

VICTORIA

Victorian
Auditor-General

Managing Risk Across the Public Sector: Toward Good Practice

Ordered to be printed

VICTORIAN
GOVERNMENT PRINTER
June 2007

ISBN 1 921060 44 1

VAGO

Victorian Auditor-General's Office
Auditing in the Public Interest

The Hon. Robert Smith MLC
President
Legislative Council
Parliament House
Melbourne

The Hon. Jenny Lindell MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report on
Managing Risk Across the Public Sector: Toward Good Practice.

Yours faithfully



DDR PEARSON
Auditor-General

21 June 2007

Foreword

Every organisation faces a variety of risks. Identifying, assessing, managing and reporting these risks is at the heart of corporate governance and organisational performance. In an era where the public sector is facing greater scrutiny and adopting new models of service delivery, effective risk management is even more important.

In 2003, the Victorian Auditor-General's Office conducted a performance audit, *Managing risk across the public sector*. The audit found that risk management was not a mature business discipline. That audit also found that public sector organisations did not rigorously assess risks or evaluate their controls.

Since then, this follow-up audit has found that better risk management protocols have been promoted in Victoria through new legislation, ministerial directions and a good practice guide on governance. Their routine application is now widely accepted, and executive management and boards have led and adopted adequate risk management strategies.

While this audit acknowledges that progress has been made, it also found that further improvements are required to identify, assess, manage and report risks. Departments and agencies are increasingly entering partnerships with other organisations, within and outside the public sector, to deliver services. New service delivery models give rise to greater risks which require careful deliberation and a consistent approach. A key challenge for the Victorian public sector is to extend the application of risk management approaches to 'joined-up government' activities.

The audit also identified areas of potential improvement in the management of statewide risks. There is a need for the central agencies to provide greater guidance on how to deal with risks which potentially affect all agencies or risks more appropriately managed at the whole-of-government level.

I believe this report has both confirmed the further entrenchment of appropriate risk management practice in the Victorian public sector and signalled that the area of 'joined-up government' delivery merits particular vigilance in the future.



DDR PEARSON
Auditor-General

21 June 2007

Contents

Foreword	v
1. Executive summary	1
1.1 Introduction.....	1
1.2 Audit objective and scope	2
1.3 Audit conclusion	3
1.4 Recommendations	9
2. Background	13
2.1 Introduction.....	13
2.2 March 2003 audit report	13
2.3 This audit.....	14
3. Risk management in public sector organisations	15
3.1 Introduction.....	17
3.2 Public sector risk management (enterprise-wide guidelines)	19
3.3 Risk management framework, strategies and processes.....	21
3.4 Application of the risk management standard	25
3.5 Risk associated with managing deductible amounts.....	28
4. Inter-agency risks – joined-up government	31
4.1 Introduction.....	32
4.2 Assessment of inter-agency risks.....	33
5. Statewide risk management framework.....	35
5.1 Introduction.....	36
5.2 Assessment of statewide risk management practices.....	37
Appendix A. Department and agencies chosen for follow-up	41
Appendix B. Assessment questions and criteria	43
Appendix C. Glossary	49

1

Executive summary

1.1 Introduction

The Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004, defines risk as the chance of something happening that will have an impact on planned achievements.

Risk management is a comprehensive process, supported by appropriate strategies and frameworks that are designed to identify, analyse, evaluate, treat and monitor those risks that could prevent a department or agency from achieving its objectives. It covers strategic as well as operational, financial and compliance risks. The Victorian public sector and the private sector use the term “enterprise-wide risk management” to describe this comprehensive approach.

Risk management within the public sector covers 3 levels.

The first is organisation-level risks. These are financial, operational and strategic risks which can be managed by individual departments or agencies, and which do not impact on other organisations.

The second type is inter-agency risks. These result from joined-up government activities where 2 or more departments or agencies work together, across organisational boundaries, to deliver government services or programs or to share services. It is expected that these risks are managed at the inter-agency level.

The third is statewide risks. These are significant risks that are related to key areas of government policy or to an activity with a high public profile and where the potential consequences extend beyond the boundaries of a single department or agency. These types of risk need to be brought to the attention of government and can occur at the agency, inter-agency and whole-of-government level. More specifically, statewide risks can emanate from:

- a **particular agency** (e.g. due to the scale of a major project or key commitment)
- a **group of agencies** (e.g. where agencies cooperate in achieving shared policy objectives and the potential risks have a statewide impact). Inter-agency risks of statewide significance could emanate from the governance arrangements and the implementation of the key government policies such as *A Fairer Victoria*, *Meeting our Transport Challenges*, and *Our Environment: Our Future*

- the **whole-of-government level**. Whole-of-government risks are those that affect the whole public sector and require a coordinated response by a central agency (e.g. whole-of-government financial, insurance and security risks).

Managing joined-up-government and statewide risks requires a different management approach to that used to manage risks that are confined within the boundaries of one department or one agency.

In March 2003, the Victorian Auditor-General's Office completed an audit on *Managing risk across the public sector*. This assessed whether 61 public sector organisations had developed and applied appropriate risk management frameworks.

The 2003 audit found that most organisations had started to address risk management in some way. However, the audit found that risk management was not yet an established or mature business discipline and that public sector organisations did not rigorously assess risks and evaluate risk controls. The audit recommended improving:

- risk management in public sector organisations
- the statewide risk management framework.

In relation to risk management within public sector organisations, the 2003 audit recommended that organisations:

- be provided with clear risk management guidelines, processes and procedures
- adopt formal risk management approaches that are appropriate to each organisation's level of risk
- rigorously evaluate risks and risk treatments, linking risk criteria to government policy, organisational objectives and stakeholder expectations and, where possible, use cost-benefit analysis.

The 2003 audit recommended that the existing government processes that help identify, assess and manage statewide risks be standardised, strengthened and better coordinated. The audit recommended that the central agencies issue guidelines to help departments and agencies identify, assess and manage statewide risks.

1.2 Audit objective and scope

The objective of the current audit was to determine whether satisfactory progress has been made by departments, and a selection of agencies, in developing appropriate risk management frameworks and in applying risk management principles in their organisations.

The current audit examined 25 public sector organisations (10 departments, 14 agencies and the Victorian Managed Insurance Authority (VMIA), refer Appendix A). It assessed the risk management practices of these organisations against the good practice principles in the *Managing risk across the public sector: Good Practice Guide* which the Victorian Auditor-General's Office produced in 2004.

1.3 Audit conclusion

Since 2003, a range of steps have been taken to improve risk management within the public sector. Risk management has been promoted through legislation, ministerial directions and a good practice guide on governance for Victorian public entities. In 2005, the VMIA's role in providing risk management services to the public sector beyond insurable risk was confirmed.

The formal application of risk management has become an accepted and widespread practice within the audited departments and almost all agencies. Their executive management or boards have both led and adopted adequate strategies, frameworks, and processes that enable them to manage risk.

The current audit also found that the risk management process is based on the standard and almost all departments and agencies provide regular risk reports to their executive management, board and audit committee.

However, there is a need for further improvements to:

- risk management (enterprise-wide) in Victorian public sector organisations, by:
 - central agencies issuing risk management (enterprise-wide) guidelines
 - strengthening risk management practices
 - applying the risk management standard more rigorously
- statewide risk management, by a central agency developing a framework and issuing clear directions and guidelines on how to manage these risks.

1.3.1 Risk management in public sector organisations (enterprise-wide) has improved, but further improvements need to be made

Public sector risk management (enterprise-wide) guidelines need to be developed

The 2003 audit recommended that the Victorian Government provide public sector organisations with clear risk management guidelines, processes and procedures.

The current audit found that some guidance is provided through legislation, ministerial directions, and a good practice guide on governance for public sector entities. Audit committees oversee the effective operations of a department or agency's risk management framework and approve internal audit plans. Public sector organisations are required to review annually their risk management system. The board of a public entity is also required to inform the minister and department head of known major risks.

While these directions provide guidance, they are not comprehensive. The findings from the current audit indicate, as in 2003, that the public sector needs clear guidelines, including minimum standards, about what is expected from them when managing risk. Central agencies have not produced this consolidated guidance. Risk management practices could be improved if comprehensive guidelines were developed that provided clear direction on:

- the content of policy and risk management frameworks
- the roles of the secretary, board and executive management; the risk coordination unit/branch; the audit committee; and internal audit
- applying risk management standards throughout the whole organisation
- linking risk assessments to corporate goals
- developing risk registers and risk profiles
- the content of risk reports to executive management and audit committee.

Departments and agencies have adequate frameworks and strategies, but further improvement is needed

The 2003 audit recommended that public sector organisations adopt formal risk management approaches that are appropriate to the organisation's level of risk.

The current audit found that departments and agencies have adopted adequate risk management frameworks, strategies and governance structures that enable them to apply risk management across most of their organisation. All departments, and almost all agencies, have an audit committee providing oversight of their risk management framework and processes. They also have formal processes to report risks to executive management, the board and audit committee.

However, key aspects that need improvement include:

- business planning - risk management needs to be an explicit part of business planning processes so that potential risks to organisational plans are identified
- risk assessments - risk management needs to be applied to the whole organisation so that all risks are identified and managed. Risk profiles need to be linked to corporate goals so that the most important risks are managed, resources are effectively used and key government objectives are met
- reporting - all key risks need to be reported in sufficient detail and clearly so that the management of risks is understood. This would assist in ensuring that executive management (of a department) and the board (of an agency) are fully informed about risks, and in a better position to make informed judgments about the allocation of resources and priorities for managing those risks

- audit committee – members of audit committees need to receive comprehensive risk registers, the enterprise risk profile and regular risk reports that fully inform them on the key risks faced by the organisation. They should also have the opportunity to review and endorse annually the risk management framework and the enterprise risk profile. This would enable the audit committee to provide executive management (of a department) or the board (of an agency) with a greater level of assurance about how well risks are managed in their organisation.

Application of the risk management standard needs to improve

In 2003, the audit recommended that public sector organisations:

- rigorously evaluate risks and risk treatments, linking risk criteria to government policy, organisational objectives and stakeholder expectations
- where possible, use cost-benefit analysis.

The current audit found that all departments, and most of the agencies, use the risk management standard AS/NZS 4360:2004 to identify, assess and manage risks. These organisations have developed informative guidance material on applying the standard within their organisations. This material includes information on the risk management process; risk categories; and tools to identify and assess the risk such as control effectiveness, consequence and likelihood ratings. Specific guidance on managing projects was also developed. As a result, risk assessments of the departments and agencies audited were broadly aligned with the standard.

The current audit also found that organisations have placed more emphasis on risk assessment (identification, analysis and evaluation) than on the management of risks (risk treatment, monitoring and review). Very few risk profiles and reports of departments and agencies indicated whether risk treatments had been implemented and whether changes to the level of risk had occurred as a result of implementing risk treatments.

None of the departments, and few of the agencies, were able to provide evidence to indicate that they measured whether the implementation of risk controls actually led to improvements to business operations. If this was addressed, it should provide executive management, the board and the audit committee with a greater level of assurance that risks are being effectively managed.

The VMIA provides education and training on the standard and other risk management topics. This should assist departments and agencies in developing a greater level of understanding of the principles behind the standard and in applying them across their organisation.

The claims management model is improving

During the course of the current audit we became aware that the Department of Treasury and Finance (DTF) is improving the whole-of-government claims management model.

Departments and agencies lodge insurance claims with the VMIA for amounts that are above the deductible amounts, (i.e. excess amounts, currently \$3 million for property losses and \$5 million for personal injury. Agencies, such as public hospitals, within the public healthcare program have a full claims service provided by the VMIA for claims below the \$3 million and \$5 million excesses). Departments and agencies are not required to inform the VMIA for claims that fall below the deductible amounts. As a result, the VMIA is not aware of the extent and value of payments made by departments and agencies for insurable claims that fall below the deductible amount. These payments constitute a risk that needs to be managed at the department and agency level. We examined 2 organisations and both were not able to provide an organisation-wide report that detailed the extent and value of payments made below deductible amounts.

DTF is aware of the issue of managing deductible amounts and has developed a whole-of-government claims management model to address it. The model requires departments, and all agencies under their portfolio, to report all claims and payments above \$10 000 to the VMIA. This data will assist the VMIA, and individual departments and agencies, to establish the extent of payments made below the deductible amounts and any associated risks. It will also assist them to explore whether public sector insurance policies need to be altered. It is expected that the benchmark value of \$10 000 will be reviewed in 2009.

It still remains for departments and agencies to consider the potential benefits of identifying all claims or payments below \$10 000 (or at a benchmark value deemed appropriate for the organisation). All claims or payments for insurable items that fall below the deductible level should be reported to executive management, the board and audit committee annually. Reports should either confirm a satisfactory situation or lead to business improvement initiatives to better manage insurable risks.

1.3.2 Risk management in joined-up government activities

The 2003 audit found that inter-agency risks could go undetected, especially as their potential impact on another agency may not be recognised.

The current audit found that memorandums of understanding, contractual arrangements and service agreements are used to deal with inter-agency matters, and some departments have prepared risk plans for some joined-up government initiatives.

The current audit also found that none of the risk management policy and frameworks supplied by departments and agencies provided guidance on dealing with joined-up government risks. As a result, their risk management approach did not include clear mechanisms for identifying and handling risks which have an impact beyond their organisation.

1.3.3 The public sector would benefit from having a framework and guidelines on statewide risks

The 2003 audit recommendation to develop a statewide risk management framework document and guidelines that assists departments and agencies to identify, assess and manage statewide risks has yet to be addressed.

The current audit found that departments did not have portfolio-wide policies and procedures that ensure that their portfolio agencies have a common understanding of statewide risks. It also found that risk profiles and risk reports of departments and agencies dealt with key risks, but did not explicitly report statewide risks. In these circumstances, the government cannot be assured that all statewide risks are reliably identified, assessed, managed and escalated, where necessary, to its attention.

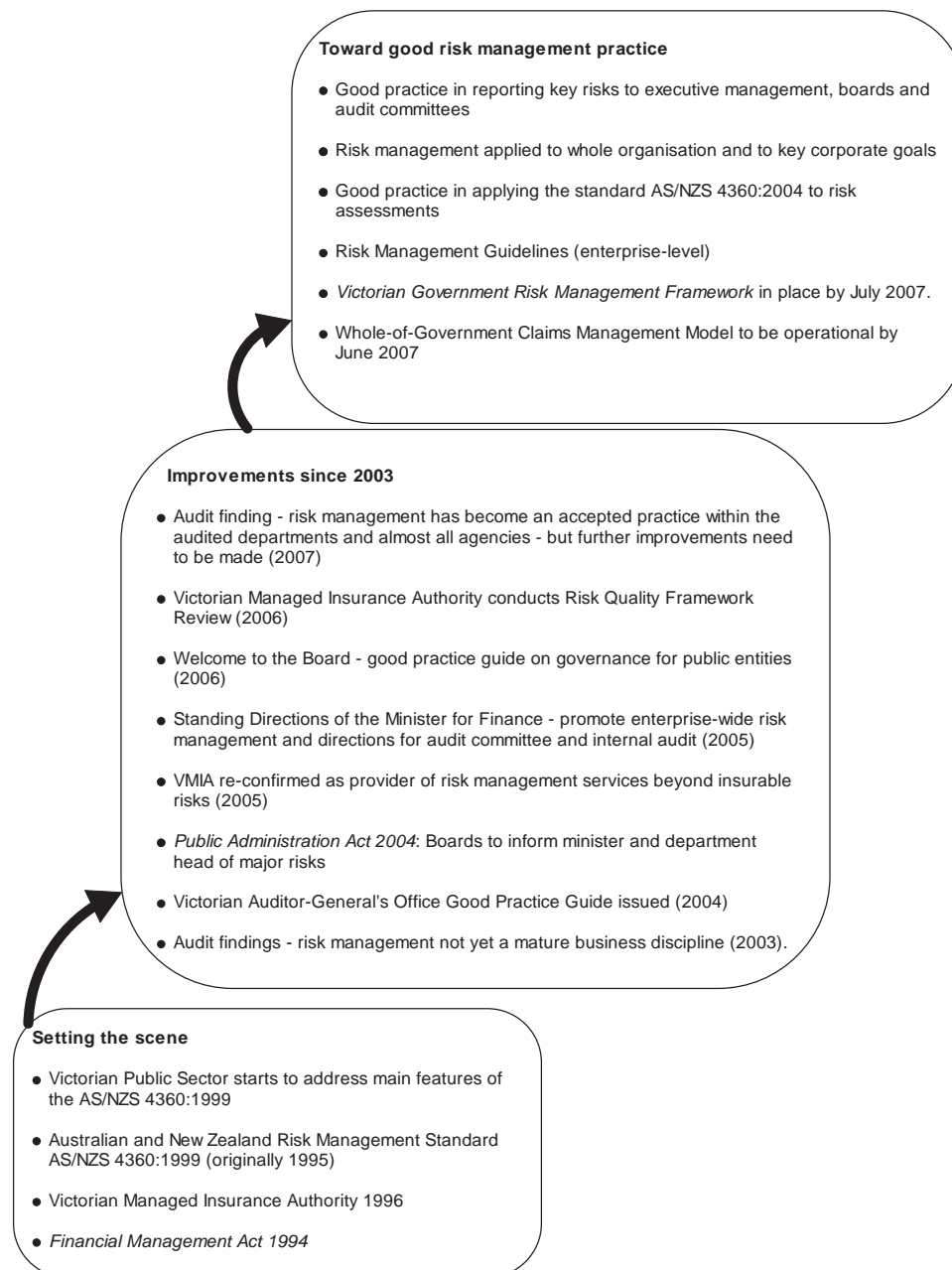
DTF, as part of its statewide risk management project, is developing a *Victorian Government Risk Management Framework* and expects to complete it by July 2007. This Framework will promote awareness of risk management processes and of the existing risk management accountabilities at the agency and whole-of-government level. One key initiative requires department and agency heads to attest in annual reports that their organisations have risk management processes in place consistent with the standard (or equivalent standard). A responsible body or audit committee is to verify that these processes are effective in controlling the risks to a satisfactory level.

This proposed Framework is a positive initiative and is supported. However, it currently does not address the issues identified in the 2003 audit and in the current audit. The public sector would benefit if the Framework is further developed so that it fully addresses the audit findings relating to statewide risks.

1.3.4 Progress toward good practice

Figure 1A shows the progress made by departments and agencies since 2003 in applying risk management in their organisations and areas where further improvements need to be made.

**Figure 1A
Toward Good Practice**



Source: Victorian Auditor-General's Office.

1.4 Recommendations

Risk management in public sector organisations

- 1.1 That the VMIA, in consultation with central agencies, the State Services Authority (SSA), departments and key public entities, develop risk management (enterprise-wide) guidelines for the public sector.
- 1.2 That departments and agencies further develop their risk management practices to ensure:
 - risk management is an explicit part of the strategic planning process
 - risk registers include risks that cover the whole organisation
 - key risks reported in the risk profile are clearly aligned with the corporate goals
 - risk reports provided to executive management, boards and audit committees contain sufficient information on key risks and are aligned with the standard (AS/NZS 4360:2004)
 - their risk management framework, risk registers and enterprise risk profile are provided annually to the audit committee for endorsement.
- 1.3 That departments and agencies align their risk management process (assessment, treatment, monitoring and review) with the standard (AS/NZS 4360:2004).
- 1.4 That DTF ensures the whole-of-government claims management model is implemented by July 2007 and reviewed in 2009.
- 1.5 That departments and agencies report annually to their executive management, board and audit committee on all claims paid that fall below the deductible amount (or below a value deemed appropriate for the organisation), and on payments made for items that could have been insured but were not insured.

Inter-agency risks – Joined-up government

- 1.6 That departments and agencies ensure that risk management arrangements are established for all joined-up government initiatives, particularly in the governance arrangements for the initiatives.
- 1.7 That the SSA consider risk management issues, including making reference to the forthcoming risk management guidelines on statewide risks, in any support material that it produces on joined-up government approaches.

Statewide risk management framework

- 1.8 That DTF, DPC and the VMIA, in consultation with other key stakeholders, develop guidelines for identifying, assessing, managing, escalating and reporting statewide risks.

RESPONSE provided by the Secretary, Department of Premier and Cabinet

The Department of Premier and Cabinet (DPC) welcomes the audit report and the opportunity it will provide to continue to strengthen risk management processes across the public sector.

On the whole we are satisfied with the content of the report, however would like to raise one concern in relation to recommendation 1.8. DPC's preferred position is that DPC should maintain its current position and role with respect to risk management. DPC should not become directly involved in risk management coordination across government. We believe that the Department of Treasury and Finance is best placed to develop the proposed guidelines. This may be done in consultation with the Victorian Managed Insurance Authority. Expertise for risk management resides within these agencies. DPC's role with respect to managing statewide risks would be to continue to provide high level advice to the Premier.

RESPONSE provided by the Secretary, Department of Human Services

The Department of Human Services (DHS) positively and proactively endorses risk management as a way of doing business. Risk management for DHS is more than just compliance. DHS is on a journey to make risk management everyone's business. The findings from the report have given DHS some areas for consideration for further improvements.

Since the audit, DHS has embarked on a number of initiatives that will enable a better management of the process, particularly risk treatment and risk reporting. These include workshops on the departmental risk registers and their structure as well as an upcoming review of the risk management framework.

DHS also note that the recommendations of central agencies having a joined-up risk management approach toward inter-agency risks and a statewide risk management framework for managing whole-of-government risks.

Notwithstanding DHS is already working closely with other departments and agencies in managing inter-agency risks such as emergencies and bushfires, I support any initiative involving practical and effective frameworks or guidelines to better manage inter-agency and whole-of-government risks.

I reiterate DHS's commitment to risk management. We will take on board all relevant recommendations that strengthen DHS in this area.

RESPONSE provided by the Chief Executive Officer, Victorian Managed Insurance Authority

The Victorian Managed Insurance Authority (VMIA) appreciate the complexity and level of maturity of risk management practice across the public sector and concur with your overall assessment that risk management has improved “but further improvements need to be made”. Your assessment closely aligns to the results of our own review, the Risk Framework Quality Review which was conducted during 2006.

VMIA is currently establishing a new client centric structure with the objective of delivering best practice risk management and insurance products and services to our clients. These services will assist in lifting the level of risk management skills and aid the improvement of risk management practice across the public sector.

We look forward to contributing toward the development of enterprise-wide risk management guidelines for the public sector and the Victorian Government Risk Management Framework. VMIA will actively engage the key stakeholders who share a common interest in your recommendations with a view to progressing these matters.

We are supportive of your recommendations and look to take a lead role in the evolution of risk management across the public sector.

RESPONSE provided by the Chief Executive, Peninsular Health

Recommendations 1.1 and 1.2. Peninsular Health support that risk management guidelines be developed for the public sector. However, we wish to emphasise the need for these guidelines to be sufficiently flexible to recognise separate requirements that are placed on agencies. For example, a public health service is required to be accredited through the Australian Council on Healthcare Standards (ACHS) and its Aged Care services by the Aged Care Standards and Accreditation Agency.

The accreditation tool used by ACHS has a specific standard relating to risk management with a number of elements that are required to be demonstrated. It is imperative that any sector wide guidelines recognise these other requirements so that duplication of resources is not required from agencies. Similarly, any monitoring framework should not be so specific that inefficiencies are created due to dual reporting requirements.

This should be able to be achieved given that both requirements are derived from the same Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004.

2 Background

2.1 Introduction

The Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004, defines risk as the chance of something happening that will have an impact on planned achievements.

Risk management is an important feature of good corporate governance. Businesses, public sector organisations and regulators use risk management policies and processes to identify, assess, manage and report risks. This way, they are better placed to achieve their objectives while protecting the interests of stakeholders. In particular, public sector organisations use risk management to deliver better policies, services, laws and regulations.

2.2 March 2003 audit report

Our March 2003 audit report *Managing risk across the public sector* examined if 61 public sector agencies had risk management frameworks that effectively identified, assessed, managed and reported risks. It examined:

- risk management in public sector organisations - to find out how risks were managed by examining strategies, structures and processes of departments and agencies. This is also known as enterprise-wide risk management
- the statewide risk management framework - to find out how those risks that had an influence outside the organisation were managed as these risks should be drawn to the attention of government. The 2003 audit identified the following 3 categories of statewide risks:
 - agency risks - because of their significance
 - inter-agency risks - because departments and agencies need to cooperate in managing risks associated with shared policy objectives
 - whole-of-government risks - because they require a coordinated response by a central agency.

The 2003 audit found that while most agencies addressed risk management in some way, risk management was not an established discipline. It also found that most agencies did not rigorously assess risks and evaluate risk controls. The audit recommended improving:

- risk management in public sector organisations
- the statewide risk management framework.

In relation to risk management in public sector organisations, the audit recommended that they:

- be provided with risk management guidelines, processes and procedures
- adopt formal risk management approaches appropriate to their level of risk
- rigorously evaluate risks and their treatments
- link risk criteria to government policy, organisational objectives and stakeholder expectations
- where possible, use cost-benefit analyses.

The 2003 audit recommended that existing government processes to identify, assess and manage statewide risks be standardised, strengthened and coordinated. It also recommended that central agencies issue guidelines to help agencies identify, assess and manage statewide risks.

2.3 This audit

The current audit examined whether 25 public sector organisations (10 departments, 14 agencies and the Victorian Managed Insurance Authority (VMIA), refer Appendix A) had made satisfactory progress in developing appropriate risk management policies, frameworks and processes. The audit assessed their risk management practices against the good practice principles in the *Managing risk across the public sector: Good Practice Guide* published in 2004 by the Victorian Auditor-General's Office.

The audit examined 15 key aspects of risk management that would be able to indicate whether public sector agencies:

- had appropriate risk management strategies
- integrate risk management into governance and strategic management arrangements
- demonstrate effective implementation of risk management
- have well-developed structures and processes to manage statewide risks.

This audit also examined progress by the Department of Treasury and Finance, the Department of Premier and Cabinet and the VMIA in addressing the 2003 audit recommendations. This included progress in developing statewide and enterprise-wide risk management guidelines.

The audit was performed in accordance with the Australian auditing standards applicable to performance audits, and included tests and procedures necessary to conduct the audit. The total cost was \$320 000. This cost includes staff time, overheads, expert advice and printing.

3 Risk management in public sector organisations

At a glance

Background

The 2003 audit found that risk management was not yet an established or mature business discipline and that public sector organisations did not rigorously assess risks and evaluate risk controls.

The 2003 audit recommended that public sector organisations be provided with risk management guidelines, processes and procedures. It also recommended that agencies formally identify, assess and manage risks, and that risk criteria link to government policy and organisational objectives.

Key findings

- Central agencies have provided guidance on risk management through legislation, ministerial directions, and portfolio guidelines, but these are not comprehensive.
- Departments and agencies have adopted adequate risk management strategies, frameworks and processes that enable them to apply risk management across their organisation.
- Most departments and almost all agencies did not align their risk assessments to their corporate goals.
- Departments and agencies prepared risk reports. Most risk reports did not contain sufficient details to enable a clear understanding of how risks are being managed.
- All departments and agencies have an audit committee with responsibility to provide oversight of risk management. Almost all of them did not formally endorse the organisation's risk management framework and risk profile for currency and appropriateness.
- Almost all audited organisations use the standard (AS/NZ 4360:2004), but have placed more emphasis on risk assessment (identification, analysis, evaluation) than on the management of risks (risk treatment, monitoring, review).
- Improvements to the whole-of-government claims management model should assist departments and agencies to better manage deductible amounts.

At a glance - *continued*

Key recommendations

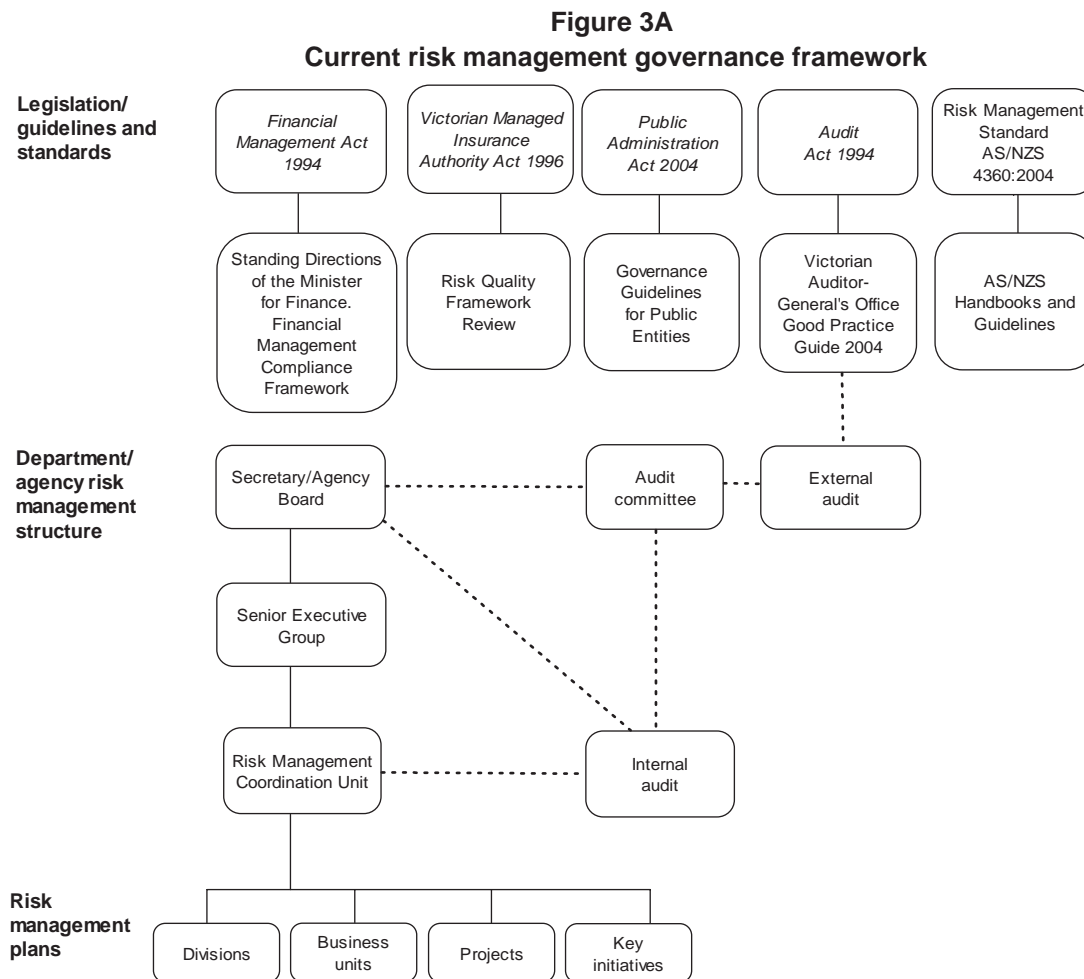
- 3.1 That the Victorian Managed Insurance Authority (VMIA), in consultation with central agencies, the State Services Authority, departments and key public entities, develop risk management (enterprise-wide) guidelines for the public sector.
- 3.2 That departments and agencies further develop their risk management practices to ensure:
 - risk management is an explicit part of the strategic planning process
 - risk registers include risks that cover the whole organisation
 - key risks reported in the risk profile are clearly aligned with the corporate goals
 - risk reports provided to executive management, boards and audit committees contain sufficient information on key risks and are aligned with the standard (AS/NZS 4360:2004)
 - their risk management framework, risk registers and enterprise risk profile are provided annually to the audit committee for endorsement.
- 3.3 That departments and agencies align their risk management process (assessment, treatment, monitoring and review) with the standard (AS/NZS 4360:2004).
- 3.4 That the Department of Treasury and Finance (DTF) ensures the whole-of-government claims management model is implemented by July 2007 and reviewed in 2009.
- 3.5 That departments and agencies report annually to their executive management, board and audit committee on all claims paid that fall below the deductible amount (or below a value deemed appropriate for the organisation), and on payments made for items that could have been insured but were not insured.

3.1 Introduction

This Office's 2004 good practice guide *Managing risk across the public sector* identified 3 key elements of good risk management practice. They were:

- appropriate risk management strategies - organisations with such strategies can identify the potential impact on the organisation, government and the community of risks within their control and take reasonable and practical steps to address these impacts
- risk management integrated with governance structures and management processes - organisations with such integration have risk management as part of their strategic and business planning, use risk and risk management indicators, fully involve senior executives, and have methods to implement the necessary measures
- effective risk management - organisations that effectively manage risk understand their risks thoroughly, apply risk management processes as required and evaluate these processes to confirm their effectiveness.

Figure 3A shows the current risk management governance framework for the Victorian public sector.



Source: Victorian Auditor-General's Office.

The 2003 audit found that most organisations used risk management processes in some of their operations. It found that boards or executive management were directly involved in risk management. It noted that oversight by the audit committee and executive management was essential for successful risk management.

The 2003 audit, however, concluded that good risk management was not yet a mature business discipline in the public sector. Many things needed to be improved, in that:

- approximately one-third of all organisations did not explicitly identify and assess their key risks and many did not evaluate risk controls
- just fewer than 40 per cent had appropriate risk management strategies in place
- only 28 per cent of organisations were effectively implementing their risk management strategies
- public sector organisations did not always report risk information to their key stakeholders.

The 2003 audit recommended that public sector organisations:

- be provided with agency-level risk management guidelines, processes and procedures
- adopt formal risk management approaches appropriate to their level of risk
- rigorously evaluate risks and risk treatments
- link risk criteria to government policy, organisational objectives and stakeholder expectations
- where possible, use cost-benefit analysis.

For the current audit, departments and agencies' risk management practices were assessed against 3 elements of good practice. The audit sought to identify how risk management is holistically applied within each organisation. It examined issues relating to leadership, organisational strategy, organisational structure, risk management governance and application of the Australian and New Zealand Risk Management Standard, AS/NZ 4360:2004, (refer Appendix B for detailed criteria).

3.2 Public sector risk management (enterprise-wide) guidelines

Although the risk management guidelines audit recommended in 2003 have not yet been developed, some guidance has been provided via legislation, ministerial directions, and a good practice guide on governance for portfolio agencies. These included the following:

- confirmation of the VMIA as the provider of risk management services beyond insurable risks
- the requirement in the *Public Administration Act 2004* for boards of public entities to inform their minister and the department head of known major risks
- the Standing Directions of the Minister for Finance under the *Financial Management Act 1994* that require a responsible body to ensure that:
 - it regularly (and no less than annually) reviews the effectiveness of the body's system of risk management and internal control
 - its internal auditor develops an annual internal audit plan to address relevant elements of its risk profile
- the requirement that audit committees:
 - include 2 independent members (3 if the organisation is governed by a board)
 - review their charter at least every 3 years, and that the responsible body approve amendments to the charter
 - approve the internal audit plan and monitor management actions to resolve issues raised by internal audits
- the requirement of the Model Financial Report for Victorian Government Departments (for the period ending 30 June 2006) that the audit committee oversees the operation of its department's or agency's risk management framework.

In 2006, the State Services Authority (SSA) published *Welcome to the Board: Your introduction to the good practice guide on governance for Victorian public sector entities*. The publication, which is also available on-line, advises board members on how best to apply good governance practices and explains (among other things) strategic planning and risk management. It advises boards to:

- integrate risk management into the organisation's strategic planning process
- notify the minister of known risks to the effective operation of the board
- monitor and review the effectiveness and currency of systems to manage and report internal financial and operational risks.

Confirmation of the VMIA as the provider of risk management services beyond insurable risks is a positive development. However, the Standing Directions of the Minister for Finance focus on financial risks and only apply to the 300 public sector organisations that meet the "public body" definition of the *Financial Management Act 1994* and are identified in the notes of the *Annual Financial Report for the State of Victoria*. While *Welcome to the Board* notes the importance of risk management in public sector organisations, it is not intended to be a risk management guide.

3.2.1 Conclusion

While risk management has improved since 2003, scope exists for departments and agencies to further improve. This would be expedited if comprehensive guidelines were developed to provide clear direction on:

- the required content of risk management policy and framework
- the roles of the secretary, board, executive management, risk coordinators/risk units, audit committee and internal audit
- how to apply the risk management standard (AS/NZ 4360:2004) throughout the whole organisation
- how to link risk assessments to corporate goals
- how to develop risk registers and risk profiles
- the content of risk reports to executive management and the audit committee.

Such guidelines would complement existing legislation, such as the *Financial Management Act 1994* which requires organisations to develop, implement and review a risk management strategy. They would also complement the *Victorian Managed Insurance Authority Act 1996* which requires organisations to provide the VMIA with a copy of their risk management strategy and a report on its implementation. The guidelines would also improve the consistency of risk management policies and processes across the public sector.

Recommendation

- 3.1 That the VMIA, in consultation with central agencies, the SSA, departments and key public entities, develop risk management (enterprise-wide) guidelines for the public sector.

3.3 Risk management framework, strategies and processes

The current audit found that most departments and agencies had adequate risk management frameworks, strategies and processes that enable them to apply risk management across their organisation. Secretaries or boards had approved their organisation's risk management policy and framework. These documents usually covered:

- the importance and scope of risk management
- the roles and responsibilities of executive management, staff, the audit committee and internal audit
- risk management processes
- guidelines about how to use the risk management standard
- reporting requirements.

The more comprehensive frameworks noted the links between risk management and strategic planning, conformance requirements and key performance indicators.

The risk management governance structures usually comprised:

- the executive management who provide leadership and direction and regularly review risk reports
- a coordination unit/risk manager who promote risk management and coordinate risk plans and risk reports
- an audit committee which provides assurance to executive management or the board by over sighting the risk management process, including internal audit
- an internal audit plan to test the effectiveness of risk management.

To facilitate the consistent application of good risk management practices throughout the departments and agencies, further improvements need to be made.

3.3.1 Application of risk plans to whole organisation, linked to corporate goals and integrated with business planning

Good risk management requires risk plans that apply to the whole organisation and link to corporate goals. Such plans should help ensure that all key risks are identified and properly managed, throughout the organisation. This should also help ensure that the organisation's goals are achieved.

The current audit found that departments and agencies apply risk management to most key parts of their organisations. It is mostly applied at a divisional and regional level (where applicable) as well as organisational branches and to key projects. Most departments, and close to half of the agencies audited, did not apply risk management to all of their business units, branches and projects. Some did not have risk plans for new business units, new branches and new budget initiatives. As a result, some key risks may not have been identified by the organisation's risk management process and reported in its risk registers and profiles.

Most departments, and almost all agencies, did not directly align their risk profiles to their corporate goals. Rather, most risk profiles focused on operational risks. Risk profiles need to link to corporate goals so that the most important risks are identified, assessed and managed. This helps to ensure that resources are effectively used and corporate goals are met and, in turn, that government objectives are met.

Most departments and agencies have made risk management an explicit part of strategic and business planning. Risk management is usually a component of annual business planning by executive and non-executive staff, and is part of divisional and business units' annual plans. However, several departments that had made risk management process an explicit part of strategic planning did not link all strategic risks to corporate goals. This indicates that they need to improve their risk management processes so that all potential risks are identified and managed.

3.3.2 Reporting risks to executive management and the board

Risk reporting is an essential part of good governance. It enables executive management and the board to monitor the way risks are being managed and to make informed decisions about policies, operational issues and resources.

The current audit found that almost all departments and agencies have formal mechanisms to report risks to executive management or the board. Some provide risk reports every 6 months. Others included risk reports in monthly departmental reports. Internal audit reports are also made available to executive management and the board.

The current audit also found that almost all departments and agencies did not report risks in sufficient detail to enable a clear understanding of how risks are being managed (treatment, monitoring, review). While risk reports vary in design and content, the audit found that they:

- focused on operational risks, and almost all did not report on emerging risks and statewide risks
- include risk assessments and risk evaluations (especially residual risks) which either did not properly or fully apply the principles and processes indicated by the risk management standard
- provide limited information on the risk treatments and whether these treatments had been implemented.

The current audit, however, also noted instances of good risk reporting. For example, some reports clearly aligned risks with the department's key strategic priorities, some reports clearly showed how risks were being managed, and one department regularly reported on emerging risks. A few departments regularly updated the level of all of their risks.

Risk reports should provide regular updates on statewide risks, strategic risks and any emerging risks. Some of the basic questions that reports should answer include:

- what are the risks?
- what is the level of each risk?
- what has been done about the risks?
- who is responsible for managing the risks?
- has the level of risks changed as a result of implementing risk treatments?
- what risks need to be escalated to strategic risks?
- what risks are no longer strategic and why?

3.3.3 Audit committees

Audit committees provide assurances to executive management and the board on the operations of their organisation's risk management framework.

The Model Financial Report for Victorian Government Departments (for the period ending 30 June 2006), issued by DTF, states that the audit committee oversees the effective operations of a department or public entity's agency's risk management framework.

The 2003 audit commented that oversight by the audit committee and executive management was essential for successful risk management. It found that an organisation's success in having appropriate risk management strategies in place increased by almost 50 per cent where an audit committee was involved in a direct leadership role. It recommended that an audit committee independently assess, for the board or executive management, how appropriately and effectively risks are identified and managed.

The current audit found that all departments and agencies have an audit committee with responsibilities for overseeing risk management. The audit committees of all departments and almost all of the agencies reviewed and approved the adequacy of their internal audit work plan. Almost all committees did not annually endorse their organisation's risk management framework or enterprise risk profile for currency and appropriateness.

Oversight by audit committees would be improved if they endorsed, rather than just noted, the risk management framework, risk profile and risk reports. Such endorsement would not diminish the responsibility of a department secretary, or the board of an agency, with respect to their organisation's risk management framework, strategies and processes. It would, however, assure them that the audit committee agrees with them. The audit committee of one department endorsed its risk management policy and framework processes, and in a couple of others they had endorsed the risk reports.

In some cases, the oversight function of audit committees was restricted because they were provided with limited information. As already noted, risk reports would provide a greater level of information if better aligned with the risk management standard, and if they reported all statewide, strategic and emerging risks. In some cases, risk registers were not provided to audit committees.

3.3.4 Conclusion

Departments and agencies have improved their risk management practices since 2003 in that they have adopted adequate frameworks, strategies and processes that enable them to apply risk management across their organisation. However, organisations need to:

- make risk management an explicit part of their strategic and business planning
- ensure that risk assessments are applied across the whole organisation
- clearly report all key risks (statewide, strategic, emerging) in sufficient detail so that the management of risks is understood
- provide their audit committees with a comprehensive risk register, risk profile and regular risk reports so that the committee is fully informed about key risks.

Recommendation

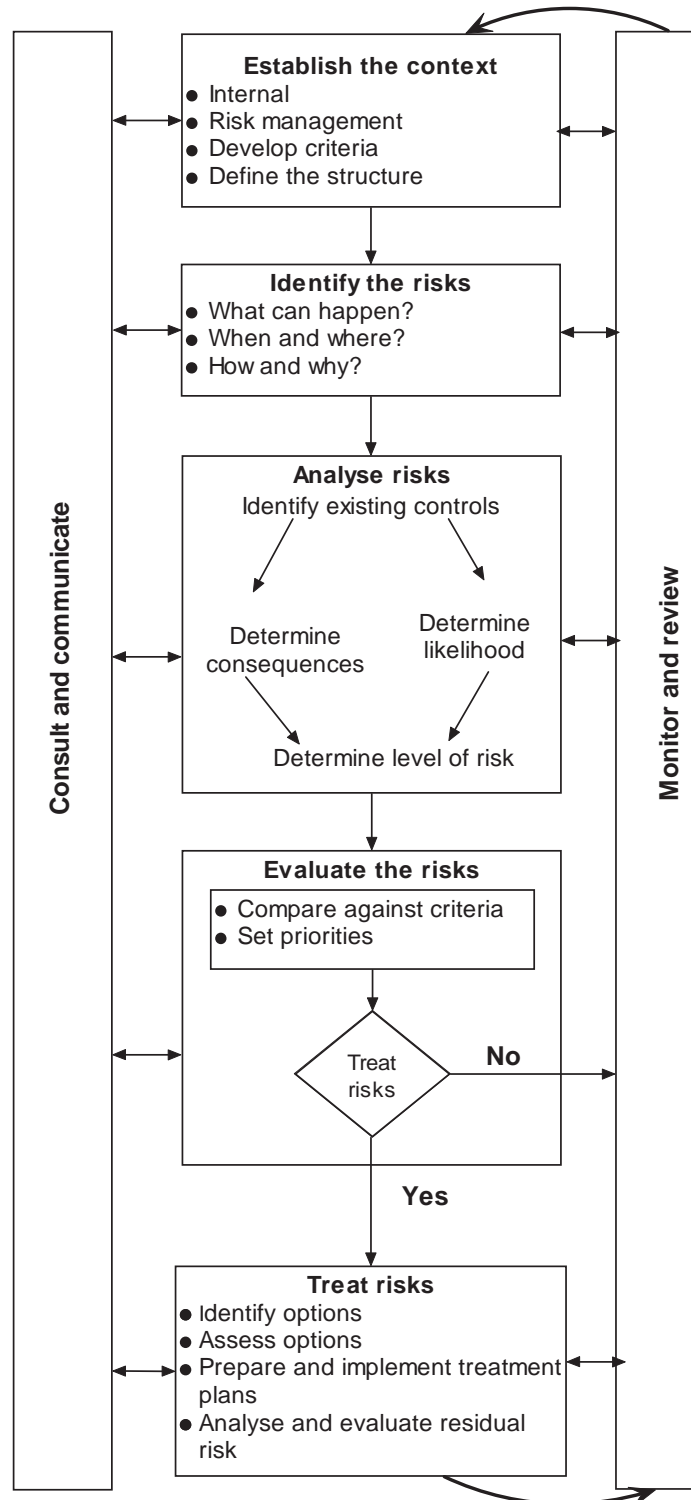
- 3.2 That departments and agencies further develop their risk management practices to ensure:
- risk management is an explicit part of the strategic and business planning process
 - risk registers include risks that cover the whole organisation
 - key risks reported in the risk profile are clearly aligned with the corporate goals
 - risk reports provided to executive management, boards and audit committees contain sufficient information on key risks and are aligned with the standard (AS/NZS 4360:2004)
 - their risk management framework, risk registers and enterprise risk profile are provided annually to the audit committee for endorsement.

3.4 Application of the risk management standard

The Australian and New Zealand Risk Management Standard, AS/NZS 4360:2004, provides public sector organisations with a rigorous approach to identifying, assessing and managing their risks. By using the standard effectively, departments and agencies are better placed to minimise risks and maximise opportunities to achieve their organisational goals.

Figure 3B shows the risk management process as presented in the standard (AS/NZS 4360:2004).

Figure 3B
Risk management process – in detail



Source: Standards Australia: Australian and New Zealand Risk Management Standard AS/NZS 4360:2004. p.13.

The 2003 audit recommended that public sector organisations rigorously evaluate risk and risk treatments.

The current audit found that all departments, and most of the agencies, demonstrably use the risk management standard to identify, assess and manage risks. These organisations have developed informative guidance material on how to apply the standard within their organisations. The material included information about the risk management process and risk categories, and tools to identify and assess risk (such as control effectiveness, consequence and likelihood ratings). They had also produced guidance material about managing projects.

Most departments, and almost half of the agencies, demonstrated that they have practices to identify and appraise risk controls and evaluate risk treatments in accordance with the standard. Very few risk profiles and reports, however, indicated whether risk treatments had actually been implemented or whether the level of risk had changed as a result of treatments being implemented.

No departments, and few of the agencies, could establish that implementing risk controls actually led to improvements to business operations (e.g. fewer incidents, reduced insurance costs). Without this information, executive management, the board and audit committee may not know whether risks are being effectively managed.

In 2006, the VMIA undertook a Risk Framework Quality Review across 79 public sector organisations which included an assessment of compliance with the standard. The VMIA also provides education and training on the standard and other risk management topics to departments and agencies.

3.4.2 Conclusion

Since 2003, departments and agencies have improved their risk assessment practices (identification, analysis and evaluation). They now need to ensure that risks are effectively managed. This means properly preparing and implementing risk treatment plans, analysing and evaluating residual risks, and monitoring whether risk treatments led to business improvements. An organisations' risk management policy and framework documents should make clear how this is to be done.

The provision of education and training by the VMIA on the standard and other risk management topics is supported. It should assist risk managers and other staff involved in risk management in developing a greater level of understanding of the principles underpinning the standard and its application.

Recommendation

- 3.3 That departments and agencies align their risk management process (assessment, treatment, monitoring and review) with the standard (AS/NZS 4360:2004).

3.5 Risk associated with managing deductible amounts

An insurable risk is a risk against which an organisation can insure to mitigate any financial consequences (e.g. theft or property damage). An insurable risk is the residual risk (the risk that remains after treatment measures are developed and implemented) that the organisation transfers to a third party (normally an insurance company).

The VMIA insures departments and about 300 state-controlled entities against their identifiable insurable risks, except that the VMIA does not provide WorkCover or transport accident insurance. Excesses (known as “deductible amounts”) are currently \$3 million for property losses and \$5 million for personal injury claims. (VMIA clients under the public healthcare program sponsored by the Department of Human Services (DHS), such as public hospitals, are provided with a comprehensive insurance program with commercially acceptable deductibles. DHS pays all insurance premiums to the VMIA on behalf of insured agencies. These agencies receive full insurance cover and claims management services from the VMIA regardless of the self-insured retention of DHS. DHS reimburses the VMIA for claims management services within their retention up to the \$3 million for property and \$5 million for public liability. Claims above these excesses are insured by the VMIA in its own right).

Except for agencies under the public healthcare program, departments and agencies lodge claims with the VMIA for amounts that are above the deductible amounts. However, they are not required to inform the VMIA about claims or payments that fall below the deductible amounts. As a result, the VMIA is not aware of the extent and value of payments made by departments and agencies for insurable claims that fall below the deductible amounts. These payments represent the level of risk that needs to be managed at the department and agency level.

It is important that organisations know the extent of deductibles paid. They should use this information to improve their management of insurable risks (e.g. by amending their insurance policy or by improving processes to reduce the number of incidents, accidents, thefts and losses).

The current audit examined how 2 organisations managed their general insurance-related deductibles, including costs incurred because of not insuring. These claims below the deductible level related to property damage, professional and public liability, security threats to personnel and threats to business safety.

The audit found that neither organisation could provide a report of the extent and value of payments made below deductible amounts for the whole organisation. This was mainly because they did not collate such information centrally. Their decentralised management systems and the way general-insurance-related payments were recorded made it difficult to identify the extent of deductibles paid. Both organisations are currently developing centralised systems that record all insurance-related claims and payments.

Departments and agencies generally apply incident reporting to occupational health and safety (OHS) matters, but not to general insurance. Most of the organisations did not collate and report non-OHS incidents, accidents, losses and claims and the associated costs incurred.

3.5.1 Whole-of-government claims management model

In October 2005, in response to an internal review of its public sector insurance and risk management practices, the government approved the whole-of-government claims management model. The model, being developed by DTF, requires departments and all their portfolio agencies to provide the VMIA with details of all claims or payments over \$10 000 for insurable items that were below the deductible level. These details are to be provided to the VMIA annually for payments made from 1 July 2006. This information shows the VMIA, and each department and agency, the extent of payments made below the deductible amount and whether insurance policies need to be altered. It is expected that the benchmark value of \$10 000 will be reviewed after 30 June 2009.

The model does not require organisations to identify claims or payments below \$10 000. Departments and agencies should consider the potential benefits of also identifying these claims or payments (or an appropriate benchmark value). Reporting all such claims and payments to executive management, the board and the audit committee annually could lead to the better management of insurable risks.

3.5.2 Conclusion

Risk management practices of departments and agencies could be improved if they identified the extent and value of deductibles paid. Such data could assist organisations to identify risks and areas where business improvements could be made.

Recommendations

- 3.4 That DTF ensures the whole-of-government claims management model is implemented by July 2007 and reviewed in 2009.
- 3.5 That departments and agencies report annually to their executive management, board and audit committee on all claims paid that fall below the deductible amount (or below a value deemed appropriate for the organisation), and on payments made for items that could have been insured but were not insured.

4 Inter-agency risks - joined-up government

At a glance

Background

The 2003 audit found that inter-agency risks could go undetected, especially as their potential impact on another agency may not be recognised.

Public sector organisations work together, across organisational boundaries, to deliver government services and programs or to share services. These joined-up government initiatives pose a new kind of inter-agency risks and warrant a risk management approach.

Key findings

- Memorandums of understanding, contractual arrangements and service agreements are used to deal with inter-agency matters, mainly where services are shared and where one department is the purchaser of services from another.
- Organisations have identified some of their inter-agency risks associated with joined-up government, but none of the risk management policy and frameworks supplied by departments and agencies provided guidance on dealing with joined-up government risks.

Key recommendations

- 4.1 That departments and agencies ensure that risk management arrangements are established for all joined-up government initiatives, particularly in the governance arrangements for the initiatives.
- 4.2 That the State Services Authority (SSA) consider risk management issues, including making reference to the forthcoming risk management guidelines on statewide risks, in any support material that it produces on joined-up government approaches.

4.1 Introduction

Public sector organisations need to actively consider any potential impact of their risks upon other government agencies and upon the State itself. This impact can take on more significance as joined-up government services and policies are implemented.

“Joined-up government” refers to public sector organisations working together, across organisational boundaries, to deliver government services and programs or to share services. This cross-agency approach is increasingly being used to deal with the more difficult issues faced by government, such as building communities, regional development, coping with demographic changes and dealing with crime.

Public sector organisations are likely to continue to work across boundaries in collaborative ways to develop policies and deliver services. Increasingly, demanding citizens, new technology, pressure on governments to do “more with less”, a greater recognition of the complexity of social problems and of the limits of attempting to solve them at a single department or agency level, are all encouraging public sector organisations to collaborate.

Joined-up government initiatives pose new kinds of inter-agency risks for the Victorian public sector and warrant a risk management approach. A key challenge for the public sector is to develop agreed and practical ways to manage these risks. Managing joined-up government risks requires departments and agencies to recognise that their actions may impact on the activities and the performance of other organisations.

Accordingly:

- formal risk management processes, usually applied at the enterprise level, should also be applied in cases where departments and agencies collaborate with other organisations for delivering services or programs or when developing policies
- there should be more information sharing among public sector organisations whenever the action of one organisation may have an adverse impact on another. Appropriate structures or communication mechanisms to deal with these risks should be established
- different departments and agencies need to understand each other’s risk management approach, and communicate effectively to jointly manage the potential aggregate risks or missed opportunities.

Inter-agency risks relating to joined-up government activities have an impact on 2 or more departments and agencies. Some inter-agency risks, however, are very significant and could have a statewide impact. These type of inter-agency risks are discussed in Part 5 of this report.

4.2 Assessment of inter-agency risks

The current audit examined whether departments and agencies identified, treated and reported inter-agency risks and inter-departmental risks associated with managing shared policy objectives.

The audit found that memorandums of understanding, contractual arrangements and service agreements are used to deal with inter-agency matters, mainly where services are shared (e.g. information technology, human resources, security services) or where one department is the purchaser of services from another.

The audit has also found that some departments have conducted risk assessments for joined-up government initiatives, such as sharing joint building facilities, one-stop shops and shared information and communication technology facilities. One department provided some guidance to staff on how to identify possible risks when dealing with other departments or agencies. However, none of the risk management policy and frameworks supplied by departments and agencies provided guidance on dealing with joined-up government risks.

The SSA is conducting research on joined-up government initiatives, including the preparation of case studies. The project, *Victorian Approaches to Joined Up Government*, may identify practices to support the achievement of government outcomes requiring joined up approaches. The utility of this project would be enhanced if any support material that the SSA produces included reference to risk management issues and the statewide risk management guidelines expected to be developed as part of the Department of Treasury and Finance's statewide risk management project.

4.2.1 Conclusion

The risk management practices of departments and agencies could be improved if a clear policy and guidelines were issued to help them deal with joined-up government risks. Until this is addressed, no reliable assurance exists that all inter-agency risks relating to joined-up government activities have been reliably identified, assessed, managed, and reported to executive management, the board and audit committee.

Recommendations

- 4.1 That departments and agencies ensure that risk management arrangements are established for all joined-up government initiatives, particularly in the governance arrangements for the initiatives.
- 4.2 That the SSA consider risk management issues, including making reference to the forthcoming risk management guidelines on statewide risks, in any support material that it produces on joined-up government approaches.

5 Statewide risk management framework

At a glance

Background

The 2003 audit found that while the Victorian public sector managed key risks, there was no clear understanding of statewide risks. Departments and agencies did not have mechanisms to collect and analyse significant statewide risks and there was no assurance that all of these risks in a portfolio had been identified. The responsibility for escalating these risks was not clear.

The 2003 audit recommended that a central agency issue guidelines that help identify, assess and manage statewide risks.

Key findings

- As in 2003, statewide risks are managed by central agencies, the Financial Management Act, the Victorian Managed Insurance Authority Act, relationship management and various administrative arrangements.
- Departments have yet to develop portfolio-wide policies and procedures that ensure their portfolio agencies had a common understanding of statewide risks.
- Risk profiles and risk reports were prepared and dealt with key entity risks, but did not explicitly report statewide risks.
- As statewide risk management guidelines have yet to be developed, departments and agencies cannot be certain that all statewide risks are reliably identified, assessed, managed, escalated and reported.
- The Department of Treasury and Finance (DTF) is developing the *Victorian Government Risk Management Framework* for balance sheet and non-balance sheet risks. It promotes risk management awareness and the requirement for agency heads to attest in annual reports that their risk management practices are consistent with the standard and for audit committees to verify that these practices are effective in controlling risks to a satisfactory level.

Key recommendation

- 5.1 That DTF, the Department of Premier and Cabinet (DPC) and the Victorian Managed Insurance Authority (VMIA), in consultation with other key stakeholders, develop guidelines for identifying, assessing, managing, escalating and reporting statewide risks.

5.1 Introduction

Organisations need to actively consider any potential impact of their high risks upon other government agencies and upon the State itself. These risks could happen at the agency, inter-agency and whole-of-government level. If not managed well, these risks could have an impact on how policy is developed and implemented, how services are delivered and whether key major projects are delivered on time and on budget.

By statewide risks we mean those risks that are very significant, are related to key government policies, have a high public profile and their potential consequences extend beyond the boundaries of a single department or agency. These risks could relate to economic, social, environmental and financial activities. Statewide risks could cover the whole state (e.g. risks relating to water management) or could be related to the metropolitan area (e.g. risks relating to metropolitan public transport) or regional areas (e.g. risks relating to *Moving Forward: Making Victoria the Best Place to Live, Work and Invest*).

Managing statewide risks is a key challenge for the Victorian public sector. This view has also been clearly articulated by Dr Peter Shergold, Secretary of the Commonwealth Department of Prime Minister and Cabinet, who in a speech delivered to the IPAA SA Connecting Government conference in 2005, stated: "I believe firmly that the need to build a whole-of-government approach to policy development and delivery is the single most challenging issue we face in public administration".

In the 2003 audit, 3 levels of statewide risks were identified:

- statewide agency level risks - can become statewide risks because of their significance, poor management, financial cost, high public profile (e.g. a major project; delivery of key electoral commitment via an agency)
- statewide inter-agency risks - are those where departments and agencies need to cooperate in managing risks associated with shared policy objectives. The governance arrangements need to include risk management and require joint management of risks or missed opportunities (e.g. *A Fairer Victoria, Meeting our Transport Challenges, Our Environment: Our Future*)
- whole-of-government risks - require a coordinated response by a central agency and would be related to areas that usually cover the whole public sector. These would include financial, insurance and security risks.

In contrast to the inter-agency risks related to joined-up government activities described in Part 4 of this report, statewide inter-agency risks, because of their significance, need to be brought to the attention of government.

Legislation has required most agencies to develop and implement a risk strategy. However, the 2003 audit found that this requirement was not supported by explicit definitions of statewide risk and guidelines to ensure these risks are identified and managed across the public sector through a consistent framework.

The 2003 audit concluded that in these circumstances:

- there was no clear understanding of statewide risks. As a result, certain types of these risks could go undetected at state level, especially inter-agency risks, as their potential impact on other agencies may not be recognised
- the public sector did not have a single explicit mechanism to collect and analyse significant risks to the State
- there was no assurance that all statewide risks in a portfolio had been identified
- there was a lack of clarity around the responsibility for escalating risks.

It recommended that a central agency issue guidelines that help identify assess and manage statewide risks.

5.2 Assessment of statewide risk management practices

To establish whether central agencies had implemented audit's 2003 recommendation, and to assess progress since 2003, the current audit examined whether:

- central agencies, departments and agencies had established policies, structures and processes to help them identify, assess and manage statewide risks
- departments and agencies identified, treated and reported inter-agency risks, and inter-departmental risks associated with managing shared policy objectives
- departments ensured that their portfolio agencies had a common understanding of statewide risks.

As in 2003, the departments and agencies examined in the current audit manage statewide risks through existing organisational structures and reporting requirements.

That is:

- the Department of Premier and Cabinet oversees and coordinates whole-of-government policy development
- DTF manages financial risks under the *Financial Management Act 1994* and provides guidance through the Whole-of-Government Financial Management Compliance Framework
- the Victorian Managed Insurance Authority manages insurable risks under the *Victorian Managed Insurance Authority Act 1996*
- under the *Public Administration Act 2004*, the board of a public entity is required to inform the minister and the department head of any known major risks
- the Central Government Response Committee informs government about responses to extreme events

- departments keep ministers informed through regular briefings and regular meetings between the secretary and the minister(s)
- memorandums of understanding, contractual arrangements and service agreements are used to deal with inter-agency matters, mainly where services (such as information technology, human resources or security services) are shared or where one department is the purchaser of services from another.

Cooperation between departments and agencies is an accepted practice in the Victorian public sector, including where they have shared policy objectives. Inter-departmental committees and/or whole-of-government working groups have been established to develop, implement and monitor policy initiatives such as *A Fairer Victoria*, *Our Environment: Our Future*, the Suicide Prevention Forward Plan.

The risk profiles and risk reports examined in the current audit did not identify and report on statewide inter-agency risks. As a result, organisations may not identify and effectively manage all statewide inter-agency risks. This could limit the successful implementation of government policy and programs.

The current audit found that while organisations have identified some of their key risks, some organisations did not have mechanisms to identify and manage statewide risks with an impact beyond their organisation. One explanation for this is the absence of statewide risk management guidelines which are yet to be developed.

The current audit also found that departments had not developed clear policies or portfolio-wide structures or communication strategies to ensure that all portfolio agencies were aware of all statewide risks and adequately deal with those risks. This is partly because portfolio agencies operate as independent bodies that are solely accountable to their minister for their performance and compliance requirements. The absence of a clear policy and guidelines for public sector organisations on how to identify and manage statewide risks is also contributing to this situation.

Departments need to make portfolio-wide arrangements to manage statewide risks. Such arrangements should inform agencies in their portfolio how to identify and deal with these risks. This should enable departments to be better informed on portfolio-wide risks and be in a better position to provide risk management advice to their minister(s) as required.

5.2.1 Statewide risk management project

In November 2006, DTF commenced the *Statewide Risk Management Project* to address identified gaps and strengthen risk management processes across the public sector. The project includes the development of a policy framework that will underpin risk management practice for Victorian public sector organisations.

One output from the Statewide project is the *Victorian Government Risk Management Framework*. The Framework will promote awareness of risk management processes and of the existing risk management accountabilities at the agency and whole-of-government level. It also notes that all risk management frameworks should be consistent with the key principles of the Australian and New Zealand Risk Management Standard AS/NZS 4360:2004. One key initiative requires department and agency heads to attest in annual reports that:

- departments and agencies have risk management processes in place consistent with the standard (or equivalent standard)
- a responsible body or audit committee verifies that these processes are effective in controlling the risks to a satisfactory level.

The Framework is expected to be applied by public sector organisations from July 2007.

This proposed Framework is a positive initiative and is supported. However, it currently does not address the issues identified in the 2003 audit and in the current audit. The public sector would benefit if the Framework is further developed so that it fully addresses the audit findings. To do this the Framework would need to include guidelines that would:

- provide guidance for identifying, assessing and managing the 3 levels of statewide risks (agency-level, inter-agency and whole-of-government risks)
- clarify responsibilities for escalating statewide risks
- ensure that reporting of statewide risks is explicit and is in line with the risk management standard (AS/NZS 4360:2004)
- explain how to make portfolio-wide arrangements to deal with statewide risks
- explain how to identify, manage and report on risks associated with joined-up government and whole-of-government policy outcomes.

Once the *Victorian Government Risk Management Framework* is further developed, the Victorian public sector should be better placed to adopt a comprehensive risk approach comprising the explicit management of:

- financial and insurable risks
- enterprise-wide risks
- joined-up government risks
- statewide risks.

5.2.2 Conclusion

The statewide risk management practices of departments and agencies could be improved if the *Victorian Government Risk Management Framework* is further developed to deal with these risks. Until this is addressed, no reliable assurance exists that all statewide risks have been reliably identified, assessed, managed, escalated and reported to the attention of government.

Recommendation

- 5.1 That DTF, DPC and the VMIA, in consultation with other key stakeholders, develop guidelines for identifying, assessing, managing, escalating and reporting statewide risks.
-

Appendix A: Department and agencies chosen for follow-up audit

Departments

- Education
- Human Services
- Infrastructure
- Innovation, Industry and Regional Development
- Justice
- Premier and Cabinet
- Primary Industries
- Sustainability and Environment
- Treasury and Finance
- Victorian Communities

Agencies

- Centre for Adult Education
- Essential Services Commission
- Kerang and District Hospital
- Kilmore and District Hospital
- Melbourne Market Authority
- Northern Health
- Office of the Public Advocate
- Peninsula Health
- Prince Henry's Institute of Medical Research
- Swinburne Graduate School of Integrative Medicine
- Victorian College of the Arts
- Victorian Managed Insurance Authority
- Western Health
- Wodonga Institute of TAFE
- Zoological Parks and Gardens Board

Appendix B: Assessment questions and criteria

Good practice principles	Criteria used to assess whether “good practice” has been met – partly met – not met
Principle 1 – Appropriate risk management strategies	
Does the organisation:	
1.1 Have an organisation-wide strategy, plan or program that is coordinated at a central or corporate level?	<p>A risk management policy/framework document that (i) is approved by the secretary of a department or CEO/board of an agency; (ii) that is current (<1-3 years old) and (iii) that informs the department or agency about:</p> <ul style="list-style-type: none"> • objectives and scope of the risk management framework • roles and responsibilities of executives and non-executives for risk management • the risk management standards to be adopted (e.g. in compliance with the AS/NZS 4360:2004 (or 4360:1999) or an equivalent recognised standard) • role of the board, audit committee or equivalent in overseeing risk management • role of risk management unit or coordinator • risk and risk management reporting requirements to executives; audit committee and agency board.
1.2 Link risk assessments to government policy, organisational goals and stakeholders?	<p>The enterprise risk profiles/risk registers of a department or agency should clearly show that:</p> <ul style="list-style-type: none"> • risk assessments are recorded in accordance with the standard AS/NZ 4360:2004 • key risks are directly aligned to government or organisational goals and priorities as identified in the entity’s current business/corporate plan • enterprise risk profiles/risk registers are current (prepared within the last 12 months).
1.3 Have a formal process (with defined standards and criteria) for identifying and analysing risks?	<p>Departments and agencies to demonstrate that their risk management process used to identify and analyse risks complies with the process outlined in the standard AS/NZ 4360:2004 (Figure 3.1, page 13 of the standard) or an equivalent recognised standard.</p>

Good practice principles	Criteria used to assess whether “good practice” has been met – partly met – not met
Principle 1 – Appropriate risk management strategies - <i>continued</i>	
Does the organisation:	
1.4 Apply risk management to the whole of its business operations?	<p>Departments and agencies to demonstrate through their risk management policy/framework and risk register/risk profile that risk management, in compliance with the standard AS/NZS 4360:2004, is applied regularly to the whole of their business operations. “Whole-of-business operations” would include:</p> <ul style="list-style-type: none"> • department/agency level, portfolio agencies (departments only) • division, branch, section or business unit; new business unit • key project, key initiative as a result of budget or ministerial statement or government statement • the individual operational areas that reflect the scope and/or structure across the entire entity (e.g. all locations or major assets, activity areas (e.g. research, policy, service delivery, community or client programs, clinical/non-clinical etc.), service providers (e.g. agents, contractors and volunteers), agency support systems (e.g. human resources, information technology, finance, legal services etc.).
Principle 2 – Risk management integrated into governance structures and strategic management processes	
Does the organisation:	
2.1 Ensure that executive management directly lead and strategically manage the organisation's risk management processes?	<p>Departments and agencies to demonstrate that:</p> <ul style="list-style-type: none"> • their risk management policy and/or framework is approved by the secretary and executive team of a department or the board of an agency • the executive/board receive regular reports (at least every 6 months) on risk management from their risk management unit • the audit committee or equivalent has oversight of the risk management framework and includes board members or has direct access to the secretary or chair of the board • executives/senior managers/branch heads identify and assess the key risks and are responsible for the risk management practices at their function and level of the organisation (i.e. for the agency, division or branch).
2.2 Ensure that risk management is an explicit part of strategic and business planning considerations, and is applied at all critical levels of the organisation?	<p>The department's or agency's risk management policy/framework or its planning guidelines should clearly show that:</p> <ul style="list-style-type: none"> • risk management is a key component of the business planning process • risk registers/profiles directly and clearly include risk assessments and any treatments for the key priorities/objectives/goals/key result areas stated in the entity's business/corporate plan, and are current (i.e. in the current planning year); OR the entity's current business plan includes a specific goal/objective/key result areas/action plan for the entity's risk management • risk management is applied by the functions and areas that reflect the levels of the organisation necessary (critical) to achievement of its current business plan.

Good practice principles	Criteria used to assess whether “good practice” has been met – partly met – not met
<p>Principle 2 – Risk management integrated into governance structures and strategic management processes - <i>continued</i></p>	
<p>Does the organisation:</p>	
<p>2.3 Formally report risks and risk management actions with sufficient detail to the executive management and board to ensure these are properly understood?</p>	<p>Departments and agencies to demonstrate that:</p> <ul style="list-style-type: none"> • the departmental executive or agency board (or its equivalent sub-committee) has a formal mechanism (like the entity’s risk policy/framework, executive/board meeting agenda and minutes) requiring reports to it on risk and risk management • they regularly (at least 6-monthly) report risks to the executives of a department or the board of an agency (or the relevant sub-committee of the board) in accordance with the standard AS/NZS 4360:2004 or equivalent recognised risk management standard • the risk reports include all the key risks as identified in the entity’s risk register or enterprise risk profile and any new risks not yet in that register as appropriate • other risk-related reports like internal audit reports including risk assessments and the Victorian Managed Insurance Authority (VMIA) Risk Quality Review Framework are drawn to the attention of executive management and the board.
<p>2.4 Have its audit committee oversight its risk management?</p>	<p>Departments and agencies to demonstrate that the audit committee’s terms of reference, agenda items or minutes demonstrate that it (or its equivalent or the full board) has oversight over risk management by having:</p> <ul style="list-style-type: none"> • considered and endorsed the risk management framework on an annual basis for currency and appropriateness • reviewed and endorsed the enterprise risk profile on an annual basis • reviewed the regular risk reports prepared by management (at least bi-annually) • oversight over the internal audit plan and this plan includes risk identification, assessment and risk treatment recommendations.
<p>Principle 3 – Effective implementation of risk management</p>	
<p>Does the organisation:</p>	
<p>3.1 Have a risk management coordinator, committee or unit?</p>	<p>Departments and agencies to demonstrate that they have appointed a risk management coordinator/unit or committee (or a combination of these) with a clear and stated responsibility for risk management that:</p> <ul style="list-style-type: none"> • provides guidance to the entity’s management about how to fulfil their risk management responsibilities • ensures the entity’s risk management policy, framework and processes are in accordance with a suitable standard for this purpose like AS/NZS 4360:2004 or equivalent recognised standard

Good practice principles	Criteria used to assess whether “good practice” has been met – partly met – not met
Principle 3 – Effective implementation of risk management - <i>continued</i>	
Does the organisation:	
3.1 Have a risk management coordinator, committee or unit? - <i>continued</i>	<ul style="list-style-type: none"> • facilitates the application of these risk management processes by the organisation to identify and assess its risk exposures and develop appropriate risk mitigation strategies • coordinates reporting on risk and risk management to executive management and to the board or its relevant sub-committee (e.g. audit and risk management committee) • monitors and reviews the risk management processes across the organisation.
3.2 Have methods to identify and evaluate risk controls according to their effectiveness, cost, cost-benefit and compliance requirements?	<p>Departments and agencies to demonstrate that:</p> <ul style="list-style-type: none"> • their risk assessment methods include the identification and appraisal of existing risk controls and their adequacy, and also the evaluation of risk treatments, consistent with a risk assessment process like that of AS/NZS 4360:2004 or equivalent recognised standard • their risk register, profile or reports to the executive management/board/audit committee identify and evaluate risk controls and indicate changes to the level of risk as a result of implementing risk treatments (risk controls and control improvements) OR • risk controls have been improved as a result of recommendations made by an internal audit or other assessments such as the VMIA's Risk Quality Review Framework or internal incident/loss/claims reports.
3.3 Formally document, report and address non-compliance, hazards, incidents, accidents, losses and claims?	<p>Departments and agencies to demonstrate that they have:</p> <ul style="list-style-type: none"> • a formal mechanism(s) like documented paper forms and/or software systems that applies throughout the organisation for timely reporting, recording, investigating and responding to incidents, accidents, losses, claims, hazards and non-compliances • maintained and used a mechanism(s) to monitor and report to executive management, board or audit committee or equivalent with sufficient data to highlight any significant matters and performance (e.g. trends, key problems, functions or areas most affected etc.) • reviewed and taken action on reported incidents, accidents, claims, losses, hazards and non-compliances.

Good practice principles	Criteria used to assess whether “good practice” has been met – partly met – not met
Principle 3 – Effective implementation of risk management - <i>continued</i>	
Does the organisation:	
3.4 Regularly 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.)?	<p>Departments and agencies to demonstrate that business process improvements were achieved as a result of their risk management strategies by:</p> <ul style="list-style-type: none"> • regularly monitoring and reviewing the enterprise risk profile (or risk reports or risk treatments recommended by internal audit) for progress and completion of risk treatments and risk mitigations shown therein with the associated measure of risk reduction • monitoring and reviewing business process improvements as a result of risk reduction evident in: reductions in incident or loss rates or downward trends or insurance costs or surveys of improvements in staff knowledge or awareness of risk control and risk reporting • relating business process improvements to insurance, policy development, administration, compliance, service delivery and regulations etc.
Principle 4 – Statewide risk structures and processes	
Does the organisation:	
4.1 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?	<p>Departments and agencies to demonstrate that:</p> <ul style="list-style-type: none"> • they have a policy or framework that has identified key statewide risks and provided guidelines on how to deal with them. Statewide risks are risks whose potential impact goes beyond that of the department or the entity, but reaches the broader community and the government • they have a structure in place that discusses and reports on statewide risks. A structure could include an organisational unit, a whole-of-government committee, an inter-departmental task force, an inter-departmental committee, clear reporting requirements to a minister and other equivalent arrangements • the secretary of a department or the chair of a board report key risks to ministers directly or via a whole-of-government committee.
4.2 Identify treat and report inter-agency and inter-departmental risks associated with managing shared policy objectives?	<p>Departments and agencies to demonstrate that they have:</p> <ul style="list-style-type: none"> • a policy that clearly explains how to treat and report inter-agency and inter-departmental risks associated with managing shared objectives • identified risks associated with managing shared policy objectives • a risk management structure or plan has been developed to mitigate, monitor and report on those risks. These would include an inter-departmental task force, an inter-departmental committee, memorandum of understanding, service agreements, contractual arrangements and other equivalent arrangements.

Good practice principles	Criteria used to assess whether “good practice” has been met – partly met – not met
Principle 4 – Statewide risk structures and processes - <i>continued</i>	
Does the organisation:	
<p>4.3 Ensure that there is a common understanding among agencies within a portfolio of relevant statewide risks? (<u>departments only</u>).</p>	<p>Departments to demonstrate that agencies within their portfolio are aware of statewide (key risks) and adequately deal with those risks. Key evidence would include:</p> <ul style="list-style-type: none"> • a policy document that outlines state–sector risks and advises portfolio agencies on how to manage those risks • departments communicating with agencies on issues relating to state (key) risks • portfolio-wide committees that regularly deals with state (key) risks • department executive committee to include CEOs of key portfolio agencies.



Appendix C: Glossary

Insurable risk

An identified risk that has a financial value which can be covered or transferred to some extent by insurance.

Residual risk

Risk remaining after implementing a risk treatment.

Risk

The chance of something happening that will have an impact on an organisation achieving its objectives.

Risk assessment

The overall process of risk identification, risk analysis and risk evaluation.

Risk management

Risk management is a comprehensive process, supported by appropriate strategies and frameworks that are designed to identify, analyse, evaluate, treat and monitor those risks that could prevent a department or agency from achieving its objectives. It covers strategic as well as operational, financial and compliance risks. The Victorian public sector and the private sector use the term “enterprise-wide risk management” to describe this comprehensive approach.

Risk management framework

The policy and procedures developed by an organisation to be used when identifying, analysing, evaluating, treating, reporting, monitoring, reviewing and communicating risks. The risk management framework should govern risk management at all levels in the organisation and would include key roles and responsibilities for risk management.

Risk profile

A prioritisation of key risks.

Risk reduction

Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk.

Risk register

A comprehensive record of insurable and non-insurable risks across an organisation, business unit or project depending on the purpose/context of the register.

The register records:

- the risk
- how and why the risk can happen
- the existing internal controls that may minimise the likelihood of the risk occurring
- the likelihood and consequences of the risk to the organisation, business unit or project
- a risk level rating based on pre-established criteria in the risk management framework, including an assessment of whether the risk is acceptable or it needs to be treated
- a clear prioritisation of risks.

Risk report

A regular report made available to executive management, boards and audit committees that informs how key risks (statewide risks, strategic risks and emerging risks) are being managed. Some of the basic questions that risk reports should answer include:

- what are the risks?
- what is the level of each risk?
- what has been done about them?
- who is responsible for managing the risk?
- has the level of risks changed as a result of implementing risk treatments?
- what are the risks that need to be escalated to strategic risks?
- what are the risks that are no longer regarded as strategic risks and why?

Risk treatment

Selection, development and implementation of appropriate options for dealing with risk.

Risk treatment plan

Identifies responsibilities, schedules, the expected outcome of treatments, budgets, performance measures and the review process to be set in place.

Deductible payments

The extent and value of payments made by departments and agencies for insurable items that fall below the deductible level (i.e. excess amount in an insurance policy).

Source: Australian and New Zealand Risk Management Standard AS/NZS 4360:2004; Australian National Audit Office, *Management of Risk and Insurance*, Audit Report 3, 2004 and the Victorian Auditor-General's Office.

Auditor-General's reports

2006-07

Report title	Date issued
Review of major public cemeteries (2006:5)	July 2006
Vocational education and training: Meeting the skill needs of the manufacturing industry (2006:6)	July 2006
Making travel safer: Victoria's speed enforcement program (2006:7)	July 2006
Results of special audits and other investigations (2006:8)	August 2006
Condition of public sector residential aged care facilities (2006:9)	August 2006
Government advertising (2006:10)	September 2006
Auditor-General's Report on the Annual Financial Report of the State of Victoria, 2005-06 (2006:11)	September 2006
Results of financial statement audits for agencies with 30 June 2006 balance dates (2007:1)	February 2007
Giving Victorian children the best start in life (2007:2)	May 2007
State Investment in Major Events (2007:3)	May 2007
Maintaining Victoria's Rail Infrastructure Assets (2007:4)	May 2007
Follow-up of Selected Performance Audits Tabled in 2003 and 2004 (2007:5)	June 2007
Results of Financial Statement Audits for Agencies with other than 30 June 2006 Balance Dates (2007:6)	June 2007
Results of Audits: Purchase of contaminated land by the Melbourne Port Corporation and Raising and collection of fees and charges by departments (2007:7)	June 2007
Public Hospital Financial Performance and Sustainability (2007:8)	June 2007
Administration of Non-judicial Functions of the Magistrates' Court of Victoria (2007:9)	June 2007
Promoting Better Health Through Healthy Eating and Physical Activity (2007:10)	June 2007
Contracting and Tendering Practices in Selected Agencies (2007:11)	June 2007

The Victorian Auditor-General's Office website at <www.audit.vic.gov.au> contains a more comprehensive list of all reports issued by the Office. The full text of the reports issued is available at the website. The website also features "search this site" and "index of issues contained in reports and publications" facilities which enable users to quickly identify issues of interest which have been commented on by the Auditor-General.



Victorian Auditor-General's Office
Auditing in the Public Interest

Availability of reports

Copies of all reports issued by the Victorian Auditor-General's Office are available from:

- Information Victoria Bookshop
505 Little Collins Street
Melbourne Vic. 3000
AUSTRALIA

Phone: 1300 366 356 (local call cost)
Fax: +61 3 9603 9920
Email: <bookshop@dvc.vic.gov.au>

- Victorian Auditor-General's Office
Level 24, 35 Collins Street
Melbourne Vic. 3000
AUSTRALIA

Phone: +61 3 8601 7000
Fax: +61 3 8601 7010
Email: <comments@audit.vic.gov.au>
Website: <www.audit.vic.gov.au>