

Queensland Audit Office

Better Practice Guide Risk Management

October 2007



© The State of Queensland. Queensland Audit Office (2007)

Copyright protects this publication except for purposes permitted by the Copyright Act. Reproduction by whatever means is prohibited without the prior written permission of the Auditor-General of Queensland. Reference to this document is permitted only with appropriate acknowledgement.

Queensland Audit Office
Central Plaza One
Floor 11, 345 Queen Street, Brisbane Qld 4000
GPO Box 1139, Brisbane Qld 4001
Telephone 07 3405 1100
Facsimile 07 3405 1111
Email enquiries@qao.qld.gov.au
Website www.qao.qld.gov.au

ISBN 978-0-9803585-3-7

Queensland Audit Office publications are available at www.qao.qld.gov.au or by phone on (07) 3405 1100

Contents

1.	Introduction	3
2.	Overview of the critical elements of the risk management framework and processes	4
2.1	Risk management framework	4
2.2	Risk management processes.....	5
3.	Key principles	8
3.1	Embed risk management in corporate culture	8
3.2	Establish and review organisational context	10
3.3	An integrated risk management framework	11
3.4	Document, implement and review contemporary risk management framework	13
3.5	Risk management is a key element of governance	16
4.	Overview of existing risk management frameworks.....	19
4.1	Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004	19
4.2	‘Enterprise Risk Management – Integrated Framework’ – COSO 2004 (USA).....	21
4.3	The Orange Book – ‘Management of Risk – Principles and Concepts’ – HM Treasury 2004 (UK)	22
4.4	‘Integrated Risk Management Framework’ – Canadian Treasury Board 2001	23

1. Introduction

This guidance material has been developed based on the results of the performance management systems audit, Report to Parliament No. 6 for 2007 Beyond Agency Risk.

The document consists of three parts:

- the critical elements of an effective risk management framework and processes
- five key principles integral to effective risk management, each matched to consider points, benefits, and implementation suggestions
- an overview of existing global risk management frameworks applicable to both the public and private sectors.

Based on the audit findings and research undertaken, a set of five key principles integral to effective risk management have been identified. These key principles, on which a whole-of-government risk management framework should be developed, are:

Embed risk management in corporate culture	Executive and senior management develop and foster a culture committed to risk management and drive integrated risk management.
Establish and review organisational context	Organisations establish and regularly review the context in which they operate. This includes defining the organisation's risk appetite and tolerance before developing or adopting a risk framework best suited to the organisation.
An integrated risk management framework	Risk management is integrated into planning, decision-making and reporting processes at each level and function of the organisation.
Document, implement and review contemporary risk management framework	Organisations ensure all elements and process steps of the risk management framework are documented, implemented and operating effectively .
Risk management is a key element of governance	Organisations put strong governance arrangements in place to ensure effective accountability of risk management framework and strategies.

The key principles are purposely broad as they are applicable at all levels of the organisation.

Note: Organisation, in the context of this guidance material, is to be understood as being the government, the portfolio or the agency depending on the reader's perspective and focus.

2. Overview of the critical elements of the risk management framework and processes

2.1 Risk management framework

To be effective, a whole-of-government risk management framework should provide detailed guidance and clearly outline the systems which agencies should be implementing as well as their performance expectations. It should:

- clearly articulate the government policy, approach and attitude on risk management
- define the framework requirements to implement
- define the mechanisms to manage beyond agency risks, including the communication process to escalate and report on risks
- outline the respective roles of central and line agencies
- describe accountability and governance mechanisms, including the role of the board of management, executive and senior management, and the risk management committee.

Such a system would provide for more comprehensive information to aid in government decision-making, as well as increase the opportunity for government to proactively manage risks, as opposed to reacting to events after they occur.

Other benefits include establishing a common understanding and approach to risk management across the public sector, thus enabling comparison, benchmarking and coordinated reporting.

Due care and consideration should be exercised when developing the whole-of-government framework to ensure it does not become another compliance exercise. For the framework to deliver benefits in the strategic decision-making process, it is vital that executive and senior management are involved and committed to the process.

It is essential that the whole-of-government framework be adopted and supported by the government, central and line agencies equally, as all have an important role to play. Effective integrated risk management can only be achieved in organisations where there is active commitment from the top down.

Central agencies should take a lead role in the coordination, management, reporting and monitoring of whole-of-government risks, as well as encourage and support developing risk management skills and competencies in the public sector. Central agencies should also promote the importance and benefits of effective integrated risk management across government.

Central agencies play a role in normalising risk management across agencies and ensuring sector-wide communication to share risk management information across all portfolios. They should consider integrating risk management reporting to existing frameworks and reporting arrangements to maximise leverage. For example, quarterly performance reporting to the Cabinet Budget Review Committee (CBRC), annual report requirements, strategic and business plan implementation cycles and mid-year budget review.

When identifying, analysing, treating and monitoring risks, line agencies should give appropriate consideration to the broader public sector context and see themselves as part of the State of Queensland. Line agencies should also ensure that adequate professional resources are allocated to risk management.

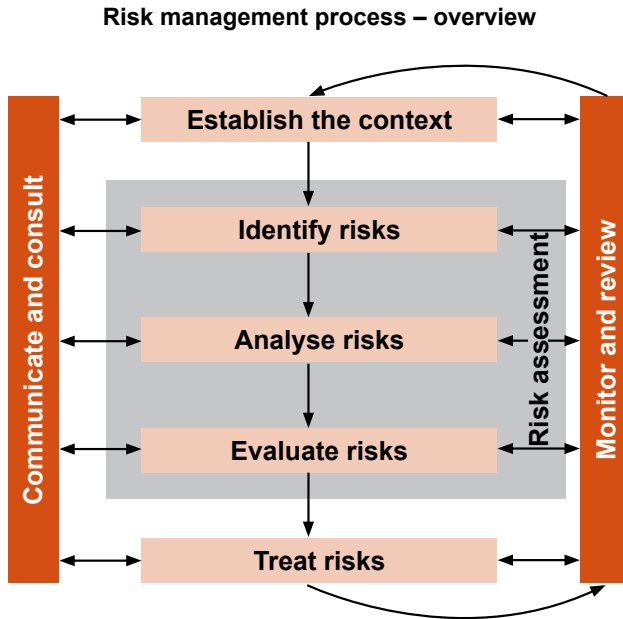
No matter which framework is adopted or developed, it needs to be flexible enough to suit the complexity of the organisation, in this case the public sector. The framework also needs to recognise that entities within the same organisation, while all contributing to the corporate objectives, operate in different environments and deliver different outputs.

2.2 Risk management processes

Across the reviewed frameworks, including AS/NZS 4360:2004, there are several common elements, namely:

- integrated risk management is embedded within the organisation's corporate culture
- the framework is applied across the organisation at every level and function
- people at every level of the organisation are involved in risk management
- risk management is a continuous process consisting of several connected steps, including setting the context, identifying, assessing, addressing, reporting and monitoring risk

- all steps of the process are effectively implemented within the established framework
- communication underpins the entire risk management framework
- the risk management framework is periodically reviewed, assessed and updated to ensure continued relevance and application.



Source: *Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004, p9.*

It is worth noting the integrated risk management frameworks reviewed and discussed in Section 4 of this document are generic. They can be easily tailored to individual circumstances and applied at every level within any organisation, whether in the public, private or non-for-profit sector.

The set of key principles discussed in Section 3 have also been broadly formulated to be relevant and applicable to all levels and functions of the organisation.

Roles and responsibilities

Identified in the table below are key roles and responsibilities integral to effective whole-of-government risk management at the central and line agency levels.

Level	Roles and responsibilities
Central agency	<ul style="list-style-type: none"> ● Develop, maintain and promote a contemporary risk management framework for use across government. ● Provide mechanisms to manage inter-agency and whole-of-government risks, including the communication process to escalate risks. ● Monitor agency risk management functions to ensure a risk management framework is being implemented effectively. ● Integrate risk management into regular agency reporting activities. For example, quarterly performance reporting to CBRC, agency annual report requirements, strategic and business plan implementation cycles and mid-year budget review. ● Develop a risk management information system to store and aggregate risk management information. ● Collate and report on whole-of-government and shared risks across portfolios and agencies. ● Share risk management information across all agencies. ● Continual development of the Queensland public sector's risk management resources and competencies. ● Coordinate and normalise the comprehensive and coherent assessment of whole-of-government risk at the state level.
Line agency	<ul style="list-style-type: none"> ● Give appropriate consideration to broader public sector when setting context, identifying, analysing, treating and monitoring risks. ● Identify and escalate significant and whole-of-government risks to central agency level. ● Review and monitor risk management framework regularly to ensure relevance. ● Document and implement a contemporary risk management framework. ● Ensure each step and process of the agency's risk management framework is implemented. ● Integrate risk management into regular reporting and performance monitoring frameworks, as well as strategic and business planning models. ● Seek risk management contributions from all staff. ● Store risk management information. ● Share risk management information across all organisational functions and activities. ● Regularly report on risk management performance to central agency level. ● Continual development of the agency's risk management resources and competencies.

3. Key principles

3.1 Embed risk management in corporate culture

Executive and senior management develop and foster a **culture** committed to risk management and drive **integrated** risk management.

Consider points

- The degree to which risk management forms part of an organisation's corporate culture is highly dependant on the tone set from the top. For risk management to become securely embedded within an organisation's culture, a high level of leadership, support and involvement is required by senior management.
- Senior management need to openly promote and champion the economic, social and environmental benefits of an effective and disciplined risk management framework. In addition, senior management need to make significant resources available for the establishment, promotion and continuity of risk management.
- The inclusion of risk management in values, the identification/appointment of a risk management champion, and the provision of risk management training all assist in raising the understanding and profile of risk management across the organisation. This contributes to an organisation-wide understanding that the identification of potential risks, along with mitigation and controlling strategies, is a responsibility shared by all staff, regardless of title or function.
- Senior management and identified risk management champions are responsible for promoting the benefits of risk management at the strategic and operational levels of the organisation. Focusing on the positives of effective risk management reduces the chances of risk management being perceived as little more than a compliance exercise, and aids in managing any transition towards a more effective risk management framework.
- To retain the integrity of risk management processes, senior management need to be open to potentially adverse situations being brought to their attention, and ready to invest time, effort and funds to mitigate/control the identified risk. Without this honest and frank identification of potential risks, robust mitigation strategies may not be implemented.

- An organisational culture that understands and supports the needs and benefits of effective risk management is more likely to be proactive when identifying potential risks. An organisation-wide regime on risk management training and promotion can positively influence this.
- The integration of risk management into all existing organisational frameworks facilitates anchoring risk management to an organisation's culture.

Benefits

- Allocation of appropriate (number and quality) resources to risk management.
- Breaking down of intra-organisation silos.
- Increased identification of potential risks and appropriate mitigation strategies.
- All staff have a greater awareness of the motives for risk management and the organisational changes to mitigate risk. This greatly benefits the change management process.

Barriers

- Change process in relation to the implementation of risk management framework not handled effectively.
- Not all levels of the organisation engaged in risk management.
- Not all functions and activities of the organisation engaged in risk management.
- Information in relation to identified risks and mitigation strategies not stored and shared across the organisation.

Making it happen

- Appoint/identify risk management champion/s.
- Promote and champion risk management and the benefits of effective risk management across all levels and functions of the organisation (senior management, risk management champion, middle and first line management).
- Include risk management in corporate values.
- Provide regular and relevant risk management training and information to staff and management.

- Involve staff from all levels in the organisation in the roll-out of the risk management framework.
- Identify examples of risk management contributions that can be made by staff at different levels of the organisation, and the associated benefits/rewards.

3.2 Establish and review organisational context

Organisations establish and regularly review the **context** in which they operate. This includes defining the organisation's risk appetite and tolerance before developing or adopting a risk **framework** best suited to the organisation.

Consider points

- Examination of the strategic, operational and risk management contexts defines the basic parameters within which the risks are to be managed and sets the scope for the remainder of the risk management process. Staff from every organisational level and function need to be involved in this process.
- The process includes examining the organisation's operating environments, both internal and external (political, economic, social, technological, etc). This environmental examination needs to consider the organisation's mandate, objectives, mission and available resources. The steps undertaken should be documented to demonstrate that the full range of environmental and contextual factors have been considered.
- The level of risk exposure that is tolerable and justifiable needs to be documented, and risk criteria developed against which risks are to be evaluated. Some risks however are unavoidable and not within the organisation's ability to completely manage. Consideration needs to be given here to the need to balance the costs, benefits and opportunities.
- Part of establishing and reviewing the organisational context includes selecting the most appropriate risk management framework.
- The timeframes for periodically reviewing the organisational context need to be documented, promoted and controlled.

Benefits

- Increased awareness of organisation's internal and external operating environments.
- Clear criteria are established for how risk is to be identified.
- Selection of the most appropriate risk management framework.
- Consistent identification of risk across organisation.

Barriers

- Limited commitment from senior management.
- Narrow view of organisational environments throughout process.

Making it happen

- Involve staff from all levels and functions of the organisation.
- Document process to ensure all environmental and contextual factors have been considered.
- Consider the requirement to balance costs, benefits and opportunities.
- Select the most appropriate risk management framework.

3.3 An integrated risk management framework

Risk management is **integrated** into planning, decision-making and reporting processes at each level and function of the organisation.

Consider points

- It is no longer sufficient to manage corporate risk at the individual program, activity or functional level. In order for appropriate identification, mitigation, monitoring and controlling of corporate risks to take place, risk management needs to be present at each organisation level, across all organisational functions, and risk management information shared organisation-wide. Senior management has the responsibility to drive this.

“Integrated risk management does not focus only on the minimization or mitigation of risks, but also supports activities that foster innovation, so that the greatest returns can be achieved with acceptable results, costs and risks.”¹

¹ *Integrated Risk Management Framework* – Treasury Board of Canada, 2001, p10.

- The interdependence of organisational levels and functional silos is integral to an integrated risk management framework. Information is shared within an organisation both vertically, and horizontally across its various functions to ensure that a coordinated approach towards identifying and mitigating risks is able to take place. This aggregation at the corporate level adds significant value to priority setting and improved decision-making.
- The identification, monitoring, reporting and controlling of risks needs to form part of the organisation's regular reporting and performance monitoring frameworks. This is something that needs to be adopted consistently across the organisation.

Benefits

- Increased lateral interaction across the organisation breaks down departmental silos.
- Consistent, organisation-wide approach to risk management.
- Risks are identified and reviewed as part of normal planning and reporting cycles, leading to more proactive, rather than reactive risk management.
- Risk management that is conducted in conjunction with other corporate, strategic and operational management processes is more effective and economical.
- Awareness of risk management is more widely promoted across the organisation.

Barriers

- Limited commitment by senior management.
- Insufficient investment of resources committed to integration process.
- Limited aggregation and sharing of risk management information.
- Confusion between risk management and business continuity planning.

Making it happen

- Promote the benefits and rewards of risk management being present at each level, and across all functions of the organisation.
- Establish risk management processes within the organisation's regular planning, reporting and performance management frameworks.

- Store and share risk management information across the organisation.
- Identify common risks, and promote coordinated treatment strategies.
- Monitor identification and treatment of risks across the organisation to ensure risk management processes are being consistently applied.
- Use risk management information to aid informed decision-making and priority setting organisation-wide.

3.4 Document, implement and review contemporary risk management framework

Organisations ensure all **elements** and process steps of the risk management framework are documented, implemented and operating **effectively**.

Consider points

- Risk management increases in effectiveness when the risks to be managed, along with their controlling and mitigation strategies, are identified through a systematic, robust and properly structured process.
- Clear documentation and implementation of a risk management framework and its associated mechanisms leads to consistent integration with existing organisational frameworks and models, and contributes to the normalisation of risk management within an organisation’s regular activities. A risk management framework that is easily understood by all staff significantly aids in the communication and training associated with the framework’s implementation.
- There is no “one size fits all” framework able to be applied across all types and sizes of organisations. Consideration needs to be given by an organisation’s senior management to implement a framework that best integrates with its existing operations, reporting mechanisms, culture, workforce skills, budget and supporting infrastructure. The organisation’s operational context and external environment, inclusive of standards and legislative compliance obligations, also need to be considered.
- The chosen risk management framework needs to directly reflect an organisation’s tolerance and appetite for risk at the strategic, tactical and operational levels. The framework also needs to be vertically integrated into all levels of the organisation and applied equally across the entire breadth of the organisation’s various programs and functions.

- It is vital to the integrity of the organisation's risk management process that all elements of the selected risk management framework are implemented effectively, and each phase of the framework is undertaken regardless of the organisational function it is being applied to.
- The initial stages of each risk management framework include identifying risks. To get the greatest value, this process needs to be systematic and consider the broader view of adverse possibilities. Simply reviewing previously identified risks will not focus the required attention on new and emerging risks.
- The dynamic and continuously changing nature of corporate risks creates a requirement for the organisation's risk management framework to include regular reporting against and monitoring of identified risks, combined with an assessment of the effectiveness of their controlling and mitigation strategies. Regular review of the economic, social and environmental impacts of these strategies needs to be included as part of the process, and linked to formalised feedback and reporting loops.
- To realise the value of continual improvement in relation to managing organisational risks, the risk management framework needs to include a requirement for the regular review and update of the framework itself. This ensures that the framework is able to adapt, and remains valid throughout any changes endured by the organisation. Review and monitoring of the risk management process takes place continually at each stage of the risk management process.
- Ownership, promotion, documentation, storage and accessibility of the risk management framework is crucial to the identification and controlling of risks which may affect the organisation's triple bottom line. The greater the awareness and understanding of the risk management framework across the organisation's workforce, the greater the contributions by staff across the organisation, as well as the accuracy of its application.
- A risk management framework that centralises and shares information across all organisational levels, functions and activities can further aid through shared responsibility, treatment and cost of treating risks. Intra-organisational root causes of risks may also be removed as part of sharing risk management information across the organisation.

Benefits

- A holistic and comprehensive approach to risk management.
- A single document that can be referenced organisation-wide.
- Increased understanding across the organisation of the benefits of effective risk management.
- Greater consistency in the application of the risk management framework across the organisation.
- Greater consistency in the tolerance and appetite for risk across the organisation.
- Relevant, timely and comprehensive information available to aid in making better informed decisions at the strategic, tactical and operational levels.

Barriers

- Limited commitment towards risk management by senior management.
- Restricted knowledge of risk management across the organisation.
- Minimal resources committed towards the documentation and implementation of risk management.
- Limiting risk management focus to economic/financial risk only.
- Insufficient change management throughout the transition process.
- Only partial integration of risk management with existing planning, reporting and controlling functions.

Making it happen

- Clearly document the chosen risk management framework.
- Ensure the risk management framework is clearly understood, and that it is both easily and openly accessible to staff across all functions and levels of the organisation.
- Implement the chosen risk management framework, policies and systems.
- Promote the risk management framework and associated benefits to senior management, middle management and risk management champions.

- Involve staff from all levels and functions as part of the implementation strategy.
- Develop risk management learning plans and tools.
- Provide significant training in relation to risk management and the chosen framework across the organisation.
- Periodically review and modify the risk management framework where required to ensure continuity of relevance and applicability.

3.5 Risk management is a key element of governance

Organisations put strong **governance** arrangements in place to ensure effective **accountability** of risk management framework and strategies.

Consider points

- Governance is the process by which an organisation is directed and controlled. Integral to this process is the requirement to effectively identify and manage an organisation's many and varied risks.
- Most organisations already have extensive governance arrangements in place to best enable senior management to plan, organise and control organisational activities towards fulfilling its strategic intents. This periodic strategic, tactical and operational planning, combined with the organisation's regular internal and external reporting cycles all need to include elements of risk management.
- Having a properly documented risk management framework is the first step towards integrating risk management into an organisation's various governance regimes. This establishes organisational roles and responsibilities, risk management steps and activities to be taken, and their associated timeframes. Without this, there is no benchmark against which to regularly measure risk management activities and performance.
- Risk management control mechanisms integrated into existing organisational governance need to monitor and control two things:
 - All elements and steps of the risk management framework are correctly and effectively implemented, clear responsibility for each step has been identified, and the risk management framework has been applied at each level and across all functions of the organisation. This includes periodically reviewing the risk management framework itself.

- Monitoring and controlling identified risks forms part of regular internal and external reporting. This enables significant and emerging risks to be closely controlled, as well as escalated to the portfolio or whole-of-government level where required.

When risk management is integrated into existing organisational strategic, tactical and operational planning, and regular reporting cycles, the additional risk management information available enables better informed planning and decision-making at the organisational, portfolio and whole-of-government levels.

Benefits

- Ability to monitor and control organisational risk management performance.
- Additional confidence to all stakeholders.
- Clear risk management roles and responsibilities.
- Additional information which is able to be used for more informed strategic, tactical and operational planning.
- Increased ability to proactively rather than reactively manage adverse events and occurrences.

Barriers

- Risk management is perceived by staff as bolting-on an additional requirement to existing procedures.
- Risk management is perceived as a compliance driven exercise.
- A corporate culture that does not support risk management.
- A risk management framework that is not clearly documented and communicated.
- A risk management focus that is too operational, with risk information not being shared vertically and horizontally across the organisation.
- Limiting risk management focus to economic/financial risk only.

Making it happen

- The risk management framework needs to be clearly documented and implemented.
- The corporate culture needs to be supportive of risk management.

- Clear roles and responsibilities must be identified and communicated (e.g. appoint a risk management champion, consider risk management committee or additional responsibilities for audit committee).
- Merge risk management into existing organisational planning, reporting and controlling frameworks, (e.g. regular exception reporting, scorecards, snapshots).
- Clearly distinguish responsibilities of promoting risk management, identifying risks and ownership of risks.

4. Overview of existing risk management frameworks

4.1 Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004

The standard was prepared by the Joint Standards Australia/Standards New Zealand Committee. It provides a generic framework for establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

The standard states:

“To be most effective, risk management should become part of an organization’s culture. It should be embedded into the organization’s philosophy, practices and business processes rather than be viewed or practiced as a separate activity. When this is achieved, everyone in the organization becomes involved in the management of risk.”²

The standard identifies that risk management can be applied at the strategic, tactical and operational levels of the organisation.

An illustration of the framework’s seven elements is provided on the following page.

² Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004, p.V.

