

#	Question	Yes	No
Governance			
1.	Is the board of sufficient size and composed of people with an appropriate range of skills and independence to ensure its responsibilities are met?	❑	❑
2.	Do all board members understand their duties as directors?	❑	❑
3.	Is there a board charter or written terms of reference for the board and for board committees?	❑	❑
4.	Is the level of delegation to board committees and management appropriate and clear?	❑	❑
5.	Is there a conflict of interest policy?	❑	❑
6.	Is there a conflict of interest and related party transactions register?	❑	❑
7.	Has the board specified the nature, source, format and frequency of the information that it requires from management?	❑	❑
8.	Does the board monitor the quality of the information it receives and ensure that it is of a sufficient quality to allow effective decision-making?	❑	❑
Compliance			
9.	Does the board ensure management has established effective systems that facilitate and monitor compliance within the organisation?	❑	❑
10.	Is the compliance framework based on a recognised standard, e.g. Australian Standard *AS/NZS ISO 19600 Compliance management systems*?	❑	❑
11.	Is the compliance management system aligned with the organisation's strategic objectives and risk appetite?	❑	❑
12	Has the board established a compliance policy?	❑	❑
13.	Does the compliance policy:		
13.1	Identify a clear compliance framework within which the organisation operates?	❑	❑
13.2	Promote a consistent, rigorous and comprehensive approach to compliance throughout the organisation?	❑	❑
13.3	Seek to ensure standards of good corporate governance, ethics and community expectations?	❑	❑

#	Question	Yes	No
13.4	Set out the organisation's compliance obligations, e.g. legal, contractual, common law, equitable obligations, relevant industry codes and compulsory standards, organisational policies, procedures and guidelines?	❑	❑
13.5	Outline who is involved in compliance management and what their responsibilities are?	❑	❑
14.	Does the organisation have a register of compliance obligations?	❑	❑
15.	Is the compliance register kept up to date?	❑	❑
16.	Is the compliance register linked to the risk register?	❑	❑
17.	Is there a committee tasked with helping the board deal with its compliance oversight responsibilities?		
18.	Does the organisation have a policy for the selection and appointment of the external auditor?	❑	❑
19.	Is there an independent and adequately resourced internal audit function?	❑	❑
20.	Are staff fully trained in the compliance obligations that affect their role and their responsibility for reporting any compliance breaches?	❑	❑
21.	Does the compliance management framework ensure that prompt and appropriate investigations of compliance breaches are undertaken, ensures appropriate disciplinary action is taken where necessary, and corrective measures are implemented to prevent future occurrences?	❑	❑
22.	Is there is a comprehensive whistleblower policy that allows whistleblowers to divulge unethical or illegal practices to their manager, whistleblower protection officer and/or regulatory authority; and provides protection for whistleblowers?	❑	❑
23.	Are there formal record-keeping processes to ensure that important documents are maintained and important dates are recorded and reported to the board (where are the employment agreements, title deeds, certificate of incorporation and insurance certificates of currency)?	❑	❑
Risk management and internal controls			
24.	Does the board ensure that risks facing the entity have been identified, assessed and that the risks are being properly managed?	❑	❑
25.	Is there a specific board committee that deals with risk?	❑	❑
26.	Has the board established a risk management policy?	❑	❑
27	Does the risk management policy:		
27.1	Provide an overview of the risk governance structure of the organisation to indicate who is involved in risk management and what their responsibilities are?	❑	❑
27.2	Outline the steps involved in the risk management process?	❑	❑
27.3	Describe how risk management is integrated and embedded into organisational processes?	❑	❑

#	Question	Yes	No
27.4	Specify risk categories to be included in in the risk register and in risk reporting (e.g. strategic, regulatory, financial, environmental, safety, people, reputation, business continuity risks (including succession planning))?	❑	❑
27.5	Specify the purpose of the risk register?	❑	❑
27.6	Outline the risk reporting requirements?	❑	❑
27.7	Outline how the performance of risk management will be measured?	❑	❑
27.8	Articulate the organisation's risk appetite through a risk appetite statement?	❑	❑
27.9	State how often and who will review the risk management policy?	❑	❑
28.	Does the board set the risk appetite for the organisation?	❑	❑
29.	When determining the key risks, does the board focus on those risks that, given the organisation's current position, could threaten its business model, future performance, solvency or liquidity, irrespective of how they are classified or from where they arise?	❑	❑
30.	Does the board approve how the key risks will be managed or mitigated and which controls will be put in place?	❑	❑
31.	Is the risk register kept up to date?	❑	❑
32.	Is the ownership of risks and risk treatment actions assigned to relevant roles within the organisation?	❑	❑
33.	Is the risk management system based on a recognised standard, e.g. *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines*?	❑	❑
34.	Does management report to the board in relation to the effectiveness of the organisation's risk management and internal control system in managing the organisation's risks?	❑	❑
35.	Does the organisation have adequate insurance for its level of operations and staff numbers?	❑	❑
36.	Are staff fully trained in their risk management responsibilities?	❑	❑
Assurance			
37.	Do the CEO and CFO provide the board with certifications/assurance that:		
37.1.	The financial records of the organisation have been properly maintained?	❑	❑
37.2	The risk management and internal control systems to the extent they relate to financial reporting are operating effectively, in all material respects, based on the organisation's risk management system?	❑	❑
Culture			
38.	Is there a corporate code of conduct or ethics?	❑	❑
39.	Do the members of the board demonstrate the qualities that the organisation seeks to embody its culture?	❑	❑

#	Question	Yes	No
40.	Do the members of the senior management team including the CEO demonstrate the qualities that the organisation seeks to embody in its culture?	❑	❑
41.	Is the risk culture integrated with the corporate culture, i.e. working behaviours and practices?	❑	❑
Business continuity management			
42.	Does the organisation have appropriate plans and systems in place to minimise the effects of a broad range of disruptions and to ensure that business operations are maintained within acceptable limits?	❑	❑
43.	Does the organisation follow an appropriate framework with respect to business continuity planning, e.g. Australian standard *AS/NZS 5050:2010 Business Continuity – Managing disruption-related risk*?	❑	❑
Strategy and risk			
44.	Does the board ensure that any discussion around strategy considers the full range of key risks that the organisation is exposed to?	❑	❑
45.	Is risk monitoring and review integrated with strategic planning, performance management, budgeting, and other management processes?	❑	❑