A Guide to Risk Management

July 2011

Queensland Government

Financial Management Framework

© The State of Queensland (Queensland Treasury) July 2011

Except where otherwise noted you are free to copy, communicate and adapt this work, as long as you attribute the authors.

This document is licensed under a Creative Commons Attribution 3.0 Australia licence.
To view a copy of this licence, visit http://creativecommons.org/licenses/by/3.0/au

To attribute this work, cite A Guide to Risk Management, The State of Queensland (Queensland Treasury) July 2011

The diagram on Page 10 has been reproduced with permission from SAI Global and is not covered by the CC BY license. Contact the copyright owner, SAI Global directly to request permission to use this material. The Standard can be purchased via http://www.saiglobal.com

Acknowledgements

This publication has been developed by the Financial Management Branch of Queensland Treasury, with assistance provided by the Department of the Premier and Cabinet.

We also **wish to acknowledge the use of material** produced by other jurisdictions in the development of this practical guide.

This document and related information can be found at www.treasury.qld.gov.au.

Queensland Government

MESSAGE FROM THE UNDER TREASURER

The *Financial Accountability Act 2009* requires all accountable officers and statutory bodies to establish and maintain appropriate systems of internal control and risk management.

In December 2007, the Department of the Premier and Cabinet and Queensland Treasury released the document *Strategic Risk Management: Guidelines*. The guidelines reflected and responded to the findings set out by the Auditor-General of Queensland Report to Parliament No. 6 for 2007: *Beyond Agency Risk* and the Auditor-General's subsequent *Better Practice Guide: Risk Management*.

In reviewing the previous guidelines, Queensland Treasury and the Department of the Premier and Cabinet have collaborated to develop a new guide titled *A Guide to Risk Management* (the Guide), thus replacing the *Strategic Risk Management: Guidelines*.

This Guide reflects the changes to the financial management legislation in Queensland, as well as the release of a new Australia/New Zealand risk management standard. The key differences from the previous guidelines are:

- the scope of this Guide has been broadened to consider all risks
- emphasis is placed on how agencies can practically integrate the risk management framework into existing governance processes, and
- assistance is provided with risk identification at the agency, cross-agency and whole-of-Government levels.

Effective risk management can deliver a range of benefits to agencies, including improved results through more informed decision making and improved accountability by demonstrating that levels of risk associated with the agency are understood and that risk treatment strategies are appropriate and cost-effective.

I commend *A Guide to Risk Management* to all Queensland public sector management and staff.

(G. Bradley)
Under Treasurer

Date: July 2011

Table of Contents

Introduction

The *Financial Accountability Act 2009* (the Act) outlines a number of accountable officer and statutory body functions, one of which is the establishment and maintenance of an appropriate system of risk management (section 61).

The *Financial and Performance Management Standard 2009* (the Standard), section 28, prescribes that the agency's risk management system must provide for:

- mitigating the risk to the department or statutory body and the State from unacceptable costs or losses associated with the operations of the department or statutory body, and
- managing the risks that may affect the ability of the department or statutory body to continue to provide government services.

Purpose of the Guide

There is a significant amount of conceptual risk management guidance material available for both the public and private sectors. The purpose of the Guide is to provide an overview of the key concepts of risk management, and guidance on how the risk management process can be practically applied by any Queensland public sector agency.

Scope and application

The Guide is intended to be an information reference and contains the minimum principles and procedures of a basic risk management process to assist departments and statutory bodies in adopting a consistent approach to risk management. The Guide is not mandatory however, application of the Guide will encourage better practice and support accountable officers and statutory bodies in the implementation of effective risk management practices at all levels within their agency.

Agencies are encouraged to tailor content of the Guide to suit their individual circumstances and to progressively develop more sophisticated processes as their risk management maturity level increases.

As risk management and its associated processes are interrelated and dynamic, the separation of the components of a risk management process in this Guide is intended to be illustrative only. Agencies may combine or undertake activities in a different order to that presented in this Guide. They may also find that certain activities overlap the individual components of the risk management process.

Australian/New Zealand standard

While not mandated by legislation, it is expected that, where appropriate, agencies will apply the Australian/New Zealand Standard ISO 31000:2009 *Risk management – Principles and guidelines* (AS/NZS ISO 31000).

This guide is not intended to replace AS/NZS ISO 31000 but should be read in conjunction with it. It is expected that application of AS/NZS ISO 31000 and this Guide will lead to agencies improving their risk management capability, resulting in risk being more effectively and efficiently managed across the Queensland public sector. Agencies are encouraged to obtain a copy of AS/NZS ISO 31000 from Standards Australia.

While this Guide is predominantly based on AS/NZS ISO 31000, agencies should be aware of additional Standards that relate to risk such as, for example, HB 266:2010 *Guide for managing risk in not-for-profit organisations*, HB 231:2004 *Information security risk management guidelines*, and HB 296:2007 *Legal risk management*.

Terminology

There are many risk related terms used in this document. Definitions for key terms are located in Application Guide 1 - Glossary of Terms. While there is an abundance of risk terminology used today, the terminology in this Guide is consistent with AS/NZS ISO 31000.

Where the Guide refers to 'agencies', this includes both departments and statutory bodies. However, the specific use of the term 'departments' indicates that the section does not apply to statutory bodies.

Practical Guidance Material

Application Guide 1 provides definitions of key terms used throughout the document.

Risk and risk management

Risk

While there are many varied definitions of risk widely available, often incorporating industry specific terminology, it is generally accepted that if we know for certain something is going to happen it has no risk attached to it. Should there be an element of uncertainty surrounding it, then risk exists.

For the purposes of this Guide, risk encompasses both possible threats and opportunities and the potential impact these may have on the ability of the agency to meet its objectives. That is, risk relates to both challenges to, and opportunities for, the agency.

The Standard separates risk into two types – strategic risk and operational risk. Strategic risks relate directly to an agency's strategic planning and management processes. Strategic risks are those which could significantly impact on the achievement of the agency's vision and strategic objectives as documented in the strategic plan. They are high level risks which require identification, treatment, monitoring and management by the agency's senior executives or board. These risks may need to be managed by more than one agency for the risk treatments to be effective.

Operational risks are those which could have a significant impact on the achievement of:

- the agency's strategic objectives (as documented in the strategic plan) from the perspective of the actions undertaken by a particular division, branch or work unit, or
- the individual programs or project management objectives.

Operational risks generally require management by the relevant senior officer responsible for the division, branch or work unit, or by the relevant program or project board. In extreme instances, these risks may require escalation to executive management.

Risk management

Risk management embodies an organisational culture of prudent risk-taking within an agency. It is the process of identifying, assessing and responding to risks, and communicating the outcomes of these processes to the appropriate parties in a timely manner.

An effective risk management system:

- improves planning processes by enabling the key focus to remain on core business and helping to ensure continuity of service delivery
- reduces the likelihood of potentially costly 'surprises' and assists with preparing for challenging and undesirable events and outcomes
- contributes to improved resource allocation by targeting resources to the highest level risks
- improves efficiency and general performance
- contributes to the development of a positive organisational culture, in which people and agencies understand their purpose, roles and direction
- improves accountability, responsibility, transparency and governance in relation to both decision-making and outcomes. This is particularly important for public sector agencies, which exist to deliver beneficial outcomes for the Queensland Government, industry and the community, and
- adds value as a key component of decision-making, planning, policy, performance and resource allocation, when subject to continual improvement.

Factors that inhibit effective risk management can include:

- a lack of support for a risk management culture from executive management
- a lack of time and resources allocated to risk management
- difficulty in identifying and assessing emerging risks, especially cross-agency risks
- a lack of independent assurance over the effectiveness of the risk management framework
- a lack of clarity over risk ownership and the responsibility for risk management
- over- or under-treatment of risks, and
- unnecessarily complex risk documentation.

When risk management has commitment from executive management by encouraging a strong organisational culture and awareness of risk, an agency should be able to overcome the factors which inhibit effective risk management.

Risk management within the Queensland public sector

Section 61 of the Act requires agencies to establish and maintain appropriate risk management systems. There are many benefits of establishing robust risk management systems to enable threats and opportunities that face an agency to be appropriately managed.

Risk is an ever present element of public policy and government service delivery. Effective risk management enables agencies to have increased confidence that they can deliver the required services, manage risks and threats to an acceptable degree, and make informed decisions about opportunities and challenges they face.

In the context of this Guide, risk management applies to the process of identifying, treating and managing risks across the entire Queensland public sector. Risks that need to be identified and managed include:

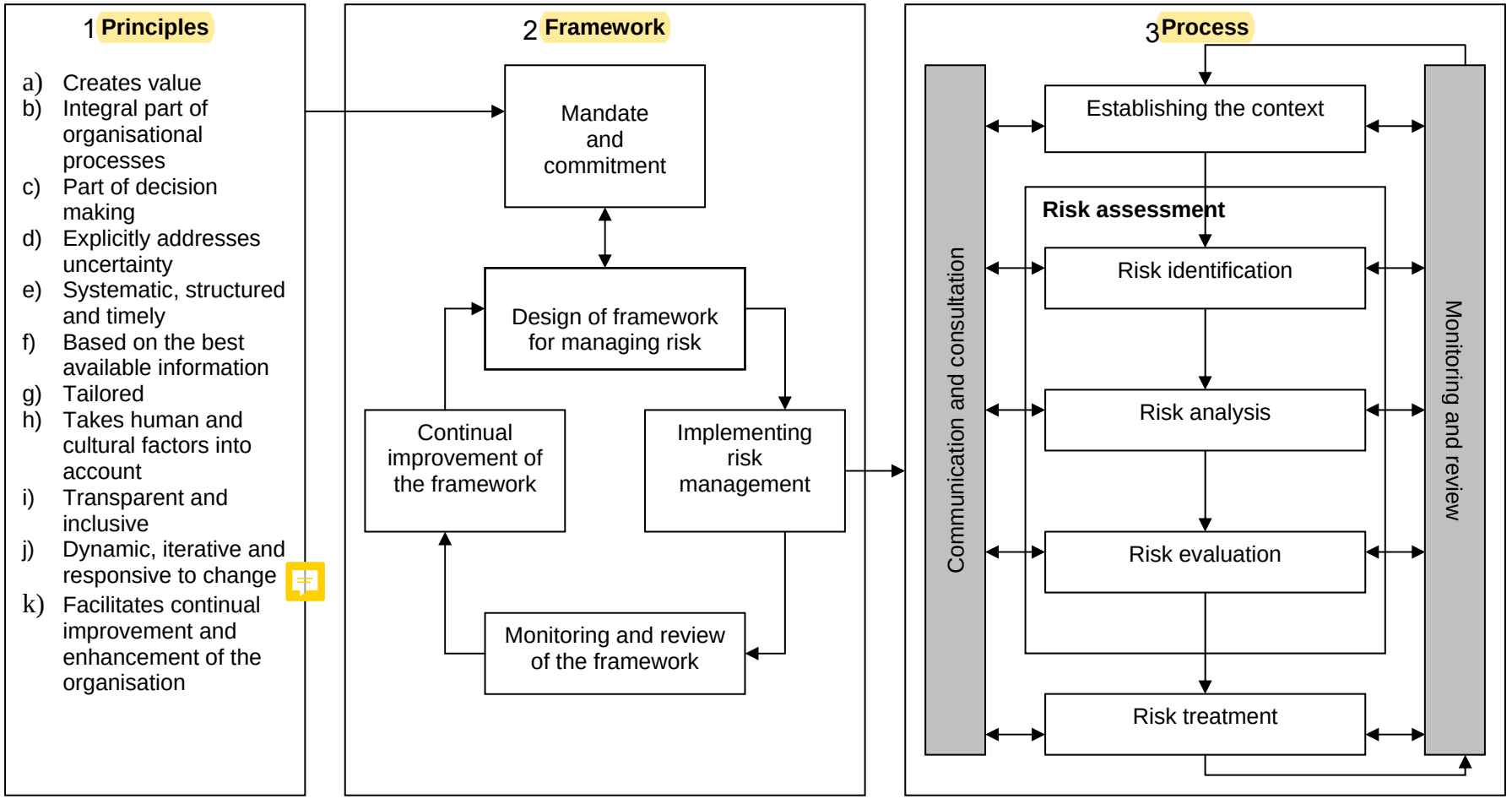
- agency strategic and operational risks which are managed by individual agencies, but which may become risks for the State, due to their size or significance
- cross-agency risks, where a risk relates to more than one agency (for example, collaborative projects) and requires treatment by multiple agencies to be effective, and
- whole-of-Government risks which are beyond the boundaries of any one agency due to their magnitude and/or impact on service delivery, and which call for a response across agencies, would require a co-ordinated approach by a central agency or by a lead agency.[1]

As whole-of-Government approaches to project management are becoming more common, there is an increased awareness of the need to manage risks at this level. All agencies need to be aware of and understand potential significant risks at the whole-of-Government level. Identifying, treating and monitoring these risks are a shared responsibility.

[1] Based on Auditor-General of Victoria (June 2007) *Managing Risk Across the Public Sector: Toward Good Practice.*

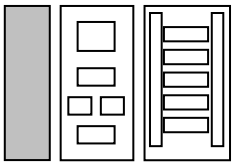
Relationship between risk management principles, framework and process The Main Topic

The diagram below is reproduced from AS/NZS ISO 31000 (with the permission of SAI Global Ltd) and depicts the relationship between the underpinning principles of risk management, the risk management framework, and the risk management process. The remainder of the Guide will provide further information and practical tips for agencies to introduce a robust framework and risk management process.



Source: AS/NZS ISO 31000 (reproduced with permission from SAI Global)

1 Principles of risk management

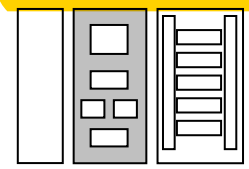


Many factors will contribute to the success of risk management throughout an agency. AS/NZS ISO 31000 provides principles that should be adopted by any organisation to successfully manage their risks.

While the principles in AS/NZS ISO 31000 are relevant to Queensland government agencies, the following principles are considered specific to Queensland government agencies:

- risk management has a firm commitment from the accountable officer or statutory body board
- the risk management framework is integrated with other agency governance processes, such as strategic planning, operational planning and executive management functions
- effective risk management is based on a strong organisational culture and awareness of risk at all levels of the agency, which involves encouraging a risk-informed workforce and culture
- risk management is supported by a program of education, training and development for staff that is devoted to risk management at key levels in the agency (for example supervisor, manager, director and executive)
- the risk management process designates clear ownership of risk accountabilities, responsibilities, duties and actions
- the risk management process is proactive with cross-agency communication of risks, and
- the risk management process draws on both current experiences and lessons learned.

Risk management framework



Risk management is not an isolated function that exists within the agency. Rather, it is an integral part of strategic planning, strategic management and the everyday activities of the agency. AS/NZS ISO 31000 provides further guidance on developing a sound risk management framework.

Three specific areas: the responsibilities of relevant officers within an agency; the integration of risk management into all areas of the agency; and the mechanisms in place to review the framework, are discussed in further detail below:

Responsibilities of agency officers

It is fundamentally the role of accountable officers and statutory bodies and their management teams to ensure that each agency has a robust internal organisational culture and process that is capable of identifying and managing its risks. As required by section 78 of the Act, the Head of Internal Audit as defined in the Act is charged with providing assistance with risk management. However, the responsibility and accountability for implementation of a risk management framework remains with the accountable officer or statutory body.

Objectives and strategies for risk management should be designed to complement the agency's existing vision and strategic objectives. In establishing an overall risk management direction, a clear vision for risk management should be articulated and supported by policies and operating principles. An up-to-date, plain English risk management framework will guide staff by:

- describing the risk management philosophy (why?) and process (how?)
- providing methods for identifying, treating, monitoring, and reviewing risk
- establishing roles and responsibilities for effective management of risk (for example, establishing a risk co-ordinator role to lead and manage the risk management program across the agency and assigning a risk owner to each risk)
- detailing an appropriate process for reporting on strategic and operational risks, and
- providing for ongoing continuous improvement through the evaluation of the objectives and results of the risk management process.

The greater the awareness and understanding of the risk management framework by all staff, the more likely it is that staff will own and apply the risk management principles promoted by the agency and incorporate them in their day to day activities. It is essential that accountable officers and senior and executive management model all aspects of risk management and principles to promote a robust risk management culture within their agency.

There is no "one size fits all" risk management framework that can be applied across the varied types and sizes of Government agencies. Executive management needs to consider the type of framework that will best integrate with its particular operational context and internal and external environment. Agencies should refer to existing policies and procedures such as the following to assist with developing a framework:

- business operations
- reporting mechanisms
- organisational culture
- workforce skills and capabilities
- planning and performance management processes
- budget and resourcing

- supporting infrastructure
- standards, legislative and regulatory requirements
- organisational and governance structure, and
- delegations of authority, responsibility and accountability.

Integration of risk management

Risk management should be embedded or integrated into the agency's philosophy and organisational culture (that is, "the way we do things around here"); existing governance policies; and planning, reporting and decision-making structures at both the strategic and operational levels. Agencies that integrate risk management have a greater likelihood of achieving their strategic objectives and delivering their services efficiently and effectively.

Successful alignment of risk management and governance requires four key factors:

1. an agency focus – where there is an identifiable source of risk management expertise in the agency and senior managers come together on a regular basis to discuss risk management issues
2. an agency direction – where a clear direction and strategy is established for risk management, including articulating the agency's risk appetite and giving a clear mandate for what constitutes effective risk management
3. decision-making structures – where risk management is not a separate process, but a key consideration at all parts of the decision-making chain: being factored into strategic and operational planning; included as a common component in all project proposals and business cases; and incorporated into advice to Ministers; and
4. agency capacity and capability – where the agency's executive management invests time and resources to build momentum, capacity and capability, including: ensuring that there is a shared language of risk management; a common understanding of the principles; training and development to build expertise; and established tools and processes for risk management.

Integrated risk management requires an ongoing assessment of potential risks and opportunities for an agency at every level. The results should inform agency level risks, facilitate priority setting and improve an agency's decision making. Clear links should be established between risk management, Government policies and priorities, agency objectives (vertical integration), and agency policy and operations (horizontal integration).

Vertical Integration

Vertical integration involves:

- integrating risk management with objectives at all levels of the agency by providing a framework that links an agency's strategic plan through to its individual operational plans
- integrating risk management with evaluation and reporting mechanisms, to ensure that risks and risk treatment strategies are monitored, analysed, reviewed and updated
- embedding risk management components into existing strategic and operational planning processes
- communicating executive management or board decisions on acceptable levels of risk
- establishing escalation processes to be followed where a risk is reviewed and falls outside the range of the accepted levels of risk appetite and tolerance, and
- improving control, governance and accountability systems and processes to take into account risk management and results from the assessment of potential risks.

Horizontal Integration

Horizontal integration involves integrating risk management into an agency's systems, processes and practices and, in particular, the planning and decision-making processes at each level of the agency. When risk management is integrated into strategic and operational planning and regular reporting cycles, the additional risk management information available should enable more informed planning and decision-making at the agency, cross-agency and whole-of-Government levels.

Information should be shared throughout an agency to ensure there is a coordinated approach to identifying and treating risks. In considering risk, business areas should take into account the potential impact of risk treatment on other business areas, and should be encouraged to share best practice/lessons learned with the rest of the agency and across agencies.

Organisational Culture

Effectively embedding risk management into the organisational culture is key to achieving integrated risk management. A challenge for all agencies is to deliver an appropriate level of investment in strategic risk management – both in time and resources – and clearly communicate the importance of risk management as a core component of the agency's business. This can be accomplished in a number of ways, such as by:

- executive and senior managers championing and modelling risk management
- promoting the view that all staff in the agency are managers of risk
- encouraging managers and staff to develop knowledge and skills in risk management, and
- training and supporting staff in incorporating risk management into their everyday roles and responsibilities.

Risk Management Champion

Agencies may consider appointing a "risk management champion" to assist with integrating risk management into the organisational culture. The risk management champion would generally report to the executive management of an agency; be a senior executive officer with knowledge of risk management; have the vision, drive and determination to lead by example; and have the authority, responsibility and support to make things happen.

In the early stages of implementing integrated risk management, the risk management champion will need to be able to demonstrate to executive management how it will help them with meeting agency objectives in the short term and better position the agency for the future. The risk management champion would be responsible for driving risk management awareness, integration, policies and strategies. The risk management champion would promote, across the agency, an organisational culture that supports:

- increased awareness of risk management techniques, practices and processes (for example, identifying and implementing training and development opportunities for all agency staff)
- uniform understanding of the agency's key strategic and operational risks and opportunities (including cross-agency and whole-of-Government risks)
- management of risk for business functions that have been outsourced from the agency (for example, payroll function), as the agency maintains ownership of such risks
- staff in identifying and reporting risks to management in a safe, no-blame environment
- awareness of how risk management can be applied to individual roles and how it can guide advice to Ministers, and

- a broad understanding of the relationship between the agency's risks, cross-agency risks and whole-of-Government risks.

Successful risk management requires involvement by all agency staff. A supportive organisational culture, where expertise, learning and innovation are rewarded, and where a "no surprises" rather than "no risks" philosophy is encouraged, should assist agencies in developing their risk management process. Agencies with a supportive work environment tend to:

- promote learning – by encouraging staff to learn and to value knowledge, expertise, new ideas and innovation
- learn from experience – by valuing experimentation, sharing lessons from past successes and failures and bringing this learning to planning and risk management, and
- demonstrate management and leadership – by selecting leaders who are good coaches and teachers, demonstrating commitment to staff by providing tools, opportunities and resources and investing in the risk management process, including reviewing the process periodically.[2]

Providing the right risk management resources, training and awareness programs for staff is critical to building an effective organisational culture.

Mechanisms to review the risk management framework

Risk management is not just about the review of risks themselves. Agencies need to review their risk management capability and governance systems to ensure they are delivering effective and robust risk management that is fit for the agency's purpose. Internal auditors may assist in providing assurance that an agency's risk management framework is operating effectively and may also assist with the development, maintenance and review of the framework, provided care is taken to maintain independence and objectivity. This may involve internal audit being part of a risk project team in an advisory capacity.

Risks, risk profile, risk management capability and systems, and the risk environment are all constantly changing and evolving. A regular review of a risk management framework will:

- provide assurances to the executive management that the agency's risk profile has been properly identified, documented and assessed
- ensure the agency's procedures and governance systems are working effectively, and
- ensure that risks are being effectively monitored and treated to an agreed level.

At a minimum, an annual review of the entire risk management process should be undertaken by the accountable officer or statutory body. It is important to consider "lessons learned", both positive and negative, and to use these to enhance current practices and processes. It is also important to assess whether all elements of the risk management framework have been implemented effectively.

Responsibility for reviewing the risk management framework may be allocated to a committee to provide support and advice to the accountable officer or statutory body. It may be a separate risk management committee, or combined with the agency's audit committee.

While the committee has no responsibility for managing the risks themselves, they may be responsible for regularly reviewing and evaluating the risk management framework and related governance systems to provide assurance on their efficiency and relevance. It is good practice for the committee to carry out such reviews at least annually, to ensure the procedures remain fit for purpose and are up-to-date. The committee should take care not to confuse reviewing risk management procedures with risk management itself. Reviewing the process is not a substitute for the active management and treatment of an agency's risks.

[2] Treasury Board of Canada Secretariat, Integrated Risk Management Framework

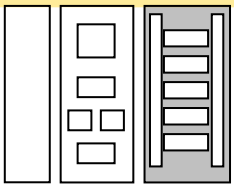
For further information about risk management and audit committees, refer to the *Audit Committee Guidelines – Improving Accountability and Performance*, December 2009.

Practical Guidance Material

Application Guide 2 provides points to be considered when developing a robust risk management framework to assist with integrating and embedding a risk management organisational culture into the agency's existing governance, reporting and decision-making processes. Agencies are encouraged to develop a risk management framework appropriate to their circumstances.

Application Guide 3 provides an illustration of how risk management interacts with the broader responsibilities and functions of an agency.

Risk management process



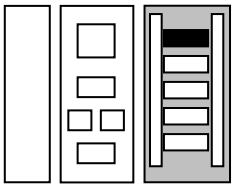
As shown in AS/NZS ISO 31000, the risk management process consists of seven steps. Each step of the risk management process will be considered in detail in this Guide, with practical examples provided on how to implement the process within agencies.

The seven steps of the risk management process are:

- establishing the context
- risk identification
- risk analysis
- risk evaluation
- risk treatment
- communication and consultation, and
- monitoring and review

While the steps are shown separately within this process, agencies are reminded that the risk management process is continually occurring. These processes can be undertaken in any sequence as agencies may find that some processes overlap or fall in a different order.

Agencies are encouraged to develop a complete risk management process that suits their circumstances. For example, the sections on risk identification, risk analysis and risk evaluation can be encompassed in the one process known as risk assessment. The risk management process developed by an agency may require refinement after a review of the process has been undertaken.



Establishing the context

The purpose of establishing the context is to determine the boundaries within which the risk management framework will operate. It should note the boundaries of the framework and the capacity of the agency to successfully address the risks that may be identified in the assessment phase of the risk management process.

In establishing the context, an agency should consider:

- the external and internal environment
- the risk profile
- risk appetite and risk tolerance levels
- a risk matrix and responsibilities, and
- the business continuity plan.

The context of the agency should be reviewed on a regular basis to ensure any effects on an agency from these areas are identified on a timely basis.

External and internal environment

Establishing the external and internal environment of the agency is the first step in the risk management process. It involves consideration of both challenges and opportunities in the context of the agency's vision and objectives, operating environment and key stakeholders.

The environment is important as it sets the parameters within which risks are identified, assessed and managed. As such, it must be sufficiently broadly defined to include a wide range of trends, influences and time horizons. Agencies will need to collect information at both the strategic and operational levels, and include both the external and internal risks facing the agency.

The primary influences on the **external environment** relate to the social, cultural, political, legal, regulatory, financial, technological and economic environments within which the agency operates. These external influences could occur at international, national, state, regional or local levels.

Influences on the **internal environment** may include:

- the agency's objectives and planned results
- plans established to ensure the agency achieves its objectives and delivers its services
- individual projects being undertaken by the agency
- the agency's governance and accountability structures
- policies established by the agency
- resources available within the agency (for example, information systems, staffing and funding), and
- existing risk management expertise and practices.

The defined external and internal environments should be regularly and systematically examined to ensure that they remain appropriate and desirable.

Risk profile

There is a significant interrelationship between developing a risk profile and the strategic planning process. Risk management underlies all aspects of priority setting, planning and resource allocation. In addition, the risk profile, with two-way linkages from and into each of these areas, provides a vehicle to integrate them at the whole-of-Government level. Thus, the risk profile is informed by and should feed back into an agency's strategic planning documents and processes. In a mature practice of integrated risk management, a robust

strategic and operational planning process should assimilate the risk profile, eliminating the need to present it separately.[3]

Risk appetite and risk tolerance

While establishing the context, the agency should also consider its **risk appetite**, which is the amount (or range) of risk which is considered by the agency to be acceptable and justifiable. Across Government, the risk appetite of individual agencies will differ depending upon the environment within which the agency operates.

Risk appetite can be expressed as a series of boundaries appropriately authorised by the agency's executive management. Different levels of staff within an agency should be given clear guidance by management on the limits of risk which they can accept. This involves key discussions being held at various levels within an agency and across agencies especially where there are interrelationships or similarities. To identify the acceptable levels of risk it is expected that discussions would be held at executive level with central agencies to clearly communicate, assess and provide direction on what are acceptable levels of risk. Discussions would concern political, economic, social, technological, legal, environmental and financial issues that impact on agencies and on the whole-of-Government.

In developing the risk appetite for an agency, consideration may be given to:

- commitments or views previously expressed by Parliament or Cabinet
- how the agency's stakeholders (for example, the public and Parliament) have reacted to past risk events and issues
- whether stakeholders have been consulted on risk tolerances and performance targets (for example, via special interest groups), and
- the agency's performance expectations, as expressed in its strategic plan and budget documentation.

The agency should consider its **risk tolerance** at this stage of the process. Risk tolerance can be defined as the acceptable variance from the agency's risk appetite boundaries. Agencies should develop processes to determine acceptable limitations and whether or not they are negotiable.

Within an agency, the risk appetite and risk tolerance will generally not be static. Rather they will differ depending upon the particular challenge or opportunity at the time. Individual projects are an example of how the risk appetite within an agency may differ.

Agencies should also consider an appropriate process where a risk falls marginally outside the desired risk tolerance, but a strong case exists as to why the risk should be accepted and managed.

Determining an agency's risk appetite is not a one-off event. Both risk appetite and risk tolerances may change over time as new information and outcomes become available, and as stakeholder expectations evolve.

Risk matrix and responsibilities

A risk matrix should combine the likelihood of the risk occurring, and the consequence should such a risk occur, to result in the risk rating for treating and/or monitoring the risk. Parameters should be set for each likelihood and consequence in an agency's risk matrix. For example, the likelihood of a risk occurring may be classified as unlikely on a simple matrix if it is expected to occur less than 5% of the time, or once in a year.

Each possibility within a matrix should be defined and the necessary action and the relevant officer responsible for the risk documented for each possibility. The matrix should be reviewed with the internal and external environments to determine the relevance to the risks

[3] Based on Treasury Board of Canada Secretariat, Integrated Risk Management Implementation Guide

identified by an agency. An agency should ensure that all risks are analysed using the same risk criteria.

Examples of risk matrices are provided below; however agencies are strongly encouraged to develop an appropriate analysis system for their individual circumstances.

Simple risk matrix example

	CONSEQUENCE		
LIKELIHOOD	**Minor**	**Moderate**	**Significant**
Unlikely	Low	Low	Medium
Possible	Low	Medium	High
Likely	Medium	High	High

Where an agency considers more complex risk analysis is required (for example, where a number of risks have been identified and more detailed analysis is required to rank the risks for implementation of risk treatment (refer to Risk Analysis section)), then a more detailed risk matrix should be used.

Detailed risk matrix example

	CONSEQUENCE				
LIKELIHOOD	**Insignificant**	**Minor**	**Moderate**	**Major**	**Critical**
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost Certain	MEDIUM Specify responsibility and treatment	MEDIUM Specify responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

Agencies may also consider developing a matrix for each division, branch, work unit, program and/or project. Alternatively, an agency may define the consequences into various risk categories, such as financial risks, occupational health and safety risks, political risks, and so on. The agency would then provide a quantitative and/or qualitative descriptor for each consequence. For example, a financial risk category may define an extreme consequence as a financial loss greater than $1 million, or the loss of a business operation.

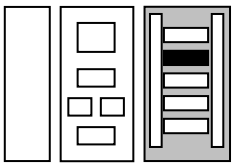
It is important that agencies determine the level of detail that will be appropriate for their circumstances and ensure they develop a risk management system that meets their needs and is within their capabilities.

Business continuity plan

Agencies must recognise that some risk is unavoidable and it is not within the ability of the agency to completely manage all risks to a level commensurate to an agency's risk appetite. For example, agencies have limited control over risks associated with terrorist activity or natural disasters. In these instances, the only action that can be taken by the agency is the preparation of contingency plans for business continuity. A business continuity plan should include appropriate crisis management plans that can be activated as required and these plans should be tested periodically to ensure their effectiveness.

Practical Guidance Material

Application Guide 4 provides elements an agency may need to consider when determining their risk criteria and their external and internal environment.



Risk identification

Once the environment within which the agency operates has been established (that is, the context), the next stage is the identification of individual risks.

The aim of this step is to generate a comprehensive list of threats and opportunities based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of the agency's strategic objectives. Comprehensive identification is crucial, because a risk that is not identified at this stage will not be included in further analysis.[4]

Risk identification should include examination of the knock-on effects of particular consequences, including cascading and cumulative effects of actions.

Environmental scanning

A common method used by agencies to identify emerging risks is environmental scanning. An environmental scan is a powerful risk management and strategic planning tool that entails careful monitoring of an agency's internal and external environments to detect early signs of challenges and opportunities that may influence the agency's current and future plans. It involves obtaining both factual and subjective information on the potential challenges and opportunities to increase the agency's awareness of the key risks it faces.

Key considerations for agencies when undertaking environmental scanning include:

- the type of risk – political, legal, economic, environmental, socio-cultural, technological
- the source of risk – external (political, economic, natural disasters) or internal (reputation, security, knowledge management)
- the causes of the risk
- the impacts of the risk – type of exposure (people, reputation, program results, priorities, funding, assets), and
- the level of control – the degree to which the agency can influence, affect or manage the risk.

In undertaking the environmental scanning process, issues that an agency should consider include:

- the frequency of scanning – depending on the agency's context, environmental scanning may be undertaken continuously or periodically (for example, monthly or yearly)
- timeframe – for example, policy development officers may be interested in developments over the next twenty-five years, whilst scanning that supports operational decision making may be restricted to a six month timeframe
- scope – some agencies may be fairly inward-looking in their risk identification processes if they perceive that the major element of risk arises from within the agency; others may need to consider a much wider scope (including international, national or interstate) if they consider that they may face risks from a wider environment
- opportunity/challenge – some environmental scanning is concerned mainly with spotting potential challenges, but it can equally be used to scan for opportunities ("positive risks"), and many challenges may be converted into opportunities if identified early, and
- rigour/informality – environmental scanning varies in the extent to which it is structured and supported by technology, that is, some agencies may use sophisticated assessment schemes and information search technologies, while other agencies will rely almost entirely on informal networks of contacts and good judgement.[5]

[4] Standards Australia, AS/NZS ISO 31000:2009 Risk management – principles and guidelines
[5] HM Treasury, The Orange Book: Management of Risk – Principles and Concepts, October 2004

Other resources or methods that can be adopted by agencies to identify risks include:

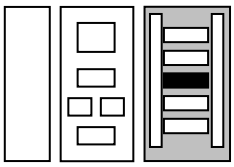
- agency documents, such as the strategic and operational plans, performance reports, budgets, and audit observations and recommendations
- Parliamentary processes and issues highlighted at Estimates Committee hearings
- media reports and commentary
- benchmarking the agency's performance against that of other agencies
- undertaking brainstorming activities
- preparing a strength-weakness-opportunity-threat (SWOT) analysis
- what-if scenarios to seek reaction from stakeholders, and
- the use of surveys and questionnaires.

Irrespective of the method used by the agency to identify the risks, it is vital that relevant and up-to-date information is used, and that people with appropriate knowledge are involved in the risk identification process.

Practical Guidance Material

Application Guide 5 provides consideration points that relate to an agency's risk identification process and highlights potential sources of risks.

Application Guide 6 outlines potential sources of risk that may occur at an agency, cross-agency and/or whole-of-Government level for agencies to consider.



Risk analysis

Risk analysis involves analysing the impact of the potential challenge or opportunity, starting with an assessment of the consequences as well as the likelihood of a risk occurring.

A common approach for analysing risk is through the use of the risk matrix that the agency would have developed previously – refer to 'Establishing the context' section. Where an agency considers the risk analysis process to be relatively straight-forward (for example, an agency with few external stakeholders may consider risk analysis simpler than for an agency with considerable public interest and scrutiny), then categorisation of the risk as high, medium or low may be considered sufficient. The agency should use critical judgement to determine the level of analysis that is required based on what is appropriate and reasonable.

The process for analysing risk will differ from agency to agency; however, an individual agency should ensure all risks within its agency are assessed using the same method. Where collaboration between agencies is required, an agency may need to adopt a flexible approach to risk analysis when assessing a cross-agency risk. However, provided practical, relevant and robust processes are in place at all levels, risk analysis should inform agency level risks and whole-of-Government risks.

Once an agency's risks have been identified and analysed, management may use a simple table to summarise the assessment. For example:

Risk	Assessment		
	Low	Medium	High
1.			
2.			
3.			

Two step approach to assessing risk

Agencies may consider using a two-step approach to assessing risk. The first step involves assessing challenges or opportunities based on their **inherent risk**. This is the risk that exists prior to any internal controls being implemented to manage the risk. After inherent risk is assessed, agencies could focus on the **residual risk**, which is the risk which remains after action has been taken to manage the risk (and assuming the action is operating effectively).

Advantages of using this two-step analysis approach include:

- assisting management with identification of excessive or ineffective controls, and
- ensuring management is aware of the agency's exposure if the control fails.

If the two-step approach is implemented, both inherent and residual risk will need to be reassessed whenever controls are adjusted or environmental scanning indicates that circumstances may have changed.

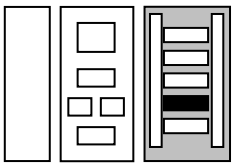
The following is a simple example of documenting risk based on a two-step approach:

RISK	Inherent assessment		CONTROLS IN PLACE	Residual assessment		ACTION PLANNED AND OWNER
	Likelihood	Consequence		Likelihood	Consequence	
1.						
2.						
3.						

As can be seen from the above table, when a two-step approach is adopted, risk analysis, risk evaluation and risk treatment are interrelated processes, which need to be considered by the agency simultaneously.

Practical Guidance Material

Application Guide 7 provides agencies with key consideration points when analysing risks.



Risk evaluation

Once an agency has identified and analysed its risks, they should be evaluated to determine which risks are to be treated and the priority for treatment implementation. This process is known as risk evaluation. Treatment options are outlined in the 'Risk treatment' section.

When evaluating risks agencies should consider:

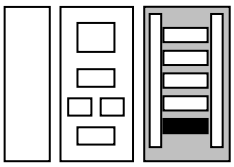
- the external and internal environment the agency operates in (that is, the established agency context) – this will largely involve the overall strategic direction of the agency
- the risk appetite of the agency, as established earlier in the risk management process – for example, where the agency is involved in speculative activities, high risk activities may not always require priority treatment
- the risk appetite of parties other than the agency (that is, the stakeholders) – for example, some high risk activities may be more acceptable to the public than others
- any legal, regulatory or other requirements which may exist – for example, if the risk could result in legal action against the agency, this risk may be a high priority if the probability of occurrence is high, and
- the cost/benefits of treating the risk.

The highest priority should be given to those risks that are evaluated as being the least acceptable. High priority risks should be given regular attention, review and evaluation.

Over time, specific risks and risk priorities will change, and an agency will need to review and evaluate its prioritisation process. Further information is provided in the section on Monitoring and review.

Practical Guidance Material

Application Guide 8 outlines some of the areas that should be considered when evaluating and prioritising risks within an agency.



Risk treatment

Once risks have been analysed and evaluated, the agency needs to determine the appropriate risk treatment/s. Any action taken to address a risk becomes part of the agency's internal controls.

There are a number of risk treatment options available, and more than one may be applied to a given risk. Risk treatment options include:

- treat the risk. This approach enables the activity or action to continue within the agency, but action is available to reduce the risk to an accepted level. The 'treat' option can be further dissected into four different types of controls:
    - preventative controls – designed to limit the possibility of an undesirable outcome being realised. The more important it is that an undesirable outcome should not arise, the more important it becomes to implement appropriate preventive controls. Examples of preventive controls include separation of duty, installing security cameras to deter criminal activity, the use of contract terms to enable recovery of overpayment or to safeguard against potential breaches of contracted project milestones.
    - corrective controls – designed to correct undesirable outcomes which have been realised. Examples of corrective controls include rotating staff positions, internal audit review of preventative and detective controls, or a change to management procedures.
    - directive controls – designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided, particularly in the area of health and safety. Examples of directive controls include a requirement for protective clothing to be worn, or that staff be appropriately trained before working unsupervised.
    - detective controls – designed to identify unfavourable events after they have occurred. As they are "after the event" controls, they are only appropriate when it is possible to accept the loss or damage incurred. Examples of detective controls include inventory or asset stocktakes, bank reconciliations, or monitoring activities which detect changes that should be responded to.[6]
- transfer the risk. Risk transfer may be achieved by taking out insurance to facilitate financial recovery against the realisation of a risk, or by compensating a third party (potentially another agency) to take the risk because the other party is more able to effectively manage the risk. Risk may be wholly transferred, or partly transferred (that is, shared). For example, an agency may, with the Treasurer's approval, enter into a forward contract (such as a contract for the agency to buy an asset from an overseas party at a specified future time at a price agreed today) to transfer some of the exchange rate risk to the other party.
- terminate the risk. Some risks may only return to acceptable levels if the activity is terminated. The opportunities in the public sector to terminate an activity may be limited due to the nature of government responsibility. That is, the government may only be involved in delivering a service which is required for the public benefit because the associated risks are too great for the private sector to be involved.
- take the opportunity. There may be opportunities for an agency to take advantage of a risk event. For example, the agency may identify that a reduction in over-the-counter payments may result in reduced opening hours. Opportunities, however, may arise where the agency could partner with another agency to combine counter services (thus maintaining opening hours but reducing personnel costs) or transfer some of the resources to improve other areas of service delivery.

[6] HM Treasury, The Orange Book: Management of Risk – Principles and Concepts, October 2004

It may be appropriate, in some instances, to accept the risk rather than treat the risk. A risk may be accepted because:

- the probability or consequences of the risk is low or minor
- the cost of treating the risk outweighs any potential benefit
- the risk falls within the agency's established risk appetite and/or tolerance levels
- whole-of-Government policy requires acceptance of the risk, or
- the agency has limited or no control over the risk, for example, natural disasters, international financial market impacts, terrorism and pandemic illnesses. To manage such risks, agencies should have a business continuity plan in place (discussed in Establishing the context) to provide effective prevention and recovery for the agency, while reducing adverse stakeholder impacts caused by the event, and these plans should be subject to regular testing and review.

When determining the most appropriate treatment option in relation to risks, agencies should consider the following:

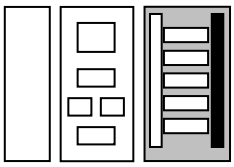
- there should be a balance between the costs and efforts involved in implementing the option against the benefits derived. Apart from the most extreme undesirable outcome (such as loss of human life) it is generally sufficient to design controls to give a reasonable level of assurance that the likely loss will be within the agency's risk appetite.
- as well as considering financial costs, agencies may also need to take into account the political, environmental or social costs and benefits.
- the values and perceptions held by stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the agency or with stakeholders, they should be involved in determining the treatment.
- risk treatment itself can introduce risks, for example, the failure or ineffectiveness of the risk treatment measures, or the introduction of secondary risks that will also need to be assessed, evaluated and treated.

Agencies should fully integrate risks into their strategic and operational plans, and prepare **risk treatment plans** to document how the chosen treatment/action will be implemented. The following points should be addressed:

- the identification of officers assigned responsibility for implementing the plan
- proposed treatment actions and timeframes, including a cost-benefit analysis of alternatives
- the physical and human resource requirements to implement the actions
- performance indicators that will be used to measure, review and evaluate the effectiveness of the treatment/action, and
- the ongoing monitoring and reporting requirements.

Practical Guidance Material

Application Guide 9 identifies key elements that need to be considered by decision makers when aiming to treat different types of risk within an agency.



Monitoring and review

Continuous monitoring and review are vital components of an effective risk management process. They may be undertaken as part of a formal periodic process, or performed on an ad hoc basis.

The primary purpose of monitoring and review is to determine whether risks still exist, whether new risks have arisen, whether the likelihood or impact of risks have changed, and to reassess the risk priorities within the internal and external context of the agency.

Monitoring and review provides important feedback with regard to assurance over the efficiency and effectiveness of controls implemented to treat risks. It enables the agency to analyse and learn lessons from event successes, failures and near-misses.

Review of risks and review of the risk management process are distinct from each other and neither is a substitute for the other. The review processes should:

- ensure that all aspects of the risk management process, including the framework, are reviewed at least once a year
- ensure that risks themselves (and their associated internal controls) are subjected to review within a suitable timeframe (with appropriate provision for management's own review of risks and for independent review/audit), and
- make provision for alerting the appropriate level of management to new risks or to changes in already identified risks so that the change can be appropriately addressed.[7]

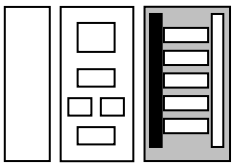
It is important that responsibilities for monitoring and reporting are clearly defined, and that results are documented and shared with all appropriate internal and external stakeholders. This includes sharing experiences and better practices internally and across government.

Under the Act, the Head of Internal Audit is responsible for providing assistance in risk management. As a member of senior management, the Head of Internal Audit is in a position to report to relevant management committees on many of the major risks the agency faces. Where specialist risk managers are appointed to undertake this reporting, the Head of Internal Audit would ensure management's reporting is effective.

The results of monitoring and reviewing the risk management process should also be used as input to the review of the risk management framework. This enables continuous improvement of the risk management process and framework which will lead to improvements in the agency's management of risk and its organisational risk culture.

Practical Guidance Material
Application Guide 10 highlights key elements to be considered when an agency evaluates its monitoring and reviewing processes that relate to risk management.

[7] HM Treasury, The Orange Book: Management of Risk – Principles and Concepts, October 2004



Communication and consultation

Communication, consultation and regular feedback must take place during all steps in the risk management process. The nature of the risk (for example, strategic, operational, political) will need to be considered in determining an appropriate consultation process.

All staff within an agency must be involved in the risk management process, including identifying, analysing, managing and reporting on risks. Internally, risk communication promotes action, continuous learning, innovation and team work. It can demonstrate how management of a localised risk contributes to the overall achievement of agency objectives.[8]

It is important to ensure that all agency staff understand, in a way appropriate to their role, what the agency's risk strategy is, what the risk priorities are and how their particular responsibilities in the agency fit into the risk management framework. If this is not achieved, appropriate and consistent embedding of risk management and an organisational risk culture will not be achieved and risk priorities may not be consistently addressed.[9]

Stakeholders outside the agency can also provide information about risks that may affect the agency, as well as assist with managing known risks.

When identifying stakeholders of a risk, and determining with whom to consult, agencies may consider:

- staff within the agency
- the agency's Risk Management Champion
- the accountable officer / Chief Executive Officer / agency executive management
- the agency's risk management committee (or similar)
- staff in other agencies or relevant Australian Government agencies
- Department of the Premier and Cabinet (DPC) and Treasury
- the agency's portfolio Minister or Cabinet
- the public
- partners and/or third party agencies used to delivery key services
- interest groups, for example, employer groups, industry groups, unions, and
- suppliers.

Cross-agency risks

Where agencies have shared priorities and challenges, and have identified risks from a joint or cluster viewpoint, a lead agency should be determined to establish clear communication and consultation processes. The lead agency would be responsible for opening up dialogue within the cluster either by an informal forum or strategic meetings within the cluster, with DPC and/or Treasury included where the risk has whole-of-Government implications.

An agency may be required to adopt a risk analysis methodology compatible with the lead agency in order to provide comparable risk reporting and ratings. The aim is to improve communication and networking within relevant clusters and to develop contacts and share knowledge.

The single code of conduct for all public sector officers provides confidentiality protocols to be followed when discussing all risks.

[8] Treasury Board of Canada Secretariat, Integrated Risk Management Framework
[9] HM Treasury, The Orange Book: Management of Risk – Principles and Concepts, October 2004

Reporting

In order to ensure the effectiveness of the risk management process, consideration should be given to establishing an appropriate reporting structure within an agency. For example, the Head of Internal Audit may be required to report to the risk committee (or the audit committee where applicable) or the accountable officer or statutory body regarding the status of the risks currently on the risk register or incorporated into the strategic and operational plans.

Reporting processes should be timely and address the following points:

- the adequacy and effectiveness of the internal controls in place to treat risk
- identification of any new risks that may have arisen, and
- implementation of new controls to address key risks.

Where significant risks are identified within an agency, processes should be in place for reporting these to the agency's Chief Executive Officer. Depending upon the risk, the Chief Executive Officer may discuss the risk with counterparts in other agencies, or escalate the risk to the appropriate Minister.

Practical Guidance Material

Application Guide 11 outlines key considerations linked to communication and consultation processes with stakeholders to identify and manage agency risks.

Application Guide 12 provides a list of potential stakeholders that agencies should consider throughout the entire risk management process.

Application Guides

The application guides are designed to provide agencies with practical guidance for the implementation of the concepts discussed throughout the document. The following application guides are provided:

- Application Guide 1 - Glossary of terms
- Application Guide 2 - Risk management framework
- Application Guide 3 - Example of integrated risk management within an agency
- Application Guide 4 - Establishing the context
- Application Guide 5 - Risk identification
- Application Guide 6 - Potential sources of risk
- Application Guide 7 - Risk analysis
- Application Guide 8 - Risk evaluation
- Application Guide 9 - Risk treatment
- Application Guide 10 - Monitoring and review
- Application Guide 11 - Communication and consultation
- Application Guide 12 - Potential Stakeholders

The application guides are provided for agencies to consider when developing their risk management process as a whole. As this document contains generic guidance, some points may not be applicable to all agencies. Agencies are encouraged to adapt the guides to suit their own individual circumstances.

Application Guide 1 - Glossary of terms

Below is a glossary of terms applicable to risk management. They are based largely on the definitions contained in AS/NZS ISO 31000.

Term	Definition/meaning
Consequence	The outcome of an event (for example, a loss, injury, disadvantage or gain) which affects the agency's ability to achieve its objectives.
Control	Any action taken to manage risk.
Likelihood	The chance of something happening.
Operational Risk	Those risks that arise in day to day operations, and which require specific and detailed response and monitoring regimes. If not treated and monitored, operational risks could potentially result in major adverse consequences for the agency.
Residual Risk	Risk remaining after new controls or treatments are taken into account.
Risk	The chance of something happening that will have an impact on the achievement of the agency's objectives. Risk is measured in terms of consequences and likelihood, and covers threats and opportunities.
Risk Acceptance	An informed decision by the risk owner to accept the consequences and the likelihood of a particular risk.
Risk Analysis	A systematic process to determine the nature of risk and the magnitude of their consequences.
Risk Appetite	The amount of risk that the agency is prepared to accept or be exposed to at any point in time.
Risk Assessment	The overall process of risk identification, analysis and evaluation.
Risk Avoidance	An informed decision not to become involved in, or to withdraw from, a risk situation.
Risk Evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk Identification	The process of finding, recognising and describing risks.
Risk Management	The coordinated activities to direct and control an agency with regard to risk.
Risk Management Committee	A standing committee responsible for providing oversight of the agency's management of risk.
Risk Management Framework	The agency's policies, procedures, systems and processes concerned with managing risk.
Risk Management Process	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Risk Profile	The documented and prioritised overall assessment of a range of specific risks faced by the agency.
Risk Rating	The rating resulting from the application of the agency's risk assessment matrix on the likelihood and consequence of a risk occurring.
Risk Register	A system or file that holds all information on identifying and managing a risk.

Term	Definition/meaning
Risk Retention	Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the agency.
Risk Sharing	Sharing with another party the burden of loss, or benefit of gain from a particular risk
Risk Tolerance	The variation from the pre-determined risk appetite an agency is prepared to accept.
Risk Transfer	Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means.
Risk Treatment	Selection and implementation of appropriate options for dealing with risk.
Strategic Risk	Risks that may affect the agency's ability to meet its strategic objectives and require oversight by senior executives.

Application Guide 2 - Risk management framework

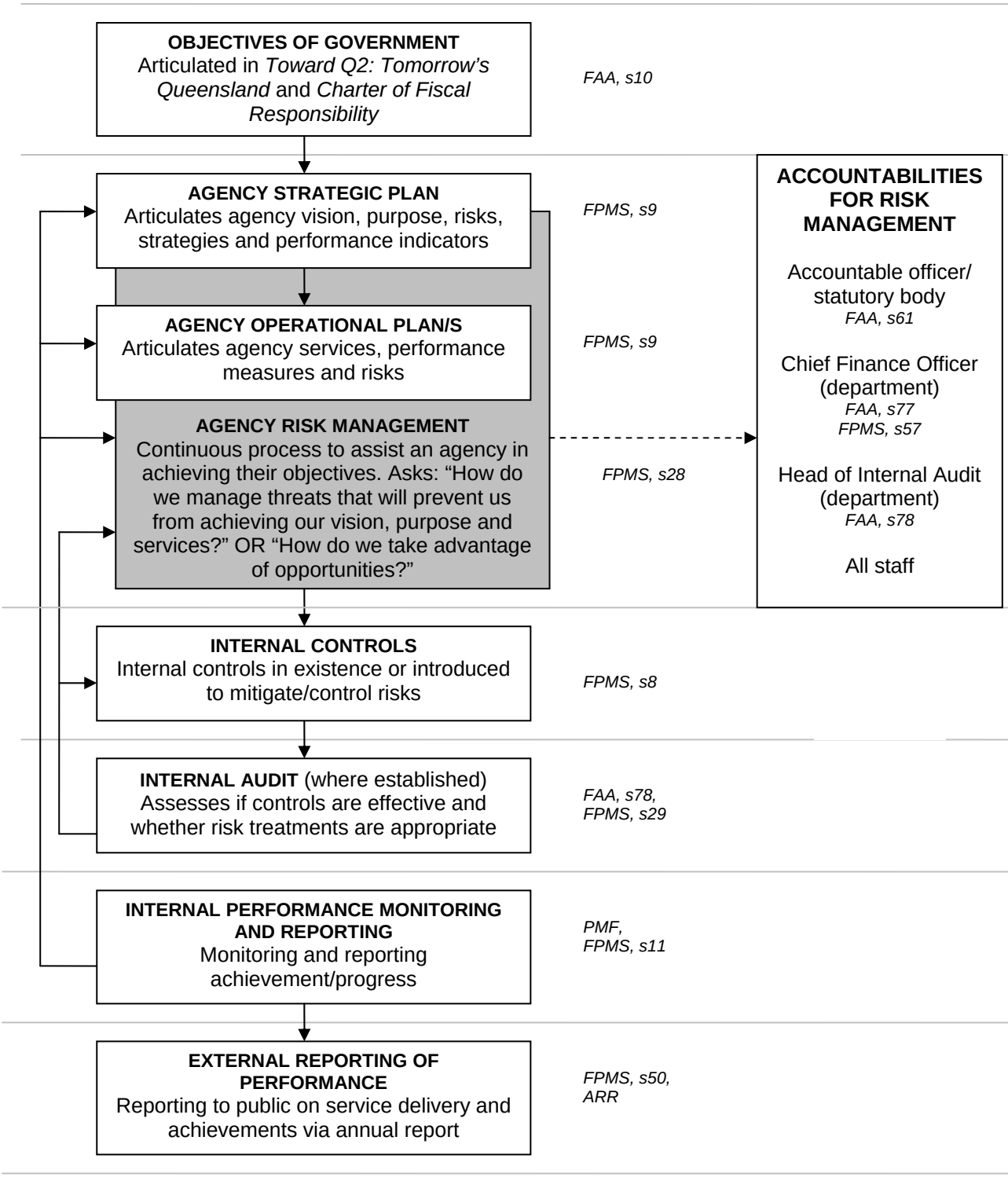
Consideration Points

Integrated risk management is about embedding risk into the agency's existing governance, planning, reporting and decision-making processes by developing a robust risk management framework. The consideration points contained below, designed to assist agencies with integrating risk management, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Has the accountable officer or statutory body developed and implemented a robust risk management framework appropriate to the size of their agency?	❑	❑	❑
• Does the agency have the necessary policies and procedures in place to support risk management?	❑	❑	❑
• Does the agency ensure all staff are informed of the risk management framework?	❑	❑	❑
• Does the agency have an explicitly stated risk management policy that complements their vision and strategic objectives?	❑	❑	❑
• Is there a designated risk management champion or unit to oversee the implementation of integrated risk management?	❑	❑	❑
• Does risk management have the demonstrated support and ongoing attention of executive management?	❑	❑	❑
• Does the agency have a risk management committee, or similar?	❑	❑	❑
• Is risk management communicated, understood, and applied throughout agency processes?	❑	❑	❑
• Is risk management integrated into existing governance and decision-making structures and performance-reporting systems?	❑	❑	❑
• Have control and accountability systems been adapted to account for risk management processes?	❑	❑	❑
• Have key performance indicators and critical success factors been identified and included in agency reports?	❑	❑	❑
• Does reporting on risk and risk management take place through existing management processes (e.g. performance reporting, ongoing monitoring, appraisals, internal auditing)?	❑	❑	❑
• Has the agency put in place effective initiatives to build risk management awareness?	❑	❑	❑
• Is written guidance (framework, policy, or operating principles) communicated throughout the agency to support individual units in building risk management into day-to-day operations?	❑	❑	❑
• Is the risk management process integrated into strategic and operational planning?	❑	❑	❑
• Does the agency identify and encourage education, training and development in risk management?	❑	❑	❑

Question	Yes	No	N/A
• Is the risk management framework reviewed at least annually? Notes:	❑	❑	❑

Application Guide 3 - Example of integrated risk management within an agency



Legend:
ARR: Annual Report Requirements for the Queensland Public Sector
FAA: Financial Accountability Act
FPMS: Financial and Performance Management Standard
PMF: Guide to the Queensland Government Performance Management Framework

Application Guide 4 – Establishing the context

Consideration Points

Establishing the context involves setting the parameters within which risks are identified, assessed and managed. The consideration points contained below, designed to assist agencies with establishing their risk context, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Has the agency implemented appropriate processes to identify both the internal and external context within which the agency operates (for example, use of environmental scanning)?	❑	❑	❑
• Has the risk been established with reference to the agency's objectives and strategic planning?	❑	❑	❑
• In determining the context, has the agency considered both challenges and opportunities?	❑	❑	❑
• Does the agency's environmental scanning process include a wide range of influences, trends and time horizons?	❑	❑	❑
• Does the agency consider both its external and internal contexts in relation to risk management?	❑	❑	❑
• Has the agency determined and documented its risk tolerances for the various components of its environment?	❑	❑	❑
• Is the context regularly reviewed to ensure it remains correct/appropriate to the agency's systems or controls?	❑	❑	❑
• Has the agency determined appropriate risk criteria that align with its objectives?	❑	❑	❑
<u>Agency-level risks</u>			
• Have the objectives of individual projects been considered as part of the risk management context?	❑	❑	❑
• Has the agency considered its capabilities and capacities (for example, funding, staff and technology)?	❑	❑	❑
<u>Cross-agency risks</u>			
• Does the agency consider the risk management practices of other agencies with which it delivers services?	❑	❑	❑
• Does the agency consider cross-agency risks and communicate these risks with relevant agencies?	❑	❑	❑

Question	Yes	No	N/A
<u>Whole-of-Government risks</u> • Does the agency consider the wider political and public sector environment? • Does the agency consider strategic risk issues (for example, climate change) that require coordination with other relevant agencies? • Does the agency consider the potential impact of risks on industry and the community? Notes:	❑ ❑ ❑	❑ ❑ ❑	❑ ❑ ❑

Application Guide 5 – Risk identification

Consideration Points

Risk identification is the process of identifying an agency's challenges and opportunities. The consideration points contained below, designed to assist agencies with identifying risk, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Are risks identified with reference to the agency's strategic plan, that is, the objectives and deliverables of the agency?	❑	❑	❑
• Are risks identified with reference to the agency's operational plans?	❑	❑	❑
• Are risks identified with reference to the agency's program and project plans?	❑	❑	❑
• Is risk identification linked to whole-of-Government policy and stakeholders?	❑	❑	❑
• Does the agency consider risks at the agency, cross-agency and whole-of-Government levels?	❑	❑	❑
• Does the agency identify both challenges and opportunities?	❑	❑	❑
• Does the agency consider both internal and external risks?	❑	❑	❑
• Does the agency have ongoing, comprehensive and systematic processes for identifying risks?	❑	❑	❑
• Are identified risks recorded in a risk register?	❑	❑	❑
• Are the staff involved in risk identification knowledgeable about the process or activity being reviewed and about the risks that must be managed as part of that activity?	❑	❑	❑
• Does risk identification involve appropriate stakeholders?	❑	❑	❑
• Are strategic risks sourced from/reflected in the agency's strategic plan?	❑	❑	❑
<u>Agency-level risks</u>			
• When identifying risks, does the agency consider the findings from past audits, evaluations and other assessments?	❑	❑	❑
• Does the agency review relevant corporate records to determine if a pattern exists (for example, financial or property losses, data/record losses, workplace health and safety reports)?	❑	❑	❑
• Does the agency consider risks identified from past	❑	❑	❑

Question	Yes	No	N/A
learning?			
• Does the agency undertake a gap analysis (that is the difference between existing practice and strategic plans, policies and practices)?	❑	❑	❑
<u>Cross-agency risks</u>			
• Does the agency consider how risks within the agency may affect other agencies?	❑	❑	❑
• Does a cross-agency committee assess risks associated with joint projects?	❑	❑	❑
• Is there a process for notifying relevant stakeholders of cross-agency risks?	❑	❑	❑
Notes:			

Application Guide 6 - Potential sources of risk

Below are some examples of potential sources of risk, separated between agency, cross-agency and whole-of-Government risk. In some cases the examples are listed in more than one level, which has been done to highlight that **the same challenge or opportunity can affect the agency in different ways**.

Agency risk	Cross-agency risk	Whole-of-Government risk
o policy and strategy	o policy and strategy	o policy and strategy
o agency reputation	o agency reputation	o political factors
o political factors	o political factors	o machinery of Government changes
o machinery of Government changes	o machinery of Government changes	o public expectations
o public expectations	o public expectations	o stakeholder relations
o stakeholder relations	o stakeholder relations	o media relations
o media relations	o media relations	o changing demographics
o industry developments	o industry developments	o globalisation
o changing demographics	o program activities	o security threats
o globalisation	o program delivery	o terrorism
o security threats	o service delivery	o emergency preparedness
o terrorism	o major projects	o natural disasters
o business continuity	o structure and reporting relationships	o economic trends
o emergency preparedness	o planning and priority setting	o competitive trends
o technology trends	o project management	o service delivery
o competitive trends	o environmental protection	o major projects
o business line activities	o accountability	o budgeting and resource allocation
o program activities	o transparency	o financial management
o program delivery	o natural disasters	o performance management
o service delivery		o project management
o alliances, partnerships		o environmental protection
o major projects		o security, privacy and confidentiality
o structure and reporting relationships		o legal liabilities and litigation
o planning and priority setting		o accountability
o budgeting and resource allocation		o transparency
o expenditure management		o Whole-of-Government reputation
o revenue and cost recovery		
o procurement and contracting		
o financial management		
o performance management		

Agency risk	Cross-agency risk	Whole-of-Government risk
o project management o change management o inventory management o asset management o human resources o information and knowledge o information technology o communications o statutory reporting o compliance with laws, regulations and policies o agreements and contractual obligations o workplace health and safety o environmental protection o security, privacy and confidentiality o legal liabilities and litigation o accountability o transparency o natural disasters		

Source: Based on examples provided in Treasury Board of Canada Secretariat, Integrated Risk Management Implementation Guide

Application Guide 7 – Risk analysis

Consideration Points

Risk analysis involves analysing the impact of a potential challenge or opportunity for the agency. The consideration points contained below, designed to assist agencies with risk analysis, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Does the agency have documented procedures to analyse the likelihood and consequence of each risk?	❑	❑	❑
• Does the agency conduct appropriate analysis of the nature and extent of the causes and impacts of the risks?	❑	❑	❑
• Are all risks analysed using a consistent methodology?	❑	❑	❑
• Are risk analyses adequately documented?	❑	❑	❑
• Has the agency examined and evaluated existing controls for the identified risks in terms of their strengths and weaknesses?	❑	❑	❑
• Are risk management controls regularly monitored?	❑	❑	❑
• Are appropriate levels of management and employees involved in the risk analysis process?	❑	❑	❑
• Does risk analysis include ensuring that the agency is not 'over-controlled' for the risks it faces?	❑	❑	❑
Notes:			

Application Guide 8 – Risk evaluation

Consideration Points

Risk evaluation involves determining which risks should be treated, and the priority for treatment implementation. The consideration points contained below, designed to assist agencies with risk evaluation, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Are risks found during the analysis process compared with the risk profile, risk appetite and risk tolerance established when the agency context was considered?	❑	❑	❑
• Has the agency fully integrated risks into their strategic and operational plans or established risk treatment plans for the management of risks, where necessary?	❑	❑	❑
• Are all risks within the agency evaluated using a consistent methodology?	❑	❑	❑
• Are evaluated risks prioritised to ensure treatment of the highest risks is considered first?	❑	❑	❑
• Are evaluated risks reviewed by an independent person to ensure risks are treated consistently?	❑	❑	❑
• Are risks re-evaluated over time to determine if priorities need to change?	❑	❑	❑
• Are risks reviewed or evaluated as part of the agency's own strategic and operational planning processes?	❑	❑	❑
Notes:			

Application Guide 9 – Risk treatment

Consideration Points

Risk treatment is the action, if any, taken to manage or mitigate a risk. The consideration points contained below, designed to assist agencies with risk treatment, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Are risks treated in accordance with the pre-determined risk criteria established by the agency?	❑	❑	❑
• Do proposed risk treatment plans include cost/benefit analyses of alternative courses or action?	❑	❑	❑
• Is the managing of risks and associated controls assigned to particular officers within the agency?	❑	❑	❑
<u>Agency-level risks</u>			
• Does the agency have formal, documented contingency plans for disaster recovery and business continuity?	❑	❑	❑
• Does the agency regularly review and test risk controls and contingency plans?	❑	❑	❑
• Are internal controls developed and documented to treat identified risks?	❑	❑	❑
<u>Cross-agency risks</u>			
• Does the agency have contractual agreements in place to manage cross-agency projects and their related risks?	❑	❑	❑
• Is there collaboration between agencies to agree risk treatments attached to identified cross-agency risks?	❑	❑	❑
• Are processes in place to ensure cross-agency risks and risk treatments are monitored over time?	❑	❑	❑
• Are Treasury and DPC informed of risk treatments, particularly if there are budget or policy implications?	❑	❑	❑
<u>Whole-of-Government risks</u>			
• Is there collaboration between agencies to agree on risk treatments attached to whole-of-Government risks?	❑	❑	❑
• Are processes in place to ensure whole-of-Government risks and risk treatments are monitored over time?	❑	❑	❑
• Are Treasury and DPC informed of risk treatments, particularly if there are budget or policy implications?	❑	❑	❑
• Have strategic risks been assigned specific risk treatments and are these shared with other agencies?	❑	❑	❑

Question	Yes	No	N/A
Notes:			

Application Guide 10 – Monitoring and review

Consideration Points

Risk monitoring and review is about determining whether risks still exist, whether new risks have arisen, whether the likelihood or impact of risks have changed, and to reassess the risk priorities. The consideration points contained below, designed to assist agencies with risk monitoring and review, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Does the agency have a regular monitoring and review process to evaluate the:			
o relevance of the risks to the achievement of the agency's objectives?	❑	❑	❑
o effectiveness of existing governance controls?	❑	❑	❑
o application of risk treatment plans in practice?	❑	❑	❑
o continuing relevance of the risk treatment plans to the agency's strategic and operational objectives?	❑	❑	❑
• Does the agency have policies and procedures in place for the reassessment of its risk profile and the opportunities provided by changes to the agency's internal and/or external environments?	❑	❑	❑
• Are adequate management information systems in place to facilitate risk monitoring and review requirements?	❑	❑	❑
• Is risk appetite assessed in light of changing circumstances (for example, at regular intervals, as well as at trigger points such as a State election)?	❑	❑	❑
• Are higher rated risks and associated current controls, and new controls/treatments reviewed regularly?	❑	❑	❑
<u>Agency-level risks</u>			
• Is there regular reporting of the status of risks (for example, to senior or executive management, risk management committee)?	❑	❑	❑
• Does the Head of Internal Audit (where established) provide assistance in risk management and identifying deficiencies in risk management? (refer section 78 of the *Financial Accountability Act 2009*)	❑	❑	❑
• Does the internal audit unit undertake regular reviews of the risk management process?	❑	❑	❑
<u>Cross-agency risks</u>			
• Do processes exist to ensure ongoing monitoring and reporting of cross-agency risks?	❑	❑	❑

Question	Yes	No	N/A
Whole-of-Government risks • Do processes exist to ensure ongoing monitoring and reporting of whole-of-Government risks? • Are strategic risks reviewed and evaluated through engaging appropriate processes such as environmental scanning? • Are the results of any strategic risk review process shared with other agencies facing similar risks? Notes:	❑ ❑ ❑	❑ ❑ ❑	❑ ❑ ❑

Application Guide 11 – Communication and consultation

Consideration Points

Stakeholders, both internal and external to the agency, should be consulted in the identification and management of risk. The consideration points contained below, designed to assist agencies with communication and consultation, are to be treated as a GUIDE ONLY. They are not to be considered to be exhaustive, and some points may not be applicable to all agencies.

Question	Yes	No	N/A
• Are all staff aware of their responsibilities with respect to risk identification, treatment and management?	❑	❑	❑
• Does the agency's risk management framework promote continuous improvement through learning and innovation?	❑	❑	❑
• Within the risk management framework, is there a process to ensure all stakeholders are identified?	❑	❑	❑
• Where appropriate, is a communication plan developed (for example, where a large number of stakeholders are involved)?	❑	❑	❑
• Are all key stakeholders consulted throughout the risk management cycle?	❑	❑	❑
• Are stakeholder perceptions of risk addressed?	❑	❑	❑
• Does the agency have processes to obtain input from Ministers and/or Cabinet on risks, their treatment and the Government's appetite for risk?	❑	❑	❑
• Are the agency's risks discussed regularly with Department of the Premier and Cabinet and Treasury?	❑	❑	❑
<u>Agency-level risks</u>			
• Is there regular communication between the Head of Internal Audit and the risk management committee (or equivalent)?	❑	❑	❑
• Does the risk management champion have direct access to the risk management committee (or equivalent) to raise concerns?	❑	❑	❑
• Is there a risk management reporting system in place that ensures all relevant parties are kept informed of the risks faced by the agency?	❑	❑	❑
<u>Cross-agency risks</u>			
• Are effective communication strategies implemented for cross-agency risks (for example, multi-agency committees, and regular executive management forums)?	❑	❑	❑

Question	Yes	No	N/A
• Do risk management champions communicate with their counterparts in other agencies?	❑	❑	❑
• Does the lead agency advise the appropriate risk analysis matrix to be followed for the cross-agency risk, and establish clear lines of communication and consultation?	❑	❑	❑
<u>Whole-of-Government risks</u>			
• Does the agency have processes to ensure Ministers and/or Cabinet are informed of high-risk or whole-of-Government risks?	❑	❑	❑
• Are effective communication strategies implemented for whole-of-Government risks (for example, multi-agency committees, and regular executive management forums)?	❑	❑	❑
• Do risk management champions communicate with their counterparts in other agencies?	❑	❑	❑
Notes:			

Application Guide 12 - Potential stakeholders

The table below provides a list of potential agency stakeholders that can be involved in risk management. This list is to be treated as a GUIDE ONLY. It is not to be considered to be an exhaustive list, and some stakeholders may not be applicable to all agencies.

Potential Stakeholder	Comments
Staff within the agency	• these may include staff members directly involved with identifying, analysing, evaluating, treating or reporting on a risk • if a risk is identified that may affect another agency business area, then this risk should be communicated to the other business area
Risk management champion	• may occur where a whole-of-agency or cross-agency risk is identified to ensure appropriate consideration and action taken • the risk management champion may also become involved if a 'risk owner' does not take responsibility for their particular risk
Accountable officer / Chief Executive Officer / agency executive management / statutory body board	• particularly to elevate risks from a business area level to an agency, cross-agency or whole-of-Government issue • other examples where executive-level reporting may be desirable include: o when additional staff and/or resources are required to manage a risk o when the consequence of a risk is considered to be extreme, or the probability of the risk occurring is very likely • this could be achieved through regular reporting of risks, or in a standard section in all briefing notes (this will assist with integrating risk within the normal processes of the agency)
Head of Internal Audit	• legislative responsibility to provide assistance and identify deficiencies in risk management
Agency's audit and risk management committee (or similar)	• the audit and risk management committee is not responsible for owning or managing risks – rather it comments on the risk management and assurance processes which are in place • the accountable officer / Chief Executive Officer / agency executive management may decide to raise particular risks with the audit and risk management committee, for advice on how to manage a risk or how a risk may interact with other risks
Staff in other agencies	• may be involved with identifying or managing a risk – particularly with cross-agency projects • may also seek expert advice from other agencies on how to manage a risk, for example, the Office for Aboriginal and Torres Strait Islander Policy may provide advice on risks with potential indigenous impacts
Department of the Premier and Cabinet and Treasury	• particularly where the strategic risks may have a whole-of-Government impact
Minister / Cabinet	• for risks with potentially significant impact on the Government's stated priorities for the State, it may be appropriate to elevate the risks to the Minister or Cabinet. • required when additional funding is considered necessary to manage risks • potential risks should be contained in all Cabinet Submissions • where considered necessary, the Minister or Cabinet may opt to

Potential Stakeholder	Comments
	advise Parliament of the potential risk
Public	• there may be instances where the public is engaged to assist with managing a particular risk, for example, the public was engaged to help manage the effects of the drought through water rationing • the public may also be engaged to assess its risk appetite regarding particular issues, for example, to assess the appetite of the public to adding fluoride to the drinking water • in order to obtain this level of involvement with the public, agency's may need to engage the media or survey companies
Partners or third party agencies	• may be considered stakeholders where a public private partnership is in place, or • where an agency uses a third party to deliver key services, for example Australia Post.
Interest groups, for example, employer groups, industry groups, unions	• instances may occur when the views of the public are sought, but targeted towards particular interest groups which may have expert knowledge or represent targeted members of the public. For example, for a risk that may impact on health services in Queensland, it may be beneficial to contact the Australian Medical Association
Suppliers	• while risk management may not need to be discussed with suppliers, where non-delivery by a supplier may compromise the agency's service delivery, communication may be necessary with the supplier to reinforce the importance of established timeframes

Useful resources

- AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines, Standards Australia (purchase required)
  http://www.saiglobal.com/
- Best practice in risk management - A function comes of age, The Economist Intelligence Unit, 2007
  http://www.kpmg.com.au/Portals/0/eiu_Risk_Management.pdf
- Framework for the Management of Risk, Treasury Board of Canada Secretariat, August 2010
  http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422
- Good Practice Guide – Managing risk across the public sector, Victorian Auditor-General's Office, 2004
  http://download.audit.vic.gov.au/files/Risk_guide.pdf
- HB 231:2004 Information security risk management guidelines, Standards Australia (purchase required)
  http://www.saiglobal.com/
- HB 436:2004 Risk Management Guidelines, Standards Australia (purchase required)
  http://www.saiglobal.com/
- Integrated Risk Management Framework, Treasury Board of Canada Secretariat (available but rescinded 27 August 2010)
  http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254&section=HTML
- Integrated Risk Management Implementation guide, Treasury Board of Canada Secretariat (available but rescinded 27 August 2010)
  http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/guide-PR-eng.asp?printable=True
- Queensland Government Insurance Fund
  http://www.qgif.qld.gov.au/
- Queensland Government State Disaster Management Group
  http://www.disaster.qld.gov.au/default.asp
- Queensland Pandemic Influenza Plan 2009
  http://www.premiers.qld.gov.au/publications/categories/plans/influenza-plan-2009.aspx
- Report to Parliament No. 6 for 2007 Beyond Agency Risk, Auditor-General of Queensland
  http://www.qao.qld.gov.au/
- Risk Management Matrix
  http://www.eventsportstephens.com.au/insurance/risk-management-tool/
- The Orange Book: Management of Risk – Principles and Concepts, HM Treasury, October 2004
  http://www.hm-treasury.gov.uk/d/orange_book.pdf
- Victorian Government Risk Management Framework, July 2007
  http://www.dtf.vic.gov.au/CA25713E0002EF43/pages/economic-and-financial-policy-victorian-risk-management-framework

If your agency has any questions concerning A Guide to Risk Management, please contact the relevant Portfolio Contact Officer (DPC) or Treasury Analyst (Treasury) for your agency.

Alternatively, email the Financial Management Helpdesk with details of your query and a response will be provided by the Financial Management Branch of Treasury:

Email: fmhelpdesk@treasury.qld.gov.au