The Institute of Internal Auditors Australia

The 20 Critical Questions Series

What Directors should ask of Risk Management

Risk management foundations

1. Does the organisation have (a) risk management framework aligned to an appropriate standard such as ISO 31000:2018 'Risk management – Guidelines' (b) defined risk appetite ideally encapsulated in a risk appetite statement? Are these endorsed by the audit or risk committee and approved by the board of directors?
2. Is there (a) a charter or terms of reference for the risk management activity (b) a risk management policy that assigns primary responsibility for risk management to operational managers? Are these endorsed by the audit or risk committee and approved by the board of directors?
3. Are there approved critical success factors or performance measures (KPIs) for the risk management activity?
4. Is there a risk management activity effectively positioned within the organisation in the 2nd line of defence that is independent of business operations?
5. Is there a specified person in the organisation such as a chief risk officer responsible for providing risk management expertise and co-ordinating risk considerations? Does this person have appropriate risk management qualifications? Does the risk management activity comprise of skilled and suitably qualified specialists rather than generalists? Is there a network of risk co-ordinators in business units across the organisation that provide a conduit between the risk management activity and the business unit (this will gernerally be a small part of a person's role)?
6. Is the organisation conforming with its chosen standard such as ISO 31000:2018 'Risk management – Guidelines'? Is the organisation consistently applying the approved risk management process across the organisation? Does this include risk assessments performed by external consultants and contract project managers? Does this extend to subsidiaries, and controlled and associated entities?
7. Is there an awareness program to assure people inside and outside the organisation know their risk management obligations including in relation to risk appetite? Is this reflected (a) internally – job descriptions, performance measures, etc (b) externally – tenders, contracts, etc?
8. Is risk management integrated with organisational activities including (a) strategic planning (b) operational business planning (c) project planning (d) ongoing operations (e) performance measurement (f) performance reporting?
9. Does the risk management and risk reporting process ensure risk appetite is a key focus of decision-making at all levels of the organisation?
10. Does the approach to risk management include various approaches to management of risk (a) Avoid – don't do it (b) Reduce – change likelihood, change consequence if possible (c) Share – insurance, partnership (d) Retain – accept?
11. Is there an annual risk management review plan approved by the audit or risk committee that aims to assure (a) risk management obligations regarding risk appetite are met (b) there is

What Directors should ask of Risk Management

continuous focus on enhancing risk management capability and effectiveness?

Risk assessment

12. Has a strategic high-level risk assessment been conducted for the organisation? Has this been encapsulated in a manageable number of strategic risks that are regularly monitored by management, audit or risk committee and board of directors in the execution of corporate strategy?
13. Have business unit risk assessments been conducted where appropriate? Have these been encapsulated in manageable business unit records that are used by management to manage and monitor operations?
14. Are risk assessments conducted for major projects and business initiatives to identify uncertainties and their implications whether they be good or bad? Are these encapsulated in manageable project documents used by management, audit or risk committee and board of directors to oversee delivery of projects and business initiatives?
15. Are proposed responses to risk recorded, allocated to appropriate management for implementation and regularly followed-up?

Risk registers

16. Is management of identified risks contained in risk registers assigned to specific managers with documented timelines for completion? Are there regular reports to management, audit or risk committee and board of directors on progress of risk remediation activities? Are hard questions asked and management held to account when risk remediation is not completed in a timely way?
17. Are records of risks regularly reviewed and updated to reflect changes to risk severity? Does this include records for (a) strategic (b) business operations (c) projects?

Review

18. Is there a process to ensure the risk management policy and framework is periodically reviewed and maintained up-to-date? Does this include regular review of the approved risk appetite? Are results reported to executive management and the audit or risk committee?
19. Are risk management results regularly reported to executive management, audit or risk committee and board of directors? Does this include executive management sign-off each year that the organisation is adequately managing risks? Is there a risk management annual report that contains performance measure results and an attestation statement from the risk management activity?
20. Is there periodic independent review of risk management for example by internal audit that is reported to management and the audit or risk committee?

The killer question

How does management, audit or risk committee and board of directors clearly know the organisation has identified and is effectively managing its risks in a timely way?