The Orange Book
Management of Risk – Principles and Concepts
A High-Level Summary
Introduction

In successful organisations, risk management enhances strategic planning and prioritisation, assists in achieving objectives and strengthens the ability to be agile to respond to the challenges faced. If we are serious about meeting objectives successfully, improving service delivery and achieving value for money, risk management must be an essential and integral part of planning and decision-making.

Public sector organisations cannot be risk averse and be successful. Effective and meaningful risk management in government remains as important as ever in taking a balanced view to managing opportunity and risk. It must be an integral part of informed decision-making; from policy or project inception through implementation to the everyday delivery of public services.

As an integrated part of our management systems, and through the normal flow of information, an organisation’s risk management framework harnesses the activities that identify and manage the uncertainties faced and systematically anticipate and prepare successful responses. Its importance and value to success should not be underestimated.

As with all aspects of good governance, the effectiveness of risk management depends on the individuals responsible for operating the systems put in place. Our risk culture must embrace openness, support transparency, welcome constructive challenge and promote collaboration, consultation and co-operation. We must invite scrutiny and embrace expertise to inform decision-making. We must also invest in the necessary capabilities and seek to continually learn from experience.

Purpose

This document provides a summary of The Orange Book: Management of Risk – Principles and Concepts. The full version sets out the main and supporting principles for risk management in government.

In considering the effectiveness of risk management arrangements, assessing compliance with Corporate Governance Code requirements, and overseeing the preparation of the governance statement, the board should consider adherence with the main principles set out in both documents, and use the supporting principles in the full version to inform their judgements.
The risk management framework supports the consistent and robust identification and management of opportunities and risks within desired levels across an organisation, supporting openness, challenge, innovation and excellence in the achievement of objectives. For the risk management framework to be considered effective, the following principles shall be applied:

A. Risk management shall be an essential part of governance and leadership, and fundamental to how the organisation is directed, managed and controlled at all levels.

B. Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.

C. Risk management shall be collaborative and informed by the best available information.

D. Risk management processes shall be structured to include:
   a. risk identification and assessment to determine and prioritise how the risks should be managed;
   b. the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
   c. the design and operation of integrated, insightful and informative risk monitoring; and
   d. timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

E. Risk management shall be continually improved through learning and experience.
A. Risk management shall be an essential part of governance and leadership, and fundamental to how the organisation is directed, managed and controlled at all levels.

The desired risk culture should be communicated, embedded at all levels and periodically assessed.

Human resource policies and performance systems should encourage and support desired risk behaviours and discourage inappropriate risk behaviours.

A strategic choice should be made about the style, shape and quality of risk management, which should be periodically reviewed to ensure it remains appropriate.

The nature and extent of the principal risks that the organisation is willing to take in achieving its objectives – its risk appetite – should be determined and communicated.

Risk information and insights should support informed decision-making in line with the risk appetite, ensure confidence in the response to risks and ensure transparency over the principal risks faced and how these are managed.

Authority, responsibility and accountability for risk management and internal control should be defined, co-ordinated and documented throughout the organisation. The ‘three lines of defence model’ provides a systematic approach that may be used to help clarify the specific roles and responsibilities that are necessary for the effective management of risks within an organisation.

The designated individual responsible for leading the overall approach to risk management should be positioned and supported to allow them to exercise their objectivity and to influence effective decision-making.

The necessary resources, skills, knowledge and experience for risk management should be assessed and supported.

Continual commitment to risk management should be demonstrated.
B. Risk management shall be an integral part of all organisational activities to support decision-making in achieving objectives.

Risk should be considered when setting and changing strategy and priorities, managing performance and delivering improvement.

Risks should be transparently assessed within the appraisal of options for policies, programmes and projects or other significant commitments.

Emerging risks should be identified and considered.

Risks to the public should be assessed and reflected within policy development and implementation.

National Risk Register risks that are particularly pertinent to the organisation should be recognised in risk assessments and discussions.

C. Risk management shall be collaborative and informed by the best available information.

There should be an aggregated view of the risk profile informed by consolidation of assessments across the organisation, arm’s length bodies and the extended enterprise.

The views of external stakeholders should be gathered and included within risk considerations.

Communication and consultation should assist stakeholders to understand the risks faced and the organisation’s response.

Expert functions should inform the identification, assessment and management of risks and the design and implementation of controls.
D. Risk management processes shall be structured to include:

a) risk identification and assessment of risks to determine and prioritise how the risks should be managed;

b) the selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;

c) the design and operation of integrated, insightful and informative risk monitoring; and

d) timely, accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.

Risk identification activities should produce an integrated and holistic view of risks.

Risk criteria should support consistent interpretation and application in assessing the level of risk.

Limitations and influences associated with the information and evidence used with risk assessments should be highlighted.

Exposures to risk should be assessed against the nature and extent of risks that the organisation is willing to take to determine where and what additional action is required.

Contingency arrangements for high impact risks should be designed and tested to support continuity, incident and crisis management and resilience.

Ongoing and continuous monitoring should support understanding of whether and how the risk profile is changing and the extent to which internal controls are operating as intended.

The nature, source, format and frequency of the information required to support monitoring of risk management and internal control should be defined and communicated.

New and changing principal risks should be highlighted and escalated clearly, easily and more rapidly when required.

E. Risk management shall be continually improved through learning and experience.

The organisation should continually monitor and adapt the risk management framework to address external and internal changes.

Policies, programmes and projects should be evaluated to inform learning from experience.

Risk management maturity should be periodically assessed to identify areas for improvement.

Improvement opportunities should be identified, prioritised, implemented and monitored.