



19 Questions Senior Officers and Members Should Ask About Risk

About this document

We have developed these questions as a way for senior management, Directors and elected members to ask themselves about risk and the way in which it is implemented in their organisations.

This is not intended to be a full treatise on Risk Management, but an easy to follow and use aide memoire to provoke conversations about risk and risk taking within the organisation.

Members' or directors' roles include asking management tough questions to assure themselves that risk has been fully considered in the strategic and business planning processes. This document poses suggested questions for Boards or Cabinets to ask the Chief Executive, senior management, and itself. For each question we have included some explanation and some recommendations. We hope that directors, senior officers and Chief Executives will find it useful in assessing their present approach to the governance of risk and enhancing it where appropriate.

Directors, Members and Risk

Boards or Cabinets are now being held increasingly accountable for participating in the development of their organisation's strategic direction, approving it and ensuring that appropriate processes and controls are in place to identify, manage and monitor the business risks that follow from their organisation's business strategy.

Board's or Cabinet's role in strategic planning and the monitoring of risks must recognise that directors and members are not there to manage the business, but are responsible for leading management and holding it to account. Where the lines are clear, and roles are respected, effective Boards or Cabinets will contribute to the development of strategic direction and approve a strategic plan. They will oversee the processes that management has in place to identify business opportunities and threats. They will consider the extent and types of risk that it is acceptable for the organisation to bear. They will monitor management's systems and processes for managing the broad range of business risk. And most importantly, on an ongoing basis, they will review with management how the strategic environment is changing, what key business risks and opportunities are appearing, how they are being managed and what, if any, modifications in strategic direction should be adopted.

There is no single process that works for every Board or Cabinet and every organisation. In our view, it is the joint responsibility of the "independent Board or Cabinet leader" and the Chief Executive to develop ways to involve the Board or Cabinet in the ongoing processes of strategic planning and risk management that are constructive and appropriate to the circumstances of the organisation.



Risk management theory and practice have evolved considerably in recent years and continue to do so. One of the biggest changes has been the development by larger organisations of a coordinated or integrated approach to risk management often described as Strategic Risk Management, or "Enterprise Risk Management" (ERM). The basis of ERM is that every part of an organisation is responsible for managing risks in its own area of business activity using processes and guidance provided by a centralised risk management coordinator. Some larger organisations appoint a Risk Manager or other senior executive. Others have risk management committees or other coordinating mechanisms.

Asking questions is only the first step. Directors and members must satisfy themselves that the answers are appropriate and that risks are properly identified and managed. They pay close attention to documents and information from management, and then test what they learned against their own personal observations, experience, general knowledge and good sense. They also respect their experienced-based intuition that warns them that something's wrong. Intuition alone isn't enough to challenge answers, but it's valuable if it gets people's attention and prompts them to ask more probing questions.

Risk management can be a complex process but the basic concepts are very simple.

- What do you want to achieve?
- What can stop you from doing it?
 - How big is it?
 - How likely is it?
- What do you do about it?
- How do you know it's made a difference?

There are really just four choices of risk management strategy – the "what do you do about it" bit:

- Avoiding risk by choosing not to undertake certain types of activity
- Transferring risk to third parties through insurance, outsourcing, etc.
- Mitigating risk through preventive, detective or contingency control measures
- Accepting risk, recognising that the benefits of doing so outweigh the costs of transfer or mitigation.

Board or Cabinet members will find it useful to bear this in mind when asking the questions and assessing the answers. The questions in this document are intended to help Board or Cabinets work with senior management to develop practical ways to monitor and assess the organisation's processes for identifying and managing its business risks. With each question there is a brief discussion that provides background on the reasons for asking the question and the risk management objectives. Following the discussions are several "recommended practices" based on the current application of Enterprise Risk Management in leading organisations. The practices do not necessarily reflect current practice or the right answer for every organisation. Rather, they provide pointers to help Board or Cabinets guide and focus their discussion with the Chief Executive and the management team. The important consideration is not "Do we follow these practices?" but "Do our practices achieve the same risk management objectives?"

Strategic Planning and Risk

Board or Cabinets are responsible for approving the overall strategic direction of their organisation. As part of the planning process, Board or Cabinets must clearly understand their organisation's current business strategy, its critical success factors and the related business risks.



Effective Board or Cabinets actively participate with the Chief Executive and senior management in setting the overall strategic direction of their organisation and approving its strategic plan. They oversee the processes and controls that management has in place to identify and manage business risks. They actively review the potential impact of these business risks on the achievement of organisation's strategic objectives. And, after careful consideration of the opportunities and risks, the Board or Cabinet determines the nature and extent of business risks that are acceptable for the organisation to bear.

THE QUESTIONS

Strategic Planning and Risk: identifying, analysing and assessing business risks and opportunities

1. How do we integrate risk management with the corporation's strategic direction and plan?
2. What are our principal business risks?
3. Are we taking the right amount of risk?

Risk Management Processes: designing and implementing strategies for managing business risks

4. How effective is our process for identifying, assessing and managing business risks?
5. How do we ensure that risk management is an integral part of the planning and day-to-day operations of individual business units?
6. How do we ensure that the Board or Cabinet's expectations for risk management are communicated to and followed by the employees in the organisation?
7. How do we ensure that our executives and employees act in the best interests of this organisation?
8. How is risk management coordinated across the organisation?

Risk Monitoring and Reporting: implementing processes to monitor and communicate business risks.

9. How do we ensure that the organisation is performing according to the business plan and within appropriate risk tolerance limits?
10. How do we monitor and evaluate changes in the external environment and their impact on the organisation's strategy and risk management practices?

11. What information about the risks facing the organisation does the Board or Cabinet get to help it fulfil its stewardship and governance responsibilities?
12. How do we know that the information the Board or Cabinet gets on risk management is accurate and reliable?
13. How do we decide what information on risks we should publish?
14. How do we take advantage of the organisational learning that results from the risk management programme and activities?

The following questions are primarily directed at the Board or Cabinet itself and may be more appropriate for discussion among the directors or members.

15. What are our priorities as a Board or Cabinet in the oversight of risk management?
16. How does the Board or Cabinet handle its responsibility for the oversight of opportunities and risks?
17. How does the Board or Cabinet ensure that at least some of its members have the requisite knowledge and experience in risk?
18. How do we, as a Board or Cabinet, help establish the "tone at the top" that reinforces the organisation's values and promotes a "risk aware culture"?
19. How satisfied are we that the Board or Cabinet is doing what it should in overseeing risk?



1. How do we integrate risk management with the corporation's strategic direction and plan?

An organisation's strategy leverages its physical, financial, intellectual, and technological resources to gain and sustain a competitive advantage in the market place or to deliver competitive services. Implementing a strategic plan often includes venturing into new and profitable business opportunities, discontinuing unprofitable ones and solidifying its other business operations. Managing the associated risks involves considering the financial viability of new initiatives and investments, as well as assessing the implications of internal and external opportunities and threats for the organisation as a whole.

Recommended practices:

The Board or Cabinet contributes to the development of strategic direction and approves the strategic plan with a thorough understanding of the business risks that may affect the achievement of the strategic objectives.

The strategic planning process takes into account the organisation's core competencies, its goals and objectives and the strengths, weaknesses, opportunities and threats faced by the organisation. The strategic planning process also takes into account forecasts and assumptions made by the management team. Risk management activities are integrated with the development and implementation of the organisation's strategic plan.

Key performance targets are based on active consideration of the tradeoffs between threat and opportunity – both of which are components of risk. Strategic and operating plans are not just based on best-case scenarios but include an active consideration of a range of scenarios that includes the worst-case.

2. What are our principal business risks?

Most organisations face a number of "principal business risks" that are critical to their success, survival and strategy. It is important that directors know and understand what these major risks are and that management provides the Board or Cabinet with regular documentation on them – perhaps in the form of a risk register.

A major contributor or potential risk to an organisation's success is the calibre of the people who work for it. Good people with the appropriate resources are more likely to get results than a team with limited talent or means.

Recommended practices:

The Board or Cabinet ensures that management has a structured process for identifying, monitoring and managing the organisation's business risks and providing regularly scheduled documents to the Board or Cabinet. Strategic planning includes considering a range of scenarios (including the worst-case) for major changes in economy, environment, prices, catastrophic events and other principal business risks.

3. Are we taking the right amount of risk?

Risk taking is closely related to an organisation's values and the expectations of its owners or key stakeholders. It is important that the Board or Cabinet and management have a common understanding of their risk tolerance levels and base them on the organisation's appetite and capacity for risk. The Board or Cabinet and management should appropriately balance "value protection" with "value creation", when agreeing upon the organisation's overall risk tolerance levels.

There is a continuum of risk taking that runs from day-to-day risk routine tasks such as bidding on or procuring major contracts, making individual investment decisions, etc., to major new investments and initiatives that change the strategic direction of the organisation. The Board or Cabinet should be satisfied that the organisation has processes to ensure that all risk-related decisions are properly made. However, the Board or Cabinet must be directly involved in major decisions and should ensure that the associated risks receive the weight they deserve.

Organisations with a large appetite for risk pursue opportunities that could pay off handsomely — or fail to repay the investment. Other organisations may have a smaller appetite for risk and place a higher value on preservation of reputation and service delivery. The capacity to take risk is also related to the organisation's financial position and the scale of investment in proposed ventures. Successful



organisations understand risk tolerance and take risks intelligently.

Recommended practices:

The strategic planning process takes into account the organisation's appetite and capacity for risk and uses techniques such as risk and sensitivity analysis to determine its exposure to risk. The impact of individual risks is minimised, where cost effective, by the use of specific risk management techniques such as insurance or outsourcing, which address timing and financial factors.

Organisations might measure their risk tolerance in terms of; reputation, financial exposure, danger to life and limb and operational or service delivery. Wise organisations will set their risk tolerance levels for each of these areas, and might have corporate thresholds of risk tolerance as well as departmental thresholds so that risks at departmental level that exceed the threshold at that level can be escalated to the corporate level.

There are clearly defined processes in place for setting, approving, monitoring, and communicating risk tolerance levels for all major types of risks and ensuring that business strategies are compatible with them. The Board or Cabinet knowledgeably approves the broad risk tolerance limits for the organisation along with the types of risks that it can or cannot take.

Risk tolerance levels are regularly reviewed and adjusted to current external conditions, and the financial capacity and current objectives of the organisation. There are processes to ensure that people in the organisation operate within the risk tolerance levels approved by the Board or Cabinet.

4. How effective is our process for identifying, assessing and managing business risks?

Board or Cabinets need not be familiar with the many individual risks that face their organisation, but they must be satisfied that it has comprehensive and effective risk management processes and that major risks are escalated to them for consideration.

Identifying, assessing, and managing the risks that an organisation faces can be a complex and challenging job. There are, however, a number of

techniques and guidelines that can save time and help identify, assess and manage business risks. The objectives of identifying, assessing and managing risk are valid for every organisation. The processes and practices they adopt will depend on their size, nature and complexity.

Recommended practices:

The Board or Cabinet ensures that the organisation has:

- A well-defined process for categorising risks that covers strategic, operational and corporate reporting risks – both financial and non-financial. The classification framework is developed in sufficient detail to enable management to use it as the basis for establishing and maintaining risk management policies and processes.
- A well defined risk management framework that clearly identifies and records the principal risk factors for the organisation's specific businesses, objectives, processes and activities.
- A well defined and executed escalation process for risks that are critical to the organisation as a whole so that these risks are actively considered and actioned at Board or Cabinet level.

5. How do we ensure that risk management is an integral part of the planning and day-to-day operations of individual business units?

Organisations need to provide clear direction and a consistent language on risk management to ensure consistent performance. Consideration of business risk should be a regular part of day-to-day operations rather than something that employees need to pay attention to separately.

Recommended practices:

There should be a comprehensive and well articulated set of risk management policies (including thresholds for acceptable levels of risk) and programmes, appropriate approvals and regular reviews to ensure ongoing relevance.

Business unit managers integrate risk management activities with business strategies and the business unit/function planning process that produces the budget and includes their performance targets. Business plans at all levels of the organisation identify business risks and opportunities and



incorporate the appropriate level of resources for managing risk.

6. How do we ensure that the Board or Cabinet's expectations for risk management are communicated to and followed by the employees in the organisation?

Strategies are more likely to succeed if everyone in the organisation knows what they are and how to contribute to achieving them. Board or Cabinets should ensure that there are processes in place to communicate a consistent message.

Recommended practices:

The organisation has a programme of communication and training on risk that includes creating awareness of risk, promoting a risk-aware culture, and providing guidelines on policies and procedures for individual employees.

Risk awareness and culture in the business units and functions are regularly monitored using such techniques as internal audit reviews, risk and control self assessment workshops and employee surveys.

7. How do we ensure that our executives and employees act in the best interests of this organisation and its stakeholders?

The Chief Executive is responsible for ensuring that the conduct of senior executives and other employees is appropriate and can withstand public scrutiny. The challenge is to act ethically while striving to meet the goals of maximising value and achieving performance targets. This requires that the people concerned have a common understanding of what it means to act in the best interests of the stakeholders and the organisation. It also means that employees are compensated and rewarded for actions that benefit the organisation and its stakeholders.

Recommended practices:

The organisation has a written Code of Conduct, reviews it annually and requires key employees to provide a signed annual statement of compliance. The Chief Executive monitors the actions of senior executives and acts on breaches of the Code. The corporation's compensation and reward systems explicitly recognise positive actions and success by senior executives in achieving targets for managing

principal business risks. The systems also recognise and respond to failures to effectively manage risks.

Corporate executives establish the risk management "tone at the top" and demonstrate leadership by setting an example for others to follow.

8. How is risk management coordinated across the organisation?

Every business unit in an organisation plays some part in risk management. In most cases, the managers and staff are responsible for the risks directly related to their day-to-day activities. There may also be specialists who handle specific aspects of risk such as insurance, health and safety and environment. The Chief Executive must make sure that all the risk management activities are coordinated and that no major risk is overlooked.

Recommended practices:

The organisation's strategic and operational planning processes coordinate the risk management processes of line management and the departments that specialise in specific risks.

Larger organisations may have a designated Risk Manager or other senior executive reporting through the Chief Executive to the Board or Cabinet of directors who is responsible for coordinating risk management across the organisation.

Risk Monitoring and Reporting

The Board or Cabinet's oversight role includes reviewing regular and timely information about the organisation's performance and the risks that could affect the achievement of its strategic and business objectives.

9. How do we ensure that the organisation is performing according to the business plan and within appropriate risk tolerance limits?

Monitoring performance against key targets is an essential business practice. Board or Cabinets need assurance that management at all levels does this and should understand in general terms what procedures are in place. This means that the organisation has appropriate mechanisms to ensure that it is achieving its business objectives and related targets without taking undue risks.



Recommended practices:

The corporate information systems incorporate reports on key performance targets and related risk factors. Managers throughout the organisation receive regular reports on performance and provide explanations of variances and planned corrective action.

10. How do we monitor and evaluate changes in the external environment and their impact on the organisation's strategy and risk management practices?

Strategic plans incorporate assumptions about factors in the external world that can change at any time and significantly affect the business plan. Some factors are relatively easy to monitor – exchange rates, commodity prices, interest rates, etc. Others, such as political, regulatory and social trends are harder to quantify and assess.

Recommended practices:

There are processes for identifying and monitoring changes in the external environment and responding as appropriate. There is clearly assigned responsibility for collecting and sharing information on the external environment.

The Board or Cabinet reviews with management how the strategic environment is changing, what key business risks and opportunities are appearing, how they are being managed and what, if any, modifications in strategic direction should be adopted.

11. What information about the risks facing the organisation does the Board or Cabinet get to help it fulfil its stewardship and governance responsibilities?

Board or Cabinet time is limited and agendas tend to be full so risk reporting should be focused and scheduled. Since strategy and risks are closely intertwined, the Board or Cabinet should allocate sufficient time to review and discuss all the risk related issues.

Recommended practices:

The Board or Cabinet's agenda planning includes regularly scheduled documents to the Board or Cabinet or designated committees on the following areas;

- Events and trends that impact strategic plans, principal business risks or the continued validity of underlying assumptions.

Briefing material should include the results of sensitivity analysis that show the range of probable financial and other outcomes.

The Board or Cabinet can then exercise oversight over the adjustment of plans in order to take advantage of new or changed opportunities and risks.

- Specific operational risks, with presentations by the managers responsible for key functions such as finance, internal audit, human resources, health and safety, credit, legal, production, research and development, and environmental protection.
- Preparedness for predictable emergencies such as the sudden death or incapacity of the Chief Executive, major fire, extensive product recall, facility failure, natural disasters, and terrorism.

Management provides prompt documents to the Board or Cabinet on:

1. Incidents that have significant financial implications or the potential to damage the organisation's reputation, for example by causing injury or death. Such incidents can be addressed in a timely telephone conference call and followed-up at the next regularly scheduled Board or Cabinet meeting, along with the actions taken and the lessons learned and an estimate of value lost.
2. Serious breaches of the Code of Conduct. When the Board or Cabinet is called upon to approve a specific proposal or action the Board or Cabinet receives a balanced picture with information about:
3. The potential risks as well as the potential opportunities
4. The alternatives that were rejected as well as the proposal being advanced
5. The worst-case scenario



6. Management's apprehensions and uncertainties as well as its optimistic expectations.

The information derived from the analysis above can be recorded in a risk register or series of linked risk registers.

12. How do we know that the information the Board or Cabinet gets on risk management is accurate and reliable?

Board or Cabinets rely on management for much of the information they get on risk and need assurance that it is complete and accurate. This typically involves a combination of formal reports and opportunities to meet and hear from a number of sources in addition to the Chief Executive. Regardless of the source, Board or Cabinet members should demonstrate healthy scepticism and ask themselves if the information they get is consistent and rings true.

Recommended practices:

The Board or Cabinet gets information from a cross-section of knowledgeable and reliable sources in addition to the Chief Executive, such as executive and financial management, internal and external auditors and external advisors.

The Board or Cabinet periodically requests a formal review and report on the effectiveness of the risk management process from an objective and independent source outside of senior management (e.g. internal audit, external auditor, consultant, etc.).

13. How do we decide what information on risks we should publish?

Board or Cabinets are responsible for overseeing their organisations' external reporting and should be aware of any applicable legal requirements for the contents and approval of annual and other reports such as the Freedom of Information Act. The requirements for including information on risk and controls in annual reports and other external communications depend on legislation and regulations that continue to evolve.

Recommended practices:

In addition to a report on principal business risks the annual report should include a statement of corporate governance practices that describes the Board or

Cabinet's governance role in the area of strategy and risk.

The Board or Cabinet obtains timely documents to confirm that public disclosures meet current reporting requirements.

14. How do we take advantage of the organisational learning that results from the risk management programme and activities?

Organisations that analyse their response to crises, problems and successes can profit from their experience, if they take advantage of the opportunities they identify.

Recommended practices:

The Board or Cabinet ensures that:

- Management promptly reviews the most significant lessons learned from each major business event, surprise and disaster and how it has responded to these findings
- Management has a process for reviewing the organisation's response to crises and takes action to improve the handling of similar events in the future.
- Management has put in place effective knowledge transfer processes, so that significant findings and lessons learned (both positive and negative) can be transferred quickly and effectively across the organisation.

Board or Cabinet effectiveness

The Board or Cabinet should take time to define its role in risk management. It should make sure it is organised to meet its responsibilities for ensuring that the corporation's risk management policies and programmes contribute to sustainable value creation for the owners and other stakeholders.

15. What are our priorities as a Board or Cabinet in the oversight of risk management?

The Board or Cabinet must decide how to make best use of its limited time for overseeing risk.

Recommended practices:

The Board or Cabinet establishes its priorities and determines the scope, depth and timing of its involvement in risk management. This decision may take into account:



- The nature and status of the organisation, the business it is in, how long it has existed, etc.
- The Board or Cabinet's level of trust and confidence in the Chief Executive
- The degree and rate of change in the industry and other aspects of the external world
- The extent to which the organisation needs to change its strategy to anticipate and respond to external opportunities and threats
- The effectiveness of the structures and processes that the Board or Cabinet has established to handle its responsibility for oversight of opportunities and risks.

16. How does the Board or Cabinet handle its responsibility for the oversight of opportunities and threats?

Wherever possible, the entire Board or Cabinet should participate in the oversight of risk. Because some areas of risk management have technical aspects that can be complex and time consuming to review, Board or Cabinets may delegate the detailed work of overseeing certain aspects of risk to one or more committees such as the audit committee. In such cases, the Board or Cabinet must make sure that it is fully informed of the findings of the committees and that no significant aspect of risk is overlooked, and that the significant risks to the business are regularly and actively reviewed at top level.

Recommended practices:

The Board or Cabinet and its committees have written policies and procedures on governance issues related to risk. Where the Board or Cabinet elects to delegate specific risk-related responsibilities to Board or Cabinet committees, the committees are required to report their activities to the full Board or Cabinet at least annually. Key risks are actively considered and actioned at top level.

17. How does the Board or Cabinet ensure that at least some of its members have the requisite knowledge and experience in risk?

Stock exchanges, institutional investors and other regulatory bodies are increasingly demanding that Board or Cabinets include directors who understand the organisation's business and its inherent risks.

Recommended practices:

The Board or Cabinet's nominating practices recognise the need to include directors who are familiar with a broad range of risks, including those that are specific to the organisation's industry. The Board or Cabinet takes steps to raise the awareness and understanding of risk among directors by:

- Scheduling educational sessions on risk issues and processes
- Using internal and external experts to advise the Board or Cabinet and committees on specific risk issues.

18. How do we, as a Board or Cabinet, help establish the "tone at the top" that reinforces the organisation's values and promotes a "risk aware culture"?

Effective Board or Cabinets play an active role in reinforcing an organisation's approach to risk taking and risk management. They do so when they participate actively and lead by example. The biggest challenges in developing strategy and identifying risks are denial and unwillingness to think the unthinkable. Most people are reluctant to contemplate the possibility of major stock market crashes, executive fraud, war or terrorist acts. Chief Executives are often optimists who may discount the risk of failure or loss. Directors can contribute to discussions of strategy and risk by providing a tough-minded "reality check."

Recommended practices:

The Board or Cabinet plays an active role in discussions of strategy and risk and asks tough questions that challenge assumptions and focus on the interests of owners and other key stakeholders.

The Board or Cabinet's actions are compatible with and reinforce the organisation's stated objectives, values and risk tolerance in such areas as:

- The choice of Chief Executive
- The selection of directors
- The strategic plan
- The code of conduct
- Executive compensation

The inclusion of risk management issues as regularly scheduled Board or Cabinet agenda items

The Board or Cabinet reviews and approves the compensation package for the Chief Executive and senior executives.



19. How satisfied are we that the Board or Cabinet is doing what it should in overseeing risk?

Effective risk management integrates and coordinates the activities of people across the organisation through strategic planning, organisational culture, and policies and procedures. The Board or Cabinet is typically involved with committees, reports, presentations and discussions, each of which complements the overall process of

risk oversight. Board or Cabinets need to take time to satisfy themselves that all the pieces are coordinated and collectively support a conclusion that risk is properly managed and that the Board or Cabinet has fulfilled its stewardship obligations.

Recommended practices:

The Board or Cabinet regularly schedules time to assess how effective it has been in meeting its responsibilities for the oversight of risk and what corrective action it needs to take.

LIZ TAYLOR RISK CONSULTING

PO Box 340
Newton Abbot
Devon TQ12 5ZX
e: info@liztaylorriskconsulting.co.uk
t: 01626 337626
f: 01626 330557

