

STRATEGIC RISK MANAGEMENT: GUIDELINES

**DEPARTMENT OF THE PREMIER AND CABINET
AND
QUEENSLAND TREASURY**

December 2007

CONTENTS

INTRODUCTION	2
Background	2
Context.....	3
WHOLE-OF-GOVERNMENT RISK MANAGEMENT FRAMEWORK	4
<i>Figure 1: The Whole-of-Government Risk Management Framework</i>	5
How do I do this?.....	7
What do I need to think about?.....	6
ORGANISATIONAL CONTEXT	8
How do I do this?.....	9
What do I need to think about?.....	9
ORGANISATIONAL CULTURE AND CAPACITY	11
How do I do this?.....	13
What do I need to think about?.....	13
CORPORATE GOVERNANCE	14
How do I do this?.....	15
What do I need to think about?.....	16
INTEGRATED RISK MANAGEMENT	17
How do I do this?.....	18
What do I need to think about?.....	19
IMPLEMENTATION AND REVIEW	21
How do I do this?.....	22
What do I need to think about?.....	23
ANNEXURE 1: LINKS AND REFERENCES.....	24

INTRODUCTION

These guidelines reflect and respond to the findings set out in 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 addition, they are consistent with the requirements of the *Financial Administration and Audit Act 1977* and the *Financial Management Standard 1997* and the principles set out in *AS/NZS 4360:2004 Risk Management*.

This document is a guide only, not a comprehensive reference for risk management. The guidelines seek to add to and contextualise the substantial body of existing material relating to risk management, including the Queensland Audit Office's better practice material.

Background

Risk management — the comprehensive process of identifying, assessing and responding to risks¹ — is not an end in itself. When undertaken effectively, it can deliver a range of benefits, by:

- improving planning processes by enabling the key focus to remain on core business and helping to ensure continuity of service delivery;
- reducing the likelihood of potentially costly 'surprises' and preparing for challenging and undesirable events and outcomes;
- improving efficiency and general performance;
- contributing to the development of a positive organisational culture, in which people and organisations understand their purpose, roles and direction; and
- improving accountability and governance — in relation to both decision-making and outcomes. This is particularly important for public sector entities, which exist to deliver outcomes for the benefit of the public.

Risk is an ever present element of public policy and government service delivery. In the *AS/NZS 4360:2004 Risk Management Standards*, risk is defined as "the chance of something happening that will have an impact on objectives". Effective risk management allows agencies to have increased confidence that they can deliver desired outcomes, manage risks and threats to an acceptable degree and make informed decisions about opportunities.

¹ AS/NZ 4360:2004 Risk Management Standards

Context

The recent Auditor-General of Queensland Report to Parliament No. 6 for 2007: *Beyond Agency Risk* identifies the need for the Government to deal with both strategic and operational risks at three levels: agency, portfolio and whole-of-Government. Strategic risks are risks that could affect the achievement of the organisation's vision and strategic objectives. Operational risks are those which could impact on the organisation's effectiveness and efficiency.

Risk management is not a "one-size-fits-all" issue, nor is it simply about compliance. Good risk management techniques are sensitive to an organisation's needs, environment and internal capacity to manage risks. However, there are techniques and approaches that can translate across different types of agencies and different sizes of organisations. The critical challenge is often one of scalability – implementing the most appropriate mechanisms that meet the agency's need.

The following sections set out a range of practical guidelines under six key areas, consistent with the Auditor-General's recommendations, to support improved risk management:

- establishing a **whole-of-Government risk management framework**;
- establishing and reviewing the **organisational context**;
- embedding risk management into the **organisational culture**;
- ensuring risk management is part of robust **corporate governance**;
- ensuring risk management is **integrated with planning**, decision-making and reporting processes; and
- ensuring agencies document, **implement and review** their risk management framework.

Each section discusses factors that contribute to the success of these areas of risk management, provides practical tips on making progress and sets out points to consider to assist agencies in assessing their performance and progress in each area.

The tips and points are by no means a complete or definitive listing, and should be tailored by agencies to suit their specific risk environments. In some cases the points are listed in more than one area. This has been done deliberately to highlight to readers that certain features of good practice may satisfy more than one element of good risk management and to allow stand-alone reference to each success factor.

Annexure 1 to these guidelines provides references for additional information.

WHOLE-OF-GOVERNMENT RISK MANAGEMENT FRAMEWORK

Strategic risk management is a means of coordinating, overseeing and modelling the interrelationship of important risk factors across an organisation's functions.² In the context of these guidelines, strategic risk management applies to the process of considering and managing whole-of-Government risks across the Queensland public sector.

Strategic whole-of-Government risks can include:

- agency-level risks which become risks for the State, due to their size or significance, the wider impact of measures to treat them, or poor management by agencies, and therefore need to be addressed at a whole-of-Government level;
- inter-agency risks, requiring management by more than one agency for treatment to be effective; and
- State risks, which are beyond the boundaries of any one agency due to their magnitude and/or impact on service delivery and call for a response across agencies, co-ordinated by a central agency.³

As a consequence of whole-of-Government approaches to projects becoming more common, there is an increased awareness of the need to manage risks at a strategic whole-of-Government level. All agencies, in conjunction with central agencies, need to be aware of and understand that there are significant strategic risks at the State level, and to pay greater attention to identifying and managing them. All agencies need to understand the risks that impact on the State in order to effectively integrate risk management into their governance and management structures.

Agencies are responsible for applying the *Australian Standard (AS4360)* for risk management to support the identification, assessment, treatment, monitoring and review of risks. Effective application of the Standard should lead to agencies improving their risk management capability through learning the lessons of practical risk management.

It is expected that the majority of risks will be managed by agencies internally. Only the most significant risks facing agencies, those which they are unable to manage alone, need to be escalated beyond the individual agency into the whole-of-Government risk management framework. The majority of risks will continue to be managed by agencies applying AS4360 internally.

² "The Long Winding Road", www.riskmanagementmagazine.com.au 10 August 2007

³ Auditor-General of Victoria (June 2004) *Managing Risk Across the Public Sector: Good Practice Guide*.

It is fundamentally the role of Chief Executive Officers (CEOs) and their executive management teams to ensure there is a robust internal process that is capable of managing their agency's strategic risks.

Agencies should ensure that the Department of the Premier and Cabinet (DPC) Portfolio Contact Officers (PCOs) and Queensland Treasury (Treasury) Analysts are involved in the regular review and monitoring of strategic risks. It is incumbent on agencies to ensure that PCOs and Treasury Analysts have a good understanding of the agency's strategic risks, appetite for risk and treatment of existing risks, as well as the risks that may need to be escalated to Cabinet.

Risks should be dealt with as part of any planning and implementation process and also as part of Implementation Sections and Plans in Cabinet submissions, which are required by the Cabinet Handbook.

DPC and Treasury will support agency risk management by:

- effective horizon scanning, i.e. identifying medium and long-term socio-economic trends and alerting relevant agencies to the implications of these trends. This will in part be achieved by DPC in its management of the Government's Policy Development Program⁴;
- providing advice and support on strategic risk management and the escalation of strategic risks as required (including via these guidelines);
- identifying, coordinating and monitoring strategic risks that may have a cross-agency or whole-of-Government impact, and reporting on the Government's overall risk portfolio to the first Strategic Cabinet meeting each calendar year; and
- supporting the consideration of strategic risks in the context of the Budget process, as appropriate.

The Strategic Cabinet meeting and State Budget processes are two established means of ensuring Government has a good overview of whole-of-Government strategic risks. These processes allow for the detailed consideration of key strategic risks at significant points in the planning cycle.

The whole-of-Government framework also allows for the escalation of strategic risks throughout the year, with any financial considerations being subject – as normal – to Cabinet Budget Review Committee (CBRC) deliberations. Risk management, however, is core agency business and the identification and assessment of strategic risks will not necessarily be a trigger for additional funding. Rather, risks may present an opportunity to reduce the Government's exposure in a field, by reprioritising Government expenditure or investment in an area.

⁴ See the Premier's Statement on *Queensland's Future* [Hansard, 578-579; 6 March 2007].

Feedback from Cabinet and CBRC discussion of strategic risks, both through formal consideration of risks through the Strategic Cabinet meetings or through Budget deliberations and assessment of risks through the regular Cabinet cycle, will be cascaded back to agencies through existing processes. Cabinet Legislation and Liaison Officers play a critical role in ensuring this feedback reaches the appropriate officers in agencies.

Agencies need to bear in mind that risk does not necessarily equate to challenge. Risks can often signal significant opportunities, and executive management needs to maintain the balance between robust risk management practices and guarding against a compliance regime or inhibiting innovation.

How do I do this?

- Ensure that strategic risks are discussed at agency and portfolio forums and ensure there is a common understanding of the risks, their likelihood and impact, and their treatment.
- Ensure that strategic risks are treated as a critical element of the agency planning cycle, and included in Budget preparations such as the development of *Portfolio Service Plans*.
- Clearly discuss potential risk issues and any risk mitigation strategies in Cabinet and CBRC submissions and other briefings and papers.
- Clearly assign management of portfolio risks to a lead agency, and a lead contact in that agency, with support from other agencies that share the risks.
- Use structures such as joint meetings of executive management groups to regularly review portfolio risks.
- Ensure that executive management has a clearly articulated escalation point for strategic risks.
- Involve Ministers in the regular identification and review of strategic risks.
- Discuss agency and portfolio strategic risks with PCOs and Treasury Analysts on a regular basis.
- Review and update strategic risks annually, in advance of discussion at the first Strategic Cabinet meeting of each calendar year.

What do I need to think about?

- Does the agency have a clear understanding of its responsibilities with respect to the whole-of-Government strategic risk framework and the roles and responsibilities of central agencies?
- Has the agency identified its strategic risks and escalated them (as appropriate) for consideration at the first Strategic Cabinet meeting of each calendar year?
- Has the agency been advised of the outcomes of the first Strategic Cabinet meeting of each year, so they can take appropriate action in avoiding/mitigating escalated risks?
- Does the agency escalate risks as appropriate to the CEO Forum and Policy Development Program CEO Committees?
- Does the agency document its strategic risks in its *Portfolio Service Plan*, for consideration as part of the Budget process?

- Does the agency regularly review risks with its PCO and Treasury Analyst?
- Are all agencies in the portfolio aware of: (a) each agency's risks; (b) portfolio risks; and (c) who is responsible for leading management of each risk?
- Does executive management meet with its counterparts in the portfolio to consider strategic risks?
- Does the agency seek Ministerial feedback on strategic risks, their treatment and the portfolio's appetite for risk?
- Is ownership/responsibility for coordinating whole-of-Government risk identification clearly attributed to a person/unit and communicated within the agency?

ORGANISATIONAL CONTEXT

To be effective, risk management has to be considered in the context of the overall organisational environment, the agency's aims and objectives and key stakeholders. The organisational context has a key bearing on the development of the corporate risk profile. The ability of modern organisations to meet their organisational objectives is dependent on a wide array of factors, both internal and external to the organisation.

The organisational context must be sufficiently broadly defined to include a wide range of trends, influences and time horizons. This will enable the timely identification of emerging risk both at, and beyond, the agency level. The defined organisational context should be also regularly and systemically examined to ensure that it remains appropriate and desirable.

In determining the corporate risk profile, agencies need to collect information at the strategic, program and operational levels to inform their understanding of the context in which they operate. Such information includes the range of risks they face, the likelihood of such risks occurring and the potential impacts. Knowledge of risks and their treatment also assists in building the corporate risk appetite, which is the amount of risk the agency will accept.

Environmental Scanning

Environmental scanning is a process of identifying emerging issues, situations, and potential pitfalls that may affect an organisation's future. Environmental scanning increases the agency's awareness of the key risks it faces, and the characteristics and attributes of these risks. Key questions for agencies to consider in undertaking this analysis include:

- the **type** of risk – technological, financial, health, safety etc;
- the **source** of risk – external (political, economic, natural disasters) or internal (reputation, security, knowledge management, etc);
- **what** is at risk – area of impact and the type of exposure (people, reputation, program results, assets etc); and
- the level of **control** – the degree to which the agency can influence, affect or manage the risk.

Understanding the organisational context and conducting an environmental scan can assist an agency in identifying key risk areas and differentiating between the types of risks – for instance, specific event risks and risks that cut across the entire agency. The scan also allows the agency to set a strategic direction for risk management, which can be amended, or adjusted, as more information comes to light, or as the agency's capacity to manage risks increases.

How do I do this?

- Conduct regular environmental scans to clearly define the internal and external context in which the agency operates.
- Use environmental scanning information to identify potential risks as, or before, they emerge.
- Use standard analytical tools, such as SWOT and PESTLE analyses, to review the environment in which the agency operates.
- After identifying and assessing risks, identify the agency's risk appetite – the level and quantity of risk it is willing to take on – and communicate this to all staff.
- Assess, with relevant agencies, risks that cut across portfolios – and their treatment, ownership and review.
- Ensure that executive management keeps the Minister informed and involved in discussions of strategic risks, their identification, assessment, treatment and review.
- Use the planning and resource allocation process to review risks and their treatment.
- Communicate risks to key stakeholders.

What do I need to think about?

- In developing its risk management plans, has your agency taken account of its internal and external environment?
- Does the agency have a formal environmental scanning process that feeds into the identification and assessment of strategic risks?
- Does the agency's environmental scanning process include a wide range of influences, trends and time horizons?
- Is the environmental scanning process documented and communicated to all staff?
- Are all staff aware of the tools that can be used in environmental scanning at all levels?
- Are the timeframes for reviewing the organisational context documented, communicated and adhered to?
- Is risk management included in all strategic, program and operational planning activities?
- Is there agreement across the organisation on which risks are unavoidable and not within the agency's ability to manage? Is this documented?
- Are the organisation's risk management framework and strategies appropriate, given the organisation's context and key risks?
- Has the agency established risk criteria – the level of risk it is prepared to accept from the various components of its environment? Is this documented?
- Has the agency identified opportunities resulting from risk identification? Have these been fed into the agency's organisational planning process?
- Has the agency systematically identified the full range of risks it faces, and the sources and consequences of those risks?
- Has the agency analysed the likelihood and consequence of each risk?

- Where risks have been identified, but evaluated as acceptable, has the rationale been documented?

ORGANISATIONAL CULTURE AND CAPACITY

Organisational culture has a key part to play in effective risk management. It ensures that the right level of priority and attention is given to risk management and that organisational objectives and priorities are sensitive to risks and their treatment.

A key 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 organisation's business.

The integration of risk management into standard business practices (including decision-making and planning) is supported by a corporate philosophy and culture that encourages everyone to manage risks. This can be accomplished in a number of ways, such as by:

- senior managers championing risk management;
- promoting the view that everyone is a risk manager;
- 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.

The lead in implementing an effective risk management framework must come from the top of any organisation, and the role and responsibility of executive management (or the Board) can never be understated. It is the role of executive management to set the vision, lead by example, empower management and staff (including specialists) and appoint a body to independently review the process. It is also the role of executive management to ensure that enough time, energy and resources are devoted to getting risk management right, including investing in appropriate training for all staff.

Risk Management Champion

A suggested approach is the appointment of a "Risk Management Champion", who would normally report to the Director-General (or their equivalent) or executive management of an agency. The Risk Management Champion is a senior executive officer with vision, drive and determination, and the authority and responsibility to make things happen. They would be responsible for driving risk management awareness, integration, policies and strategies and promoting, across the organisation, a culture that supports:

- increased awareness of risk management techniques and processes;

- uniform understanding of the agency’s key strategic, program and operational risks and challenges (including cross-agency and whole-of-Government 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 – particularly policy roles – and how it can inform advice to Ministers; and
- a broad understanding of the relationship between the organisation’s risks and whole-of-Government risks.

Executive management needs to ensure that Risk Management Champions have the authority, support and space to promote this culture. Cultural change does not occur overnight and will require a sustained effort on behalf of all staff.

Supportive Work Environment

A supportive organisational culture is one where expertise, learning and innovation are rewarded and celebrated, and where a “no surprises” rather than “no risks” philosophy is encouraged.

Organisations with a supportive work environment tend to:

- promote learning – encouraging staff to learn and gain knowledge, fostering an environment that motivates staff to learn and value knowledge, expertise, new ideas and innovation;
- learn from experience – valuing experimentation, sharing lessons from past successes and failures and bringing this learning to business planning; and
- demonstrate management and leadership – 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.⁵

Providing the right risk management resources, training and awareness programs for staff is critical in this regard.

⁵ *Integrated Risk Management Framework* [Treasury Board of Canada; April 2001]

How do I do this?

- Appoint a Risk Management Champion to promote a risk management culture in the agency.
- Develop and implement a risk management policy throughout the agency.
- Implement a communication strategy to disseminate the policy and facilitate understanding across the agency.
- Ensure risks are owned by senior managers and business units, and these risks are considered as part of the agency's planning and reporting cycle.
- Create a forum for senior managers to discuss risks, their treatment and current/emerging issues.
- Identify appropriate training to support staff in developing appropriate skills.
- Commit to ongoing staff training on risk management to ensure corporate knowledge is maintained.

What do I need to think about?

- Is there an explicit, stated risk management policy that has been communicated to all staff?
- Does risk management have the demonstrated support and ongoing attention of executive management?
- Are senior managers involved in the identification and assessment of the agency's risks?
- Has an appropriate Risk Management Champion been appointed?
- Does the agency apply risk management to the whole of its business operations and services?
- Does the agency ensure that all risk management actions directed by executive management are formally reported back to them to confirm their progress or completion?
- Does the agency have the knowledge and skills to manage risks?
- Are strategies in place (including education and training) to develop knowledge and skills?
- Does executive management directly lead and strategically manage the agency's risk management process?
- Has the agency determined who will be responsible for identifying strategic risks?
- Are executive management open to having potentially adverse situations brought to their attention?
- Are strategic risks and risk management plans regularly communicated to all staff?
- Are the benefits of risk management communicated to all staff?
- Does executive management take responsibility for allocating adequate resources for the ongoing implementation of risk management policies, plans and procedures?
- Is risk management a fundamental element of all existing organisational frameworks?
- Is risk management reflected in the agency's corporate values?

CORPORATE GOVERNANCE

Risk management is about improving an organisation's ability to manage its business more effectively. It is focussed on unlocking potential, building capacity and achieving an organisational culture that supports dialogue about risk, risk appetite and the potential impacts of specific risks. Integrating risk management into corporate governance may not be successful if the act of integration is seen as "bolting on" an additional requirement to existing procedures.

Risk management is not an additional compliance-driven exercise in accountability. Successful alignment of risk management and corporate governance is predicated on concrete progress in four key areas:

- establishing a **corporate focus**, where there is an identifiable source of risk management expertise in the organisation and senior managers come together on a regular basis to discuss risk management issues;
- communicating the **corporate direction**, where the Board sets a clear direction and strategy for risk management, including articulating the organisational risk appetite and giving a clear mandate for effective risk management;
- integrating risk management into **decision-making** structures, where risk management is not a separate process, but a key consideration at all parts of the decision-making chain, including being factored into advice to Ministers; and
- building **organisational capacity**, where the organisation's executive management invests time and resources to build momentum and capacity, including ensuring that there is a shared language of risk management and a common understanding of the principles, tools and processes of risk management. Building organisational capacity is a long-term commitment.

Successful integration of risk management with corporate governance can be characterised by success in each of the following areas:

- organisations creating a supportive environment, where there is regular and open debate and dialogue on risks and risk management, where risks are collectively owned and where there has been up-front investment in getting the groundwork right;
- executive management setting a clear vision, establishing a specific and broad mandate for effective risk management across the organisation, and following up to ensure the commitment is recognised and valued throughout the organisation;
- an identifiable team of specialists and knowledge experts supporting more detailed consideration of risks and risk treatment strategies at operational levels, the identification of strategic and whole-of-Government risks and taking responsibility for ensuring a clear, common language for risk management;

- responsibility for risks being clearly distributed, with roles and responsibilities clearly defined across the organisation and executive management recognising their leading role in managing strategic risks;
- risks being regularly reviewed and reported to the executive management and a designated committee of executive management being responsible for independently reviewing risk management practices and procedures on (at least) an annual basis;
- risk management being effectively linked to corporate planning and priority-setting processes, particularly to resource allocation and other core decision-making processes, and risk issues being factored into advice to Ministers;
- implementation of risk management tools, practices and procedures being scalable, to ensure that the proposed risk management system is sensitive to the organisation's needs and environment and is fit for purpose; and
- building capacity, where executive management invests time and resources to build momentum and capacity, including by ensuring there is a shared language of risk management and a common understanding of the principles, tools and processes of risk management. Building capacity is a long-term commitment.

How do I do this?

- Integrate a risk management focus into the agency's corporate governance, including in advice to the Minister.
- Clearly document and implement a risk management framework that establishes organisational roles and responsibilities, risk management steps and activities and associated timeframes.
- Have the risk management framework approved and regularly reviewed by executive management and a risk management committee (whether combined with an audit committee or not). Such a committee would be responsible for overseeing the risk management framework, systems, controls and procedures and providing assurance on their efficiency and relevance.
- Ensure there are clear roles, responsibilities and accountabilities to support the organisation's risk management framework and its application.
- Monitor and obtain regular updates of the organisation's risk profile and risk treatment progress.
- Integrate risk management into existing organisational planning, reporting and controlling frameworks (regular exception reporting, scorecards, snapshots).

What do I need to think about?

- Are the appropriate structures in place for effective risk management?
- Is there a senior-level risk management committee? Alternatively, are risk management issues discussed as a regular agenda item at executive management meetings?
- Are responsibilities for promoting risk management, identifying risks and ownership of risks clearly distinguished and have these been communicated throughout the agency?
- Is there a clearly documented and implemented risk management framework that establishes organisational roles and responsibilities, risk management steps and activities and associated timeframes?
- Is the risk management framework approved and regularly reviewed by executive management?
- Does strategic risk reporting reflect the accountabilities and risk appetite of executive management and the Minister?
- Is risk management included in organisational planning, reporting and resource allocation frameworks?
- Do you consider the risk management practices of other organisations with whom you do business or engage (for example, other agencies, contractors and service providers)?
- Has the Australian Standard on Risk Management been taken into consideration in developing the agency's risk management policies, strategies and treatment plans?

INTEGRATED RISK MANAGEMENT

Effective risk management requires the integration of risk management practices with business standard processes. This helps to ensure that risk management is aligned with agency objectives and priorities.

In order to achieve this integration, organisations need to ensure their risk management systems do not operate in isolation and are applied as part of their strategic and business planning considerations. Where risk management has reached a high level of maturity in organisations, there are usually clear links to corporate priority setting and resource allocation processes.

For risk management to be a consideration in priority setting and resource allocation, it needs to be integrated within existing governance and decision-making structures at the operational, program and strategic levels. Clear links should be established between risk management, Government policies and priorities and corporate objectives (vertical integration) and into policy and operations (horizontal integration).

Agencies should consider drawing up a portfolio view of risks to assist this process and support Ministerial consideration of priorities and resource allocation.

Successful integration also requires that elements of the risk management framework are implemented consistently throughout the organisation.

Vertical integration

The establishment and communication of the agency's risk management priorities, objectives and operating principles are vital to providing overall direction, and ensure the successful integration of the risk management function into the organisation. Using these instruments can reinforce the notion that risk management is everyone's business.

All agencies will need to find their own ways to align risk management with the agency's priorities. Agencies will face common considerations, including:

- aligning risk management with objectives at all levels of the agency;
- introducing risk management components into existing strategic, program and operational planning processes;
- communicating executive management's decisions on acceptable levels of risk; and
- improving control and accountability systems and processes to take into account risk management and results.

Aligning risk management with planning and resource allocation is only part of the task – risk management also has to be aligned with evaluation and reporting mechanisms, to ensure that risks can be monitored and updated easily and that risk treatment strategies can be monitored, evaluated and improved. Reporting also facilitates learning and improved decision-making by assessing both successes and failures, monitoring the use of resources and disseminating information on best practices and lessons learned.

Horizontal integration

The risk management framework also needs to be integrated into an agency's systems, processes and practices and, in particular, the planning and decision-making processes at each level of the organisation. When undertaken in conjunction with other strategic, program and operational management processes, risk management will be more effective as well as economical.

As *AS/NZS 4360:2004* suggests, the risk management plan should aim to incorporate risk management into critical business processes, particularly policy development, strategic, program and operational planning and change management processes. When risk management is integrated into strategic, program and operational planning and regular reporting cycles, the additional risk management information available should enable more informed planning and decision-making at the agency, portfolio and whole-of-Government levels.

Information should be shared throughout an agency to ensure there is a coordinated approach to identifying and mitigating risks. Senior management should be responsible for driving this. Aggregation of information at the agency level will add significant value to priority setting and improved decision-making.

Identifying, monitoring, reporting and controlling risks should form part of an agency's regular reporting and performance monitoring frameworks. This should lead to more proactive risk management. All business areas across the organisation should be required to incorporate risk management into their normal planning and reporting cycles.

In considering risk, business areas should consider the potential impact of risk treatment on other business areas. They should also be encouraged to share best practice/lessons with the rest of the agency and across agencies.

How do I do this?

- Ensure risk management is aligned with corporate objectives and Government policies and priorities.
- Ensure elements of the risk management framework are implemented consistently throughout the organisation – at each organisational level and across all organisational functions.

- Encourage ownership of risk management at the senior management level by having management establish the agency's risk appetite and risk management strategy.
- Include discussion of strategic risks where appropriate at the executive management and Ministerial levels.
- Include strategies for integrating risk management into systems, processes and practices in the risk management plan.
- Consider risk management in all planning and critical business processes including strategic planning, program planning, operational planning, policy development and major initiatives.
- Incorporate risk management into the organisation's usual reporting and performance monitoring systems.
- Demonstrate that risk management has been driven down through the agency through incorporating risk management expectations into key performance indicators, employee performance agreements and work descriptions.
- Invest in integrated risk management infrastructure that can store and share risk management information across the organisation.
- Provide strategic risk management education at the executive management level.
- Develop ownership of risk management oversight at the executive management level.
- Develop a risk management framework that applies to your organisation.
- Use common risk management language and concepts.
- Complete a risk management plan on a regular basis.
- Communicate about risk using appropriate channels and technology.
- Ensure executive management reviews risk reports for the organisation.

What do I need to think about?

- Does the agency have an endorsed risk management plan which considers strategies for the integration of risk management throughout the organisation?
- Does the agency have a concise strategic risk register? Has this been signed off by executive management and communicated to all staff?
- Does the agency identify and assess the significant risks relating to each of its goals, objectives and planned outcomes?
- Are risk assessments linked to policies, programs and priorities?
- Are risk assessments linked to Government policy, organisational goals and stakeholders?
- Is agency expenditure reflective of the corporate risk profile?
- Is risk management considered in planning and business activities at all levels?
- Is risk management included in reporting and performance monitoring at all levels?
- Is risk management included in managers' responsibilities?
- Is risk management information shared across the organisation?
- Does the agency regularly monitor risk management by all business areas to check for consistency?
- Has executive management been given clear ownership of overseeing risk management?

- Has senior management established and does it regularly review the agency's risk appetite and risk management strategy?
- Has risk management information been collated and considered at the agency level?
- Has risk management training been provided to staff, management and, in particular, executive management?
- Does the agency measure and monitor improvements to business processes as a result of its risk management strategies (e.g. reduction in the cost of claims, number of incidents etc)?

IMPLEMENTATION AND REVIEW

There is no “one size fits all” risk management framework that can be applied across the varied types and sizes of Government entities. Executive management needs to consider the type of framework that will best integrate with its particular operational context and external environment including: business operations; reporting mechanisms; culture; workforce skills; budget; supporting infrastructure; standards and legislative requirements; organisational structure; and delegations of authority and responsibility.

The risk management framework should guide staff by:

- describing the risk management process;
- establishing roles and responsibilities;
- providing methods for managing risk; and
- providing for the evaluation of the objectives and results of risk management practices.⁶

Agencies should have a documented and up-to-date risk management framework, policy and plan. A risk management framework, written in plain English, will assist in the communication and training associated with the implementation of the framework. 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 organisation.

Risk management is not just about the review of risks themselves. Organisations need to review their risk management systems to ensure they are delivering effective and robust risk management that is fit for the organisation’s purposes. Risks, the corporate risk profile, risk management systems and the risk environment are all constantly changing and evolving. The regular review of systems and risks is needed to: ensure the organisation’s procedures are working effectively; provide assurances to the executive management that the organisation’s risk portfolio has been properly identified and assessed; and ensure that risks are being effectively treated.

Reviewing the risk management framework should be a role for a committee of the executive management. Rather than being responsible for managing the risks themselves, this committee would be responsible for regularly reviewing and evaluating the risk management framework and systems to provide assurance on their efficiency and relevance. It is good practice for such reviews to be carried out at least annually, to ensure the procedures remain fit for purpose and are up-to-date. Executive management should also take care not to confuse reviewing risk

⁶ Treasury Board of Canada Secretariat (2001) Integrated Risk Management Framework p20.

management procedures with risk management itself. Reviewing the process is not a substitute for managing or treating risks.

Development of a risk management policy and annual risk management plans should underpin the effective implementation of risk management in an organisation. This should also be supported by management and communicated across the organisation.

Effective implementation also requires adequate and appropriate resourcing. Overall responsibility for implementation of a risk management framework for an agency should ideally rest at the executive management level with appropriate resources provided to support the implementation and review.

It is important for an organisation to monitor and regularly report to executive management against identified risks given the dynamic and constantly changing nature of organisational risks. At a minimum, an annual review of the entire risk management process should be undertaken. It is important to also consider “lessons learned” and ensure that management learns from past experiences, both positive and negative, and use these to enhance current processes. It is also important to assess whether all elements of the risk management framework have been implemented effectively.

How do I do this?

- Document the agency’s selected risk management framework in plain English.
- Provide all staff with access to the risk management framework.
- Promote the risk management framework and its associated benefits through all management levels and the Risk Management Champion.
- Involve staff from all levels and functions in the implementation strategy.
- Regularly review the risk management framework, policies, plan and systems. Such reviews should consider whether all elements of the risk management framework have been implemented effectively.
- Regularly review the performance of adopted risk management strategies against set criteria to measure and report their effectiveness and determine future risk treatment needs.
- Assign responsibility for review and monitoring to a risk management committee or add this to an existing board of management’s responsibilities.
- Provide adequate resourcing for the risk management function, whether this be by creating a new position(s) or adding it to an appropriate business area of the organisation.
- Establish a risk reporting system (consider an electronic database).
- Ensure regular communication of critical risk information, including at Ministerial level.
- Provide training in relation to risk management across the organisation.
- Incorporate risk management into strategic, program and operational planning and resource allocation.

What do I need to think about?

- Is there a documented risk management framework approved by executive management that is accessible by all staff e.g. on the intranet?
- Does the agency's framework enable integration with organisational operations, reporting mechanisms, culture, workforce skills, budget and supporting infrastructure?
- Does the framework reflect the agency's tolerance and appetite for risk at the strategic, program and operational levels?
- Does executive management review the risk management framework – and not just risks themselves – on an annual basis?
- Is there a documented risk management policy and plan?
- Is the outcome of the annual risk management plan reported to the Risk Management Committee (or its equivalent)?
- Are existing practices and processes (including culture, integration, and constraints) reviewed when developing your annual risk management plan?
- Are there regular risk management meetings with management?
 - Who participates in these meetings?
 - How frequent are these meetings?
 - What authority do these meetings have?
- Has the agency developed, where relevant, treatment plans for its strategic risks? Are these plans linked into the corporate strategic plan?
- Are risk treatment plans monitored to identify business improvements and changed outcomes?
- Is critical risk information regularly communicated to senior management?
- Has the agency devoted resources to ensuring an appropriately skilled person(s) can support implementation and monitoring of risk management in the organisation?
- Has an effective risk reporting system been developed?
- Is feedback regularly provided to the risk owner?
- Is training on risk management available for staff where required?
- Does the agency regularly review its risk management framework, policies, plan and systems?
- Does the agency regularly review the performance of adopted risk management strategies against set criteria to measure and report their effectiveness and determine future risk treatment needs?

ANNEXURE 1: LINKS AND REFERENCES

ACT Insurance Authority (2004) *Guide to Risk Management and Risk Management Toolkit*

AS/NZS 4360:2004 *Risk Management*

ASX Corporate Governance Council (March 2003) *Principles of Good Corporate Governance and Best Practice Recommendations*

Auditor-General of Victoria (June 2004) *Managing Risk Across the Public Sector: Good Practice Guide*

Auditor-General of Victoria (June 2007) *Managing Risk Across the Public Sector: Toward Good Practice*

Casualty Actuarial Society Enterprise Risk Management Committee (2003) *Overview of Enterprise Risk Management*

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (September 2004) *Enterprise Risk Management – Integrated Framework*

CPA Australia (2004) *Risk Management Integration in the Public Sector*

HB436:2004 *Risk Management Guidelines (Companion to AS/NZS 4360:2004)*

Grace, D (1999) *Using AS3806 as a Tool to Develop an Effective Risk Management Program*, paper presented at *Managing Risk in the New Millennium: A Public Sector Perspective*

KPMG (2001) *Enterprise Risk Management: An Emerging Model for Building Stakeholder Value*

Lund, T (1999) *Practical Approaches to Risk Management*, paper presented at *Managing Risk in the New Millennium: A Public Sector Perspective*

Ministry of Premier and Cabinet, Western Australia (1999) *Guidelines for Managing Risk in the Western Australian Public Sector*

New South Wales Audit Office (2002) *Managing Risk in the NSW Public Sector*

Queensland Auditor-General (October 2000) *Governance and Risk Management: Self Assessment Program for Departments*

Queensland Auditor-General (September 2007) *Beyond Agency Risk*

Queensland Auditor-General (October 2007) *Better Practice Guide – Risk Management*

Treasury Board of Canada Secretariat (April 2001) *Integrated Risk Management Framework*

Treasury Board of Canada (2004) *Integrated Risk Management: Implementation Guide*

United Kingdom HM Treasury (October 2004) *The Orange Book: Management of Risk – Principles and Concepts*

United Kingdom HM Treasury (November 2006) *Thinking About Risk – Managing your risk appetite: Good practice examples*

United Kingdom HM Treasury (November 2006) *Thinking About Risk – Managing your risk appetite: A practitioner's guide*