VAGO issued this better practice guide in 2004.

This document should be considered historical information only and is not representative of current better practice.

Managing risk across the public sector

GOOD PRACTICE

GOOD PRACTICE GUIDE

Auditing in the Public Interest

AUDITOR GENERAL
VICTORIA

Contents

Published by the Victorian Auditor-General's Office,
Level 34, 140 William Street, Melbourne.
First published June 2004. Also published on
<www.audit.vic.gov.au>

ISSN 1449–2733
ISBN 0 9752308 1 6

2004 : 2

Foreword

The business of government is increasingly more complex. The boundaries between the public, private and community sectors are ever more porous, and policies that demand whole-of-government approaches are more and more common. Public sector organisations must manage not only their own risks, but also the risks that come with joined-up government and inter-agency partnerships.

Managing this complexity involves managing increasingly complex risks. This highlights the importance of an appropriate and effectively implemented risk management framework to guard an agency against threats to its performance. Such a framework should also assist organisations to take advantage of opportunities to manage their businesses better.

In our 2003 performance audit, *Managing risk across the public sector*, my Office looked at how public sector organisations manage risk. We found that most organisations we examined used risk management processes in some part of their business and services, and that the board or executive was involved directly in this.

However, we also concluded that many things needed to be improved, and much needed to be done. Importantly, we found that:

- Good risk management was not yet a mature business discipline in the Victorian public sector.
- Approximately one-third of all organisations did not explicitly identify and assess their key risks and many did not evaluate risk controls.
- Public sector organisations did not always report risk information to their key stakeholders.
- Oversight by the audit committee and executive management was critical to successful risk management.
- Generally, risk management performance was more robust in organisations that took account of their state-sector risk (i.e. risks that affect the state as a whole).

This guide has been developed to help public sector organisations develop better practice risk management frameworks and strategies.

I encourage agencies to use the guide and accompanying check list, to achieve the full benefits of an appropriate and effectively implemented risk management framework.

J. W. CAMERON

Auditor-General

About risk management

"Risk arises out of uncertainty. It is the exposure to the possibility of such things as economic or financial loss or gain, physical damage, injury or delay, as a consequence of pursuing a particular course of action. The concept of risk has two elements, the likelihood of something happening and the consequences if it happens[1]."

What is risk?

Risk can arise from internal or external sources, and might include exposure to such things as economic or financial loss or gain, physical damage, failure of a project to reach its objectives, client dissatisfaction, unfavourable publicity, a threat to physical safety or breach of security, mismanagement, failure of equipment and fraud.

Risks should not necessarily be avoided. If managed effectively, they allow us to sieze opportunities for improving services and buisness practices.

Risks can be categorised according to the goals, objectives or outcomes in the agency's corporate, strategic or business plans. At the highest level, these represent risks to the agency's ability to implement government policy.

Risks also can be categorised into:

- strategic risks (risks to the agency's direction, external environment and to the achievement of its plans)
- commercial risks (risks of commercial relationships, such as failed contractual relationships)
- operational risks (risks to core business activities, such as inadequate human resources, physical damage to assets or threats to physical safety)
- technical risks (risks of managing assets, such as equipment failure)
- financial and systems risks (risks with financial controls and systems, such as fraud)
- compliance risks (risks to meeting regulatory obligations).

Agencies often face risks that significantly influence other risks (such as inadequate staff skills or low morale that influence the risk of losing key customers). These links between risks are important: a risk may not look significant in isolation, but is significant when its flow-on effect is considered.

As whole-of-government approaches become more common, state-sector risks – risks that affect the state as a whole – are becoming more significant. Agencies need to understand state-sector risks, and to pay greater attention to identifying and managing them.

There are 3 types of state-sector risk, each of which calls for a different response:

- agency-level risks (such as the risks above). These can become risks to the state because of their size and significance, because of the wider impact of measures to manage them, or because of poor management by agencies
- interagency risks, which if unmitigated by one agency, become risks for other agencies (such as if young people do not complete school, they may require employment support and adult and community education)
- statewide risks, which are beyond the boundaries of any one agency and call for a response across agencies coordinated by a central agencies (such as bushfires and other emergencies).

[1] Management Advisory Board's Management Improvement Advisory Committee (MAB/MIAC), *Guidelines for Managing Risk in the Australian Public Service*, Report No. 22, Canberra, October 1996, p. 3.

What is risk management?

"Risk management is the systematic application of management policies, procedures and practices to the task of identifying, analysing, assessing, treating and monitoring risk[2]."

There is no such thing as a risk-free environment, but many risks can be avoided, reduced or eliminated through good risk management. Good risk management also takes advantage of opportunities while analysing and dealing with risks.

Risk management is an explicit tool for business, public sector organisations and regulators to identify, evaluate and manage both risk and opportunity. It is a logical and systematic process which can be used when making decisions and in managing performance. It is a means to an end and should be integrated into everyday work.

Good risk management is forward looking and helps to improve business decisions. It is not just about avoiding or minimising losses, but about dealing positively with opportunities. It is a powerful tool for public sector managers.

Good risk management is based on a well-planned, logical, comprehensive and documented strategy. This strategy provides general policy guidance, and plans and procedures that can be used as part of the organisation's everyday work to manage risk. The complexity and extent of the strategy should be commensurate with:

- the level of risks (i.e. the likelihood and consequence of each risk) to which the agency is exposed
- the frequency and magnitude of risks.

Good risk management must be based on a strategy, but a strategy itself doesn't manage risks. Leadership, effort by all levels of management and staff, and careful monitoring by boards and audit committees, are needed to make the strategy a success.

Risk management in the Victorian public sector

In Victoria, key drivers for implementing risk management strategies include the *Victorian Managed Insurance Authority Act 1996*, the *Financial Management Act 1994*, the Victorian Government's Management Reform Program, and policies associated with private-public programs such as Partnerships Victoria.

More than 300 departments, authorities and public bodies and associated entities are subject to the Financial Management Act, which is administered by the Department of Treasury and Finance. The Act requires the agencies to develop and implement a risk management strategy, and keep it under review.

Aspects of risk management also are incorporated into the reporting arrangements established between the Department of Treasury and Finance and other departments as part of the quarterly monitoring process established under the Act.

Under the Victorian Managed Insurance Authority (VMIA) Act, the VMIA insures more than 170 state departments and participating bodies against their identified insurable risks. The Act also requires participating bodies to develop and implement a risk management strategy, and keep it under review[3]. While the VMIA focuses on the state's insurable risks, it also advises and trains agencies in managing risk.

[2] Ibid.

[3] "Participating bodies" include any statutory authority and body corporate that in the current or any previous financial year received more than 50 per cent of its funding from the Consolidated Fund.

Other guidance

The Australian and New Zealand Standard AS/NZS 4360:1999, *Risk management* and its accompanying handbook, HB143:1999, *Guidelines for managing risk in the Australian and New Zealand public sector*, are 2 important publications that provide detailed guidance about risk management practices.

These constitute a step-by-step guide for organisations wanting to develop risk management frameworks, encouraging organisations in all industries to formally structure their risk management and to integrate business risk with other more technical or financial risk assessment. The main elements of the risk management process described by the standard are illustrated below.

The Risk Management Process

Source: Standards Australia, AS/NZS 4360: 1999 *Risk management.*

Although not all organisations use the standard's approach, public sector risk management continues to expand beyond a financial focus to encompass all parts of an organisation's business and services. The Commonwealth Government based its *Guidelines for Managing Risk in the Australian Public Service*[4] on the standard. See <www.apsc.gov.au/mac/index.html>.

The VMIA endorses the use of the standard for managing business risk. The authority's online risk management performance assessment tool *(RIMPAT)* provides agencies with the means to assess their risk management practices against the standard. See <www.vmia.vic.gov.au>. Other services and information available through VMIA include client liaison, seminars, print and internet publications.

In its 2001 publication, *Risk Management Performance Benchmarking*, the Commonwealth Government's insurance body, Comcover, released 10 key performance indicators (KPIs) of best practice to help Commonwealth agencies benchmark their performance[5].

The Australian National Audit Office describes the key components of effective risk management, as well as the importance of developing a risk management culture, in its better practice guide, *Public Sector Governance Volume 1*[6]. See <www.anao.gov.au>.

CPA Australia has a number of publications relating to public sector risk mangement. They include *Case Studies in Public Sector Risk Management: Better Practice Guide; Enterprise-wide Risk Management: Better Practice Guide; Public Sector Risk Management: A State of Play;* and *Research Report on Public Sector Risk Management.* See <www.cpaaustralia.com.au/20_cpastore>.

Risk management check list

What follows is a check list designed to help public sector organisations evaluate and improve their risk management frameworks and strategies. The check list is based upon the criteria outlined in our 2003 performance audit, *Managing risk across the public sector.* The check list identifies the elements of good practice, which if effectively applied, would ensure that an organisation's risk management framework is appropriate, effectively implemented, integrated with governance structures and addresses state-sector risks.

[4] Management Advisory Board's Management Improvement Advisory Committee (MAB/MIAC), *Guidelines for Managing Risk in the Australian Public Service*, Report No. 22, Canberra, October 1996.

[5] Department of Finance and Administration, *Risk Management Performance Benchmarking*, Comcover, Canberra, 2001.

[6] Australian National Audit Office, *Public Sector Governance Volume 1*, Canberra, July 2003 p. 19-20.

Risk management check list

Appropriate risk management strategies

Public sector organisations with appropriate risk management strategies would have deliberate and evident management strategies and processes commensurate with the nature, scope, frequency and magnitude of risk to which they and the state may be exposed. These strategies and processes would be in line with a suitable risk management framework such as the Australian and New Zealand Standard AS/NZS 4360:1999, *Risk management*, and enable organisations to:

- identify potential impacts on the organisation, government and/or the community
- have reasonable and practical measures to address these impacts.

Good practice	***Good practice met***	***Action plan***	***Target date***
Does your organisation:			
Have an explicit, stated risk management policy?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Have an organisation-wide strategy, plan or program that is coordinated at a central, or corporate level?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Assign organisational risk management responsibility clearly? That is, has a specific structure defining responsibilities, accountabilities and measures for risk management?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Have a formal process (with defined standards and criteria) for identifying and analysing risks?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Identify and assess the main risks relating to each of its declared goals, objectives and planned outcomes?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Link risk assessments to government policy, organisational goals, and stakeholders?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Apply risk management to the whole of its business operations and services?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Develop separate, formally documented risk treatment plans that describe the nature of current risk controls?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Have formal, documented contingency plans for disaster recovery and business continuity?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		

Effective implementation of risk management

An organisation is implementing its risk management strategies effectively if:

- it understands its risks thoroughly
- it applies all proposed risk management strategies and processes to the intended functions and activities, and at the desired levels of the organisation
- its tests, reviews and business improvements confirm that its risk management strategies are providing the projected value and outcomes.

Good practice	Good practice met	Action plan	Target date
Does your organisation:			
Have a risk management coordinator, committee or unit?	Yes ☐ In part ☐ No ☐		
Formally review its risk management strategy at least annually?	Yes ☐ In part ☐ No ☐		
Ensure that all risk management actions directed by the executive and board are formally reported back to them to confirm their progress or completion?	Yes ☐ In part ☐ No ☐		
Have methods to identify and evaluate risk controls according to their effectiveness, cost, cost-benefit and compliance requirements?	Yes ☐ In part ☐ No ☐		
Regularly review and test risk controls and contingency plans?	Yes ☐ In part ☐ No ☐		
Ensure that other organisations it works with (like contractors and service providers) have suitable risk management practices that meet your standards?	Yes ☐ In part ☐ No ☐		
Formally document, report and address non-compliances, hazards, incidents, accidents, losses and claims?	Yes ☐ In part ☐ No ☐		
Formally communicate its risk management strategy with stakeholders to assess understanding and commitment?	Yes ☐ In part ☐ No ☐		
Provide, at least annually, risk management training to staff that is tailored to the needs of the organisation?	Yes ☐ In part ☐ No ☐		
Measure and monitor improvements to business processes as a result of its risk management strategies (e.g. reduction in cost of claims, number of incidents etc.)?	Yes ☐ In part ☐ No ☐		

Risk management integrated into governance structures and strategic management processes

An organisation with risk management integrated into governance structures and strategic management would:

- apply risk management as a clear part of its strategic and business-planning considerations, and at all critical levels of the organisation
- explicitly incorporate indicators of risk and risk management into its governance and management structures
- ensure its board and/or executive management:
  - are properly informed of the organisation's risk exposures
  - confirm that suitable risk management strategies are in place and working effectively
  - are fully and directly involved in setting and reviewing the organisation's risk management strategies
- have methods to:
  - set out the objectives to manage its risks and desired outcomes
  - allocate suitable and sufficient resources to risk management, taking into account the nature and level of the identified risks and the size of the organisation.

Good practice	Good practice met	Action plan	Target date
Does your organisation:			
Ensure that executive management directly lead and strategically manage the organisation's risk management process?	Yes ☐ In part ☐ No ☐		
Involve executive management in the identification and assessment of the organisation's risks?	Yes ☐ In part ☐ No ☐		
Ensure that executive management confirm that the organisation's risk management framework and strategies match the key risks of the organisation?	Yes ☐ In part ☐ No ☐		
Ensure that risk management is an explicit part of strategic and business planning considerations, and is applied at all critical levels of the organisation?	Yes ☐ In part ☐ No ☐		
Formally report risks and risk management actions with sufficient detail to the executive and board to ensure these are properly understood?	Yes ☐ In part ☐ No ☐		
Explicitly incorporate key performance indicators of risk and risk management into its governance and management processes?	Yes ☐ In part ☐ No ☐		
Have its audit committee oversight its risk management?	Yes ☐ In part ☐ No ☐		
Allocate adequate resources for ongoing implementation of risk management policies, plans and procedures?	Yes ☐ In part ☐ No ☐		

State-sector risk structures and processes

An organisation needs to understand the risks that impact on the State of Victoria if it is to effectively integrate risk management into its governance and/or management structures. This impact - on the state or on other public sector organisations – can take on more significance as joined-up-government services and policies are implemented. Consequently, the identification and management of state-sector risks between cooperating agencies requires greater attention.

Good practice	*Good practice met*	*Action plan*	*Target date*
Does your organisation:			
Have risk management structures and processes that assist the: • identification, • management and • reporting of key risks that should properly be drawn to the attention of the government?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Ensure that there is a common understanding among agencies within a portfolio of relevant state-sector risks?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Regularly share information with the department and other portfolio agencies on the identification and treatment of existing/emerging inter-agency risks?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Identify, treat and report inter-agency risks associated with managing shared policy objectives?	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		
Include all the agencies that fall within a portfolio within its risk management strategy? (departments only)	***Yes*** ☐ ***In part*** ☐ ***No*** ☐		

Good practice guides produced by the Victorian Auditor-General's Office

2004:1 Chief Finance Officer: Role and responsibilities