LEGISLATIVE ASSEMBLY

Public Accounts Committee

RISK MANAGEMENT IN THE NSW PUBLIC SECTOR

Report No.12/53 (No.155) – September 2005

New South Wales Parliamentary Library cataloguing-in-publication data:

New South Wales. Parliament. Legislative Assembly. [Public Accounts Committee]

Report on Risk Management in the NSW Public Sector/ Public Accounts Committee, Parliament NSW Legislative Assembly. [Sydney, NSW] : The Public Accounts Committee, 2005 - pages xii, p 60; 30 cm.

Chair: Matt Brown

"September 2005"

ISBN 073476636

1. Public Accounts Committee – New South Wales
2. Report on Risk Management in the NSW Public Sector

I Title.

II Series: New South Wales. Parliament. Legislative Assembly. Public Accounts Committee Report; no. 155 (12/53)

DDC 658.155

Table of Contents

Membership & Staff

Chairman	Matt Brown MP, Member for Kiama
Vice Chairman	Paul Mcleay MP, Member for Heathcote
Members	Steve Whan MP, Member for Monaro
	Gladys Berejiklian MP, Member for Willoughby
	John Turner, MP, Member for Myall Lakes
	Richard Torbay, MP, Member for Northern Tablelands
Staff	Vicki Buchbach, Committee Manager
	Jackie Ohlin, Senior Committee Officer
	Mohini Mehta, Assistant Committee Officer
	Karen Taylor, Advisor to the Committee
Contact Details	Public Accounts Committee Legislative Assembly Parliament House Macquarie Street Sydney NSW 2000
Telephone	02 9230 2631
Facsimile	02 9230 2831
E-mail	pac@parliament.nsw.gov.au
URL	www.parliament.nsw.gov.au/publicaccounts

Charter of the Committee

The Public Accounts Committee has responsibilities under Part 4 of the *Public Finance and Audit Act 1983* to inquire into and report on activities of Government that are reported in the Total State Sector Accounts and the accounts of the State's authorities.

The Committee, which was first established in 1902, scrutinises the actions of the Executive Branch of Government on behalf of the Legislative Assembly.

The Committee recommends improvements to the efficiency and effectiveness of Government activities. A key part of committee activity is following up aspects of the Auditor-General's reports to Parliament. The Committee may also receive referrals from Ministers to undertake inquiries. Evidence is gathered primarily through public hearings and submissions. As the Committee is an extension of the Legislative Assembly, its proceedings and reports are subject to Parliamentary privilege.

Terms of Reference

The Public Accounts Committee has resolved to conduct an inquiry into risk management in the New South Wales public sector.

Risk Management is defined in the Australian/New Zealand Standard *AS/NZS 4360:2004, Risk Management* (the Standard) as the culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects.

The Committee will examine:

- How NSW public sector has responded to the recommendations in the 2002 Auditor-General's Report to Parliament: *Managing Risk in the NSW Public Sector;*
- How NSW public sector agencies are implementing the requirements of the new Standard*;* and
- The level of progress towards development of better risk management practice in the NSW public sector.

Chairman's Foreword

I am pleased to present this report on the inquiry into risk management in the New South Wales public sector. This inquiry follows up on the 2002 Auditor-General's Performance Audit Report: *Managing Risk in the NSW Public Sector.*

The Auditor-General found that risk management in most agencies was not in accordance with best practice standards. Generally, Public Trading Enterprises were approaching risk management in a more systematic way and performing better in this area than the General Government Sector. Recommendations were made on how the Government and NSW Treasury could improve risk management practices across the NSW public sector. The Committee found in this inquiry that despite Treasury supporting the findings not all of the recommendations made by the Auditor-General have been progressed.

Managing risks effectively is important because of the potential for dire consequences. One such example that was the subject of an inquiry by this Committee was the loss of $41 million in potential revenue during the relocation of the Infringement Processing Bureau.[1]

However, the New South Wales public sector has managed risks positively to prevent disruption or loss of public funds from Y2K and to ensure the smooth implementation of the Goods and Services Tax.

Effective risk management also means maximising opportunities. Typically, the public sector, both in Australia and overseas, has been a risk averse environment. More business-focussed agencies tend to manage risks better. In this inquiry, some agencies identified as challenges to risk management a lack of understanding of how risk management can provide opportunities for improvement and positive outcomes. The Committee considers that training in risk management needs to be more widespread so that more officials develop skills in how to identify and manage opportunities.

During this inquiry, the Committee was provided with specific examples of positive steps being taken by various agencies in relation to risk management. The main impetus behind this continuous improvement appears to be the executive teams within the individual agencies rather than direction from central agencies.

The main way the Committee gathered evidence for this inquiry was through a survey of agencies. The Committee was pleased with the high response rate and the comprehensive information that some agencies, such as NSW Health, supplied to support their survey responses. The majority of agencies surveyed either had well developed risk management practices or provided details of strategies being undertaken to move towards the best practice requirements of the Australian/New Zealand Standard *AS/NZS 4360:2004 Risk Management.* The results of the survey show that progress has been made since the Auditor-General's performance audit, but the following key areas require further development:

- Communication and consultation needs to be a formal two way process that involves both internal and external stakeholders;

[1] NSW Public Accounts Committee, *Inquiry into Infringement Processing Bureau,* Report 6/53 (149), September 2004.

- All agencies should have a risk management policy and treatment plan;
- All agencies should have a business continuity plan and disaster recovery plan;
- Training in risk management needs to be more widespread and develop skills in how to identify and manage opportunities;
- Responsibilities for risk management need to be included in performance agreements and linked to appraisals; and
- The monitoring and review processes need to be enhanced.

I would like to thank all agencies that took the time and effort to complete the questionnaire, make submissions to the Committee and participate in public hearings for the inquiry. I would also like to thank Karen Taylor of the Audit Office of NSW and Vicki Buchbach of the Secretariat for drafting this report for the Committee's consideration. Finally, I would like to thank my fellow Committee members for their discussion of the matters raised in this report.

Matt Brown MP
Chairman

Summary of Findings and Recommendations

FINDING: The key component of the Financial Management Framework is the Results and Services Plans (RSPs). In relation to risk management the following issues remain:

- Not all risks will be addressed as the primary focus is on service delivery risks;
- Preparation of the RSP is not evidence that the agency has implemented effective risk management practices;
- External communication of risks and risk management, as required by best practice standards, is only marginally enhanced. Treasury is only one of the external stakeholders that may be interested in this information; and
- The guidelines are based on standards that are not current best practice.

RECOMMENDATION 1: The guidelines for preparation of the Results and Services Plans (RSPs) need to be updated to incorporate current best practice standards. Treasury should continue to assist agencies with developing their Results and Services Plans. Additionally, external reporting of risks and risk management should be enhanced for example, annual reports to include performance indicators from the RSPs.

FINDING: The Treasury Toolkit is still a useful tool that can assist agencies in assessing and enhancing their internal control systems. COSO II was developed, as COSO I did not provide a robust framework for identifying, assessing and managing risk. As the Toolkit is based on COSO I, the same need for improvement exists.

RECOMMENDATION 2: The Toolkit either needs to be updated to reflect current best practice standards for risk management or be identified as purely an internal control tool. If the Toolkit is updated it should include sample policies, procedures and templates that agencies could adopt.

FINDING: There is no legislation or other requirements that direct agencies to have an effective risk management framework. The executives of individual agencies have been the main impetus behind development of risk management practices. The Treasury Managed Fund has developed the *TMF Guide to Risk Management* to encourage a more consistent and improved approach. However, this guide is not mandatory and its current use is not widespread.

RECOMMENDATION 3: The Government should provide public sector agencies with a risk management framework that supports an enterprise-wide approach. The guidelines, directions, circulars or memorandums should require the following:

- All agencies to have a risk management policy and risk treatment plan;
- All agencies to have business continuity and disaster recovery plans;
- Communication and consultation that is two-way and involves both internal and external stakeholders;
- Responsibilities for risk management to be included in performance agreements and linked to performance appraisals;
- Independent assessment of the appropriateness and effectiveness of identifying and managing risks;

- The heads of agencies to sign off on a corporate governance statement of responsibility; and
- Improved reporting of risk management strategies in annual reports.

RECOMMENDATION 4: The risk management framework should be supported by changes to the NSW financial and annual reporting legislation. These changes should include:

- Defining risk management;
- Assigning the overall responsibility for risk management; and
- Updating the annual reporting regulations to specify the minimum reporting requirements.

FINDING: There are NSW public sector agencies whose functions are interrelated and transcend portfolio boundaries. These and other agencies have common stakeholders and may have common risks. The Committee considers that there is scope for collaboration between these agencies. Such strategies could improve the efficiency and effectiveness of identifying, assessing and managing risks.

RECOMMENDATION 5: Agencies should consider whether collaborating with other agencies with interrelated functions and common stakeholders would be beneficial to their risk management processes. For example, there may be an opportunity to perform multi-agency risk assessments or manage risks in partnership.

Glossary

Term	Definition
AASB	Australian Accounting Standard Board
AS/NZS 4360:2004	Australian and New Zealand Standard AS/NZS 4360:2004 Risk Management
ASX Listing Rules	Australian Stock Exchange standards of behaviour for listed companies.
Business Continuity Plan	A document that defines the organisation's approach to ensuring key functions can continue under any events or circumstances that may develop to interrupt business continuity.
COSO	Committee of Sponsoring Organizations of the Treadway Commission
GCIO	Government Chief Information Office
GFS	Government Financial Statistics
GGS	General Government Sector
ICAC	Independent Commission Against Corruption
IFRS	International Financial Reporting Standards
IPART	Independent Pricing and Regulatory Tribunal
Monitor	To check, supervise, observe critically or measure the progress of an activity, action or system on a regular basis to identify performance levels.
PTES	Public Trading Enterprise Sector
Risk	The chance of something happening that will have an impact on the achievement of objectives.
Risk Analysis	A systematic process to determine the level of risk after consideration of sources, consequences and likelihood.
Risk Criteria	Measures / standards by which the significance of risk can be assessed.
Risk Evaluation	Process of comparing the level of risk against the risk criteria.
Risk Identification	Process of determining what, where, when, why and how something could happen.
Risk Management	The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects.
Risk Management Process	The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk Management Framework	A set of elements and an organisation's management system concerned with managing risks.

Term	Definition
Risk Management Plan	A document containing the: • strategic context and objectives for risk management, • analysis, assessment and prioritising of identified risks, and • approach to managing key risks.
Risk Treatment	Process of selection and implementation of measures to modify risk.
RSP	Results and Services Plan
Stakeholders	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk. They are both internal and external to the organisation.
SBI	Statement of Business Intent
SCI	Statement of Corporate Intent
TMF	Treasury Managed Fund

Chapter One - Introduction

THE PERFORMANCE AUDIT REPORT

1.1 In June 2002, the Auditor-General tabled the performance audit report titled *Managing Risk in the NSW Public Sector.*[1]

1.2 The performance audit examined risk management within the NSW public sector by surveying 26 selected agencies about:

- their understanding of risk and the importance of managing risks in terms of performance;
- how agencies identify risks; and
- the steps they take to manage risks.

1.3 The Audit Office designed and developed a questionnaire to conduct the survey. The questions were based on research of risk management practice in Australia and overseas.

1.4 The performance audit opinion was that:

> while agencies are aware of the need to manage risks, their risk management falls short of best practice. Many agencies do not consider their risk management to be adequate.[2]

1.5 Overall, the audit found that responses from Public Trading Enterprises were more aligned with better practices. Most agencies from the General Government Sector were still operating under the traditional risk management approach of insuring against common types of risk.

1.6 The Auditor-General recommended that the Government:

- Require all agencies in the public sector to manage risks in accordance with accepted standards.
- Progress the recommendation by Treasury that the Chief Executive Officer (and a Board Member, where there is one) provide an attestation to the adequacy and implementation of the internal framework maintained by the agency.
- Require the attestation and risk management procedures adopted to be included in Annual Reports.[3]

1.7 The following recommendations were made to NSW Treasury:

- Ensure that there is a standard for risk management across the public sector which is applied consistently.
- Monitor and report on the implementation of risk management by agencies and the adequacy of information provided in Annual Reports of agencies on management of risk.[4]

[1] Audit Office of New South Wales, *Performance Audit Report: Managing Risk in the NSW Public Sector,* June 2002
[2] ibid, pg 2
[3] ibid, pg 7
[4] ibid, pg 7

NSW TREASURY'S RESPONSE TO THE AUDIT

1.8 Mr John Pierce, Secretary of the NSW Treasury, responded to the performance audit report. He supported the audit report and stated that:

> the audit report supports Treasury's initiatives to manage risk in the NSW public sector.[5]

1.9 At that time, the NSW Treasury asserted that they were monitoring risk management practice in agencies and encouraging better practices. This was being achieved through the following mechanisms:

- Financial Management Framework for the General Government Sector;
- Service and Resource Allocation Agreements (SRAA) between agencies and their Ministers;
- Reviewing the Statements of Corporate Intent/Business Intent for Public Trading Enterprises; and
- Risk Management and Internal Control Toolkit (the Toolkit).

1.10 NSW Treasury made a commitment to promote the use of the Australian/New Zealand Standard on Risk Management, *AS/NZS 4360:1999* by agencies.[6] (It should be noted that this standard was revised in 2004 and is currently *AS/NZS 4360:2004 Risk Management*.)

1.11 The response also included a commitment to consider the audit recommendations and best practice when developing new legislation addressing annual reporting, financial reporting and auditing.[7] To date no significant legislative changes have been made to address these issues.

THE INQUIRY

1.12 The Committee has the power under section 57(1) of the *Public Finance and Audit Act 1983* to examine any report of the Auditor-General laid before the Legislative Assembly. The Committee resolved at its meeting on the 23 March 2005 to conduct a follow up inquiry on the performance audit report titled *Managing Risk in the NSW Public Sector.*

1.13 The Committee called for submissions through publicly advertising on 2 April 2005 and by writing to key stakeholders. Thirty-three submissions were received from a variety of government agencies and private sector consultants. These are available from the Committee's website www.parliament.nsw.gov.au/publicaccounts and are listed in Appendix 2.

1.14 In addition, a survey was conducted across 29 agencies. These agencies are listed in Appendix 1. The survey comprised of a series of questions about the way that agencies manage risk. The questionnaire covered the requirements of *AS/NZS 4360:2004* and also included questions previously asked by the Audit Office to enable an assessment of the progress since 2002. Appendix 4 contains a copy of the questionnaire.

[5] ibid, pg 8
[6] idid, pg 9
[7] ibid, pg 10

1.15 The survey had a response rate of 93 per cent (27 agencies). The Department of Primary Industries was recently restructured and chose to provide a submission in lieu of the survey. One agency did not complete the survey or provide a submission to the inquiry.

1.16 The Committee held public hearings in Sydney on 10 and 24 June 2005. Transcripts of the evidence are available from the Committee's website www.parliament.nsw.gov.au/publicaccounts. Refer to Appendix 3 for the list of witnesses.

1.17 The Committee would like to thank to all individuals and organisations that contributed to the inquiry.

STRUCTURE OF THE REPORT

1.18 Chapter Two provides an overview of risk management including a summary of the best practice requirements of the Australian and New Zealand Standard *AS/NZS 4360:2004 Risk Management*.

1.19 Chapter Three outlines the existing framework in the NSW public sector and how the Auditor-General's recommendations have been addressed.

1.20 Chapter Four outlines how recent developments have been managed and the future challenges that face the NSW public sector.

1.21 Chapter Five discusses enterprise-wide risk management and highlights some of the experiences and the progress that has been made by NSW public sector agencies.

1.22 Chapter Six summarised the results of the survey.

Chapter One

Chapter Two - Risk Management: An Overview

RISK MANAGEMENT

2.1 The revised Australian/New Zealand Standard *AS/NZS 4360:2004*, *Risk Management* was issued on 31 August 2004. The revised standard places greater emphasis on the positive side of risk and provides additional guidance to assist with practical application.

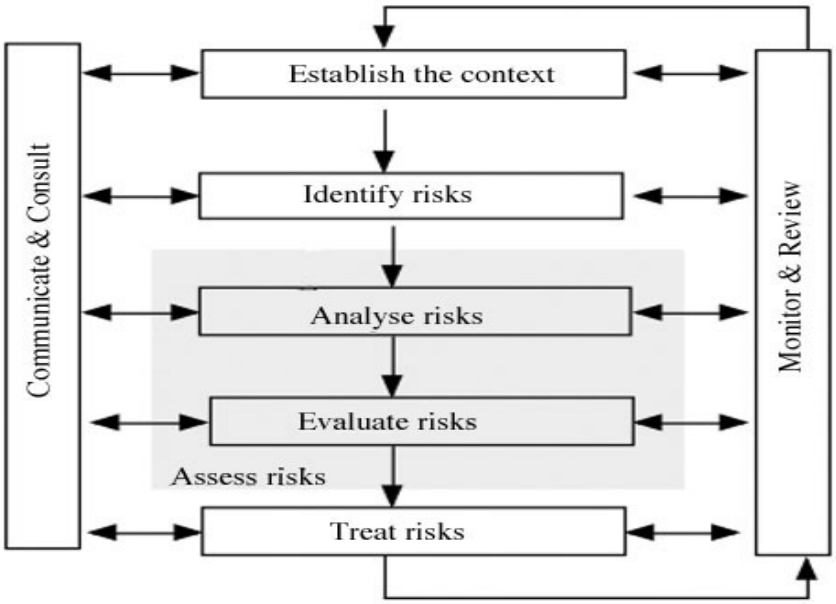
2.2 Risk management is defined in the Standard as:

> the culture, processes and structure that are directed towards realising potential opportunities whilst managing adverse effects.[1]

2.3 The key components of the risk management process are:

- Communicate and consult
- Establish the context
- Identify risks
- Analyse risks
- Evaluate risks
- Treat risks
- Monitor and review[2]

Table 1: Risk Management Process (AS/NZS4360:2004)



2.4 The communication and consultation phase requires two-way communication with internal and external stakeholders. This enables stakeholders to have their views considered and gain an understanding of the decision-making process.

[1] *AS/NZS 4360:2004 Risk Management*, pg 4
[2] ibid, pg 7-8

Communication also influences the culture or an organisation, which has a direct relationship with the ability to effectively manage risks. This step is related to all other parts of the overall process.

2.5 An entity needs to define their relationship with the external environment, understand the internal environment and set the scope and boundaries for application of the risk management process. A set of performance measures for assessing risk need to be established.

2.6 The next phase of the process is to identify, analyse and evaluate risks. It is important that risk identification is thorough to minimise negative outcomes and reduce the likelihood of missed opportunities. Risks are analysed to determine their potential causes, probability of an event occurring and the possible impact. Risk evaluation is when the decisions are made on possible courses of action.

2.7 The traditional approach to treating risk was to insure against the possible financial loss. The rising cost of insurance coupled with the fact that not all major risks can be covered means that this approach is no longer the only option for mitigating risks. Insurance is merely one of the options available for treating risks. Other alternatives include avoiding the risk, reducing the likelihood of negative outcomes, modifying the consequences to reduce the extent of losses, sharing the risk with another party or retaining the risk.[3]

2.8 Regular monitoring and review is a key element of a successful risk management system. Performance of risk management plans need to be assessed and corrective action taken on a timely basis. This step is also vital to the providing continuous improvement to the overall risk management process. Senior executives, line management, internal auditors, external auditors and the audit committee all play a role in monitoring and reviewing the process.

2.9 The risk management framework is an essential element of good corporate governance. It assists in the development of the internal control structure, provides a structure for communication and consultation between stakeholders, reduces the impact of adverse events and provides reasonable assurance to management that the organisation's objectives will be met with an acceptable degree of residual risk.

2.10 The Chief Executive Officer and/or Board have the overall responsibility for risk management, but all employees have a role. The responsibility and accountability for risk management needs to be clearly assigned in job descriptions and key performance indicators be developed to monitor performance. Employees will be more likely to support decisions on risk management if their input in considered, for example being involved in identifying weaknesses in the control environment and having input for possible solutions. Communication channels need to be open to all levels in the organisation to support employee empowerment.

2.11 Commentators have emphasised that it is not just about having the policies and procedures in place. To be effective the substance is clearly more important than the form. The quality of the directors, audit committee members and other executives will have a significant impact on the effectiveness of overall corporate governance. An organisation needs to have a culture that is open, acts with integrity and is

[3] ibid, pg 20

accountable. This requires the correct 'tone at the top', strong leadership, the free availability of information and a willingness to be transparent and behave ethically.[4]

2.12 Effective risk management also means maximising opportunities. The public sector in Australia and overseas has typically been a risk averse environment. Opportunities for wealth creation may be lost where the culture is risk averse. Businesses need to have incentives that encourage creativity and innovation. If a well structured approach to managing risks in undertaken, positive risks can be identified and likelihood of beneficial outcomes assessed. Where both the probability and consequence of a positive outcome is high, plans can be developed to take advantage of the opportunity and manage any associated downside.

2.13 One of the greatest benefits that can be gained in the public sector through the risk management process is the ability to allocate limited resources to areas of greatest need. Some of the other benefits would include:

- improved planning, performance and effectiveness;
- greater opportunity for continuous improvement through innovation;
- improved stakeholder relationships and enhanced reputation;
- improved information for decision-making;
- increased ability to meet corporate goals and be prepared for adversity;
- director/executive protection; and
- accountability, assurance and governance.[5]

2.14 Research conducted by CPA Australia found that line agencies have performed better than central agencies in aligning their strategic objectives with risk management. They found that public sector organisations were most effective in identifying, analysing, evaluating, prioritising and recording risks, but less effective in developing key risk performance indicators and monitoring their performance against these indicators. Central agencies were found to be less effective in all areas, which is of great concern if they are providing the guidance and training to the line agencies.[6]

CONSEQUENCES OF INEFFECTIVE RISK MANAGEMENT

2.15 Obviously, when risk management is ineffective the benefits discussed in the previous section would not be realised. This could lead to more damaging outcomes such as fraud or the business not being able to continue operating.

2.16 The recent corporate collapses in Australia and overseas are evidence of what can happen when risk management and corporate governance are ineffective. Whilst researching the cases of HIH, Enron and the NSW Grains Board, the following common themes became evident:

- Management taking active steps to conceal the true financial position;
- A culture that compromised governance by allowing directors to put their own needs above those of the shareholders, taxpayers and employees;

[4] RJ Sendt, *Driving Organisation Performance Through Best Practice Risk Management in Corporate Governance*, Speech at 8th Annual Corporate Governance in the Public Sector Conference, 27 April 2005, pg 9.
[5] HB 436:2004 *Risk Management Guidelines – Companion to AS/NZS 4360:2004*, pg 8-9.
[6] CPA Australia, *Public Sector Risk Management: A State of Play,* 2002, pg 11.

- Inadequate processes to identify and manage risks; and
- Failure of the auditors and regulators to detect early warning signs.

2.17 The Committee's recent inquiry into the Infringement Processing Bureau highlighted what can occur when project risks are not identified and managed effectively. Not all risks associated with relocating to Maitland or implementing a new computer system were identified. As a result, contingency plans were not in place to mitigate risks such as the risk of fines not being processed within the statute of limitations timeframe. The transition did not go as smoothly as expected resulting in $41 million in lost revenue.

2.18 There is a high expectation that resources will be protected against fraud. In the private sector, shareholders hold these expectations as does the whole community in relation to the public sector. The Australian Institute of Criminology estimates the cost of fraud to Australia to be over $5 billion a year. One of the ways to reduce fraud is to enhance controls that limit the opportunities and increase the likelihood of detection.

2.19 Information technology has an increasingly important role in today's society. Businesses are using the Internet for sales, purchases and other crucial transactions. This exposes organisations to new ways that fraud can be perpetrated or business continuity can be disrupted, for example computer viruses and 'hackers'. The *2004 Australian Computer Crime and Security Survey* found that 49 per cent of respondents had experienced electronic attacks on their systems. These risks need to be managed to reduce the likelihood and impact.

2.20 All consequences of ineffective risk management will result in financial loss, whether in the short term through wasting resources or the long-term through damage to reputations. There may be a failure to meet planned outcomes and excessive resources may be required to delivery services. Lack of preparation requires reactive responses to situations as they arise, which typically uses more resources than identifying risks and putting plans in place to efficiently manage those risks.

RECENT DEVELOPMENTS

2.21 The far-reaching consequences of inadequate corporate governance and risk management practices have forced governments to amend legislation and establish regulators to protect consumers. In the United States (US), the *Sarbanes-Oxley Act of 2002* has resulted in a move towards enterprise risk management. A number of Australian subsidiaries of US listed companies and Australian companies that wish to raise capital in the US are affected by this legislation.

2.22 The *Corporate Law Economic Reform Program (CLERP 9)* was introduced in Australia to give legal backing to corporate governance. It requires a robust enterprise-wide risk management framework and internal control system. Companies registered under the *Corporations Act 2001* and public sector agencies that are subject to this Act are affected by these changes.

2.23 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a private sector organisation dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. On the 27 September 2004, they published *Enterprise Risk Management – Integrated Framework* (COSO II) to provide a robust enterprise wide framework for identifying,

assessing and managing risks.[7] This document goes beyond internal control, which was the main focus of *Internal Control – Integrated Framework* (COSO I). The Treasury Tookit was based on COSO I.

2.24 The Australian Stock Exchange (ASX) issued Corporate Governance Council guidelines in March 2003.[8] The guidelines consist of ten principles each with best practice recommendations. Risk is a factor in many of the principles, but principle 7 specifically requires the establishment of a sound system of risk oversight and management and internal control. Under ASX Listing Rule 4.10, companies must disclose in their annual reports any departures from the best practice recommendations contained in the guidelines.

2.25 There has been an increase in the number of regulators and other bodies whose main objectives are to protect consumers. The powers of the existing bodies have been expanded to satisfy the demands placed on governments by the general public. The changes in the regulatory environment will continue to impact on the risks that an organisation faces.

2.26 There is a major change in financial reporting on the horizon with the international harmonisation of accounting and auditing standards. The Australian Accounting Standards Board (AASB) has issued all of the Australian equivalents to the International Financial Reporting Standards and Interpretations. All reporting entities in both the public and private sector need to adopt these requirements for financial years commencing on or after 1 January 2005. Organisations need to ensure that changes to software, amendments to policies and procedures and restatement of opening balances are completed within the time frame. Financial reports are at risk of being qualified and this along with volatility in reported profits may have an impact on share prices.

2.27 The next issue for the AASB is the harmonisation of Government Financial Statistics (GFS) with generally accepted accounting principles. This will enable Government reports to be comparable across jurisdictions and have a direct relationship with the budget statements. The AASB has established the Reference Committee to monitor the project. This Committee includes representatives from the AASB along with senior members of State and Commonwealth Treasury Departments.[9]

[7] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework*, September 2004, Executive Summary, pg v

[8] ASX Corporate Governance Council, *Principles of Good Corporate Governance and Best Practice Recommendations,* March 2003.

[9] www.aasb.com.au, *GAAP/GFS Convergence: Implementing the FRC Strategic Direction,* 13 December 2004, pg 4.

Chapter Two

Chapter Three - NSW Public Sector Framework

PUBLIC EXPECTATIONS

3.1 The public have placed increasing demands on governments to protect consumers, deliver services and utilise limited resources for the benefit of taxpayers. In New South Wales, this has resulted in the formation of regulators such as the Independent Pricing and Regulatory Tribunal (IPART) and authorities like the Independent Commission Against Corruption (ICAC). Whilst shareholders are primarily interested in the return on their investments, taxpayers have varied and conflicting objectives. They want quality services without an increased tax burden. Taxpayers expect that their contributions will be utilised in the most efficient and effective way.

3.2 In similar ways that companies are accountable to their shareholders, public sector organisations are accountable to taxpayers. Robust performance reporting is required to allow the public to assess how resources are being utilised. Increased transparency will inevitably highlight agencies that have managed risks poorly. Members of the community expect that limited resources will be used wisely and that the exposure to negative outcomes, including loss of public funds, will be minimised.

3.3 Planning in the public sector is moving from the traditional focus on inputs and processes to results and services. This more strategic approach increases the complexity and number of mechanisms required to ensure individuals and agencies are fulfilling their responsibilities. Public sector agencies are formally accountable to Ministers, Parliament, the Auditor-General, central agencies, clients and other governance bodies. They are informally accountable to their profession, peers, political parties, media, interest groups and the general public.[1] Annual reports are the main source of publicly available information on the performance of an agency. However, not all agencies are including comprehensive information on how taxpayers are receiving value for money.

3.4 Consequently in 2002, the NSW Auditor-General made the following comments in relation to the effectiveness of accountability arrangements:

> ...public sector agencies in New South Wales – with very few exceptions – are still reluctant to publish meaningful performance information. Many do include some statistics in their annual reports comparing performance over recent years...very few agencies release information benchmarking themselves against their interstate or overseas counterparts.....They seem to feel little obligation to demonstrate they are achieving value for the taxpayer's dollar.[2]

3.5 In their submission to this inquiry, NSW Treasury linked accountability to risk management:

> The NSW public sector operates in an environment characterised by changing community expectations about service delivery, the need for greater cost efficiencies, and higher levels of accountability and transparency. It is important, therefore, that public sector agencies develop the capacity to routinely identify, prioritise and manage risks.[3]

[1] John Halligan, *Australian handbook of public sector management*, December 2000, pg 176-177.
[2] The Audit Office of NSW, *Auditor-General's Report to Parliament 2002 Volume Four,* November 2002, pg 1-2.
[3] Submission No. 33, NSW Treasury, pg 2.

3.6 This poses the following question: what framework has been established to ensure agencies are equipped with the knowledge, tools and guidance to develop effective risk management practices? Public sector entities are subject to a variety of regulations and policies that cover risk management requirements. The remainder of this Chapter will explore the roles that Government, Treasury, audit committees and auditors play and then outline some of the current NSW requirements.

ROLE OF GOVERNMENT

3.7 The UK Government Strategy Unit describes the three distinct roles that the Government has in handling risk and uncertainty. Firstly, they have a regulatory role to provide a legal framework to balance the risks and rewards where individuals or businesses impose risks on others. Secondly, they have a stewardship role to provide protection against risks from the outside, such as natural disasters, security risks or public health risks. Finally, they have a management role in relation to their own business of providing services and performing regulatory and stewardship functions.[4]

3.8 The Strategy Unit points out that public expectations of government service delivery continues to increase and meeting these expectations carries considerable risks. The role of government in risk management and the issues raised are relevant to Australian Governments.

3.9 As noted in Chapter One, the Auditor-General recommended in the performance audit report that the Government:

- Require all agencies in the public sector to manage risks in accordance with accepted standards.
- Progress the recommendation by Treasury that the Chief Executive Officer (and a Board Member, where there is one) provide an attestation to the adequacy and implementation of the internal framework maintained by the agency.
- Require the attestation and risk management procedures adopted to be included in Annual Reports.[5]

3.10 The submission from Treasury included responses on behalf of the Government in relation to these recommendations. Treasury believes that the existing risk management framework is consistent with generic risk management practices, but has made a commitment to review guidelines to ensure they are consistent with the revised best practice standards. The Government has decided to defer changes to financial and reporting requirements until convergence with international standards is completed. The attestation requirements will considered at this time.[6]

ROLE OF TREASURY

3.11 The identification and management of risk is a key element of resource allocation and therefore it is appropriate for Treasury to oversee this process.[7]

[4] The UK Government Strategy Unit, *Risk: improving government's capability to handle risk and uncertainty,* November 2002, pg 9-10.
[5] Audit Office of New South Wales, *Performance Audit Report: Managing Risk in the NSW Public Sector,* June 2002, pg 7.
[6] Submission No. 33, NSW Treasury, Executive Summary
[7] Submission No.9, John Bushell Value Management Pty Limited, Pg 1

3.12 Treasury confirmed in their response to the recommendations in the performance audit report that they play a vital role in facilitating better risk management in the NSW public sector. This includes:

- Monitoring and reporting on implementation of risk management by agencies;
- Ensuring there is a standard for risk management across the public sector; and
- Reviewing adequacy of information disclosed in annual reports.[8]

3.13 The core function of Treasury is financial management so consequently financial risks are the primary focus of their reviews.[9] Treasury monitor agency and project level risk as part of General Government budget monitoring. This process includes reviewing the results logic, risks and risk management strategies captured in the Results and Services Plans (RSPs). Treasury monitor Government businesses through the negotiation of the Statements of Business Intent/Corporate Intent (SBI/SCI) and the quarterly reporting regime. Treasury also review asset strategies and asset performance related risks captured in the Total Asset Management Plans.[10]

3.14 Treasury's current focus has been on the Results and Services Plans (RSPs) for General Government budget dependent agencies. The guidelines for preparing these plans along with other policies and guidelines that cover risk management are outlined in the remainder of this Chapter. There is no current standard for risk management that is applied consistently across the sector. However, Treasury do review the adequacy of information provided in the annual reports.

3.15 The submission from Treasury outlines how it contributes to the Government's objective of ensuring there is a consistent approach to managing risks associated with service delivery:

- Managing aggregate financial risk through the fiscal strategy and balance sheet management;
- Managing agency and project level risk and advising the Government about these risks; and
- Promoting risk management processes by providing agencies with access to guidelines on good risk management.[11]

3.16 Treasury believes that it will encourage improved risk management practices by raising awareness of better practice, building the capacity of agencies to undertake strategic risk analysis and by monitoring and providing feedback to agencies. It will ensure that guidelines are consistent with current risk standards.[12]

3.17 In July 2004, Treasury began a project to help analysts to improve their knowledge of agencies, build better relationships with agencies and enhance their analytical skills. As part of this project, Treasury is developing a new financial risk management framework to provide a decision process to guide analysts in identifying and assessing the level of agency risk. Analysts will have a streamlined set of guidelines that aligns

[8] Audit Office of New South Wales, *Performance Audit Report: Managing Risk in the NSW Public Sector,* June 2002, pg 8-9.
[9] Correspondence from Mark Ronsisvalle, 2 August 2005, pg 3.
[10] Submission No. 33, NSW Treasury, Executive Summary
[11] ibid, Pg 2
[12] Correspondence from Mark Ronsisvalle, 2 August 2005, pg 5.

monitoring strategies with risk levels and will assist with allocation of Treasury's resources.[13]

Treasury Managed Fund

3.18 The Treasury Managed Fund (TMF) is the indemnity scheme that covers all insurable risks of the participating government agencies. There are currently 155 agencies utilising this scheme.[14] The overall purpose of the TMF is to provide structure and services to assist agencies in reducing the impact of risks and maximise resources available to conduct their core business. Treasury assists the TMF by promoting risk management and efficient insurance practices within agencies.

3.19 The explanatory notes for insurance contracts with the TMF state:

> The obligation attached to the coverage is accountability through the implementation and practice of risk management principles. Government, like the private sector, believes that following risk management principles creates a more efficient management environment and reduces both the frequency and severity of losses, thus saving taxpayers' money.[15]

3.20 Under the *TMF Scheme Structure*, agencies must:

- conduct regular risk assessments and perform risk management tasks for all exposures; and
- implement appropriate risk identification measurements, mitigation and management procedures. [16]

3.21 To assist agencies with these responsibilities, the fund manager provides risk management services including development and dissemination of best practice risk management models and systems, training and support of agency-initiated projects. However, it should be noted that the primary focus of the TMF is on insurable risks whilst the main area of focus for this inquiry is on risks that cannot be mitigated through insurance.

3.22 In their submission to this inquiry, the NSW Fire Brigades acknowledges the TMF Risk Management Unit for the assistance it has provided in developing the risk management framework for the Brigade.[17]

ROLE OF AUDIT COMMITTEES

3.23 The Committee recently reviewed the operations of audit committees and found that all respondents had an audit committee in place or were in the process of forming one. However, not all of the audit committees were complying with better practice of having external members and being chaired by someone other than the Chief Executive Officer or the Chairman of the Board. The Committee recommended that all agencies have an audit committee with suitably qualified members including an

[13] ibid, pg 6
[14] ibid, pg 2
[15] Treasury Managed Fund, *Treasury Managed Fund Scheme Structure*, March 2004, pg 3.
[16] ibid, pg 6
[17] Submission, No.21, NSW Fire Brigades, Pg 2

external member and that a Treasury Direction be drafted to assist agencies in improving the operations of their audit committees.[18]

3.24 Audit and/or risk management committees play an important role in corporate governance. In relation to risk management, the committee should assess the scope and effectiveness of systems that identify, assess, manage and monitor risks faced by the organisation.[19] To enable this role to be fulfilled, the committee members must be appropriately qualified and/or receive adequate training in risk management.

3.25 To be effective in their role, the audit committee needs to be independent and have the power to seek explanations and ask the difficult questions. As noted in the Committee's recent report, an audit committee should have external members to enhance actual and perceived independence.

3.26 During this inquiry, the Deputy Auditor-General made the following comments about the how an audit committee fits within the risk management framework:

> **Mr WHITFIELD:** ....A good example would be Sydney University where they have appointed a risk manager. Their audit committee is a risk management committee as well as an audit committee, and at each meeting they are updated as to the progress that has been made and the risk manager has gone out to various business units within the university, the faculties and schools, briefed the people and helped them assess the risk from a bottom up level as well as the audit committee looking at risk from the top down. If that type of structure was used more widely throughout the sector, together with reporting requirements, then it would strengthen the whole risk management within the public sector.[20]

3.27 In relation to risk management, the audit committee should be responsible for ensuring:

- There is a current and comprehensive risk management framework that allows risks to be identified and managed effectively;
- A sound and effective approach has been followed in developing risk management plans for major projects;
- The internal audit coverage and annual work plan is reviewed and based on the entity's risk management plan;
- The impact of the risk management framework on the control environment and insurance arrangement is reviewed;
- Business continuity plans have been implemented and disaster recovery plans are tested periodically; and
- The fraud control plan is reviewed and the entity has appropriate processes and systems in place to capture and effectively investigate fraud.[21]

ROLE OF AUDITORS

3.28 The Chairman of the Australian Prudential Regulation Authority has stated the following on the role of internal auditors:

---

[18] NSW Public Accounts Committee, *Review of Operations of Audit Committees,* Report 11/53 (154), April 2005, v-vii.
[19] KPMG, *Internal Audit's Role in Modern Corporate Governance,* September 2003, pg 1
[20] Anthony Whitfield, Transcript of Hearing, 24 June 2005, pg 8.
[21] ANAO, *Better Practice Guide – Public Sector Audit Committees,* February 2005, pg 10-13.

> Now more than ever, a robust and objective internal audit function, with the skills to identify risk control problems and the authority to pursue its concerns, is essential to the proper discharge of directors' responsibilities....In this demanding environment, boards and senior management need quality advice from sources that can be trusted and that can offer an objective viewpoint.[22]

3.29 According to *AS/NZS 4360:2004*, internal and external audit both have roles in risk management assurance and monitoring. Their scope is narrower and reviews performed less frequently than continuous monitoring and line management review. The focus should be on compliance with policies and procedures. However, to be effective, the assurance and monitoring processes need to be continuous and dynamic. Agencies cannot simply rely on auditors to fulfil this requirement.

3.30 Under the principles of COSO II, internal auditors have key support responsibilities whilst external auditors are not responsible for the effectiveness of enterprise-wide risk management.[23] The audit committee must utilise internal audit to assist with the fulfilment of their responsibilities. Auditors need to have a direct reporting line to the audit committee to enhance independence.

3.31 The Institute of Internal Auditors state that risk management is the foundation for effective internal control and internal auditing. The role of internal audit is to assist an organisation by identifying and evaluating the significant exposures to risk, and making contributions to improve risk management and control systems. Internal audit also evaluates internal control effectiveness and efficiency and promotes continuous improvement in these areas.[24]

3.32 Auditors-General, private sector auditors and accounting bodies contribute to improving risk management practices through issuing better practice guides, conducting research and making recommendations to their clients.

3.33 NSW public sector agencies have an internal audit function that is either in-house, outsourced to an external party or a combination of the two. Internal Audit Bureau Services provide internal audit, risk management and other consultancy services exclusively to the NSW public sector. Their methodology for providing risk assessments and developing risk management frameworks is based on *AS/NZS 4360:2004.*[25] The Committee heard evidence on the role of internal auditors:

> **Mr O'TOOLE**: Yes, the role of internal auditors have evolved and our organisation has evolved over recent years from being compliance based - what is referred to as tick and flick auditing, accounts payable, accounts receivable audit, those sort of asset items financially focussed to being more of a risk based program, which is operational based on the key objectives of the organisation. So rather than just recycling the previous programs, we go to speak to the executive or to the audit committee and recommend that as a precursor for the development of a new focus for audit planning that we undertake a risk assessment. Once we get into the process they see the value of that.[26]

[22] John F Laker, Chairman of APRA, *The Role of Internal Audit – A Prudential Perspective,* Speech given to The Institute of Internal Auditors-Australia, NSW Chapter Sydney, December 2004.
[23] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrated Framework*, September 2004, Executive Summary, pg 6
[24] Institute of Internal Auditors Australia, *National Position Statements on Accountability and Control,* 2003, pg 5-6.
[25] Submission No.13, IAB Services.
[26] Phillip O'Toole, Internal Audit Bureau Services, Transcript of Hearing, 10 June 2005, pg 23.

3.34 In the NSW public sector, the Auditor-General is the external auditor for all government agencies. The findings of these audits are reported to the agencies concerned and to Parliament. Information provided by both internal and external auditors can be used to identify risks, manage risks and improve the overall control structure.

3.35 The main role of the Audit Office is to provide assurance over the financial statements and they do not review the risk management practices. The Committee heard in evidence that:

> **Mr WHITFIELD**: What we do look at is the risks that are associated with the financial aspects of the organisation, so the preparation of financial statements, in terms of determining what sort of controls they have put in place to mitigate those risks so that we can conduct the audit in an effective way. As the Auditor-General has said, we do not look at the entire risk profile of the organisation. When we are doing an audit, we are assessing risks from an audit perspective, not from an organisation operational perspective from the agency's viewpoint.
>
> **Mr SENDT**: In fact, we might find shortcomings in the controls that an organisation has. That does not mean we will give an adverse audit opinion, because if any auditor finds that controls are not working as they should, or not as strong as they should be, the auditor will apply other procedures to gain enough evidence to demonstrate that the financial report is materially free of misstatement, so I think organisations need to understand that a clean audit opinion is not a guarantee of their risk management approach is sound or the controls are in place.[27]

University Reviews

3.36 The NSW Auditor-General reviewed the risk management processes at each university during 2003 and continued to monitor their progress during 2004. Initially it was reported that the universities were at different stages of developing and implementing their risk management policies and procedures:

> At some universities the full array of risks is neither known nor explicitly managed and there is an absence of formal risk assessment processes. Universities that are at a more advanced stage……have: reviewed existing risk profiles; identified and analysed key risks; produced inherent risk profiles; produced risk registers; and developed treatment/action plans. These universities now need to develop on-going monitoring and reporting processes….[28]

3.37 The most recent review found that all universities have taken steps to address the issues reported in the prior year. In evidence before the Committee:

> **DEPUTY CHAIR:** Can we talk about your review into universities, risk management practices at universities. I understand that you did recently review risk management practices at universities. Did you hit all of them?
>
> **Mr WHITFIELD:** Yes, we did that as part of a compliance review. Because we do the audit ourselves of the ten universities it is a good group to actually trial some of our new diagnostic tools and one of them was a risk management tool that we are going to be rolling out over the top 50 agencies. We trialled it on the universities to make sure that we had the right package. What we did find was that it varied. I quoted the example of Sydney University is probably up one end of the spectrum and down the other end there

[27] Transcript of Hearing, 24 June 2005, pg 10

[28] Audit Office of New South Wales, *Auditor-General's Report to Parliament 2004 Volume Two,* 19 May 2004, pg 27.

are some of the smaller universities that are just starting to get in to the swing of putting together a risk management plan.[29]

3.38 This review has resulted in universities moving towards best practice in risk management. It would be beneficial to expand this audit process to other public sector entities. This independent review would strengthen risk management monitoring and review processes and assist agencies in continuously improving their risk management practices. The Committee supports the Audit Office performing similar reviews of risk management practices for the top 50 agencies.

LEGISLATIVE REQUIREMENTS

3.39 The *Public Finance and Audit Act 1983* requires agencies to have an effective system of internal control, but does not specifically address risk management. The internal control system is one of the mechanisms that assist management in minimising negative outcomes. However, it is not the only component of an effective risk management process.

3.40 Treasurer's Direction 900.01 assigns the responsible for risk management and insurance arrangements to the head of an authority. Historically in NSW and in other jurisdictions, entities have tended to focus on managing insurable financial risks. This assignment of responsibility is commendable, but directions have limited application and as the tendency has been to focus insurance not all risks are being captured.

3.41 General Government agencies are required under the *General Government Debt Elimination Act 1995* to have sound risk management principles for financial risks. There is no corresponding legislative requirement for agencies outside this sector. Also, as mentioned previously, financial risks are only one of a number of risks facing the NSW public sector.

3.42 The enabling legislation of certain agencies includes specific requirements in relation to risk management. For example, under the *Rural Fires Act 1997,* the NSW Rural Fire Service is required to appoint Bush Fire Management Committees who are responsible preparing bush fire risk management plans.

3.43 Under annual reporting legislation, agencies are required to report on risk management.[30] The legislation does not define risk management or specify the how much detail needs to be included. Treasury performs a review of selected agencies annual reports. The Annual Reports Review program for both the 2002-03 and 2003-04 financial years identified that some agencies only provided limited details on risk management.[31]

3.44 NSW Treasury in its 1998 discussion paper, *Fundamental Review of NSW Financial and Annual Reporting Legislation*, suggested that amendments to legislation would include expanding the definition of internal control to include risk management and requiring the CEO to include a statement of responsibility. Also, in its response to the 2002 Auditor-General's Report , Treasury agreed to amend legislation to improve the NSW risk management framework. The Committee has been advised that, since

[29] Anthony Whitfield, Transcript of Hearing, 24 June 2005, pg 13.
[30] *Annual Reports (Departments) Act 1985* and the *Annual Reports (Statutory Bodies) Act 1984* and associated Regulations
[31] Treasury Circulars 04/05 and 05/07*Annual Reporting Update*.

then, the Government has decided to defer consideration of changes to this legislation until the implementation of International Financial Reporting Standards is completed.[32]

3.45 Treasury is of the opinion that:

> ...the most cost-efficient and effective approach to improving risk management practices is to create incentives for practising – rather than simply mandating – better risk management processes. A strategic approach to business planning can create these incentives by promoting the integration of risk management with corporate, business, financial, physical asset and workforce planning.[33]

3.46 There is evidence that changes to legislation alone will not equate to effective risk management. Under Victorian legislation, most agencies are required to have a risk strategy, but their Auditor-General has found that risks are not being identified and managed consistently or effectively. The Victorian Auditor-General has recommended, among other things, that standard guidelines be issued for the identification, assessment and management of State-sector risks and that agencies report on their risk management framework in their Annual Reports.[34]

3.47 This view was supported by the Chief Financial Officer of the Department of Commerce:

> **Mr HUNTER:** You could have legislation and that would just mean that whatever you put in the legislation that is exactly what you will get, but I think the Government probably wants a bit more than that. I think you said it is culture.
> **CHAIR:** Who is going to drive that, you or Treasury?
>
> **Mr HUNTER:** Within our own organisation it is the Commerce executive, but within the public sector generally, Treasury, Premier's, Cabinet Office. It is probably a central agency that will drive that.[35]

3.48 Mr Phillip O'Toole, from IAB Services, expressed the following opinion:

> **CHAIR:** ...Do you think any amendments to public sector legislation need to be made to strengthen the risk management framework?
>
> **Mr O'TOOLE:** I don't know about legislation. I think that there could be guidelines attached to the Public Finance and Audit Act which would strengthen the risk identification and reporting to Treasury, make it a regular component of their reporting regime. I think there could be probably some sort of mandatory actions or recommendations arising out of audit committees.[36]

3.49 However, in the case of occupational health and safety (OH&S), there is a strong legislative framework with penalty provisions that has led to consistent risk management practices.[37] The OH&S area is primarily being managed in isolation from the corporate risk management framework so even where best practice exists in this area it is not permeating throughout the organisation. An example of this would be that websites and annual reports of agencies often include comprehensive descriptions of their OH&S risks and how they are managing these risks, but are mainly silent on other risk areas.

---

[32] Submission No. 33, NSW Treasury, pg 17.
[33] Correspondence from Mark Ronsisvalle, 2 August 2005, pg 3.
[34] Auditor-General Victoria, *Managing risk across the public sector,* March 2003, pg 52-54.
[35] Alastair Hunter, Transcript of Hearing, 24 June 2005, pg 34.
[36] Phillip O'Toole, Transcript of Hearing, 10 June 2005, pg 23
[37] Submission No. 1, Recovre Pty Ltd

3.50 Witnesses from the Audit Office made the following comments on how to improve risk management practices:

> **CHAIR:** In your opinion what would be the most effective way to ensure all agencies apply the best practice requirements of the standard?
>
> **Mr SENDT:** …there should be a greater requirement on CEOs or boards, where there are boards, to report on risk management approaches and activities they undertake and an obvious place for them to report on that would be in their annual report. I think those requirements should be strengthened.
>
> **Mr WHITFIELD:** I would agree with that, Mr Chairman. I think whilst there is an existing requirement under the Annual Reports Act to report on risk management. I think there needs to be more direction given from central agencies, such as Treasury, as to the type of information that should be reported and the frequency of it …
>
> **Mr HORNE:** …it would now be considered absolutely essential for any private sector organisation to include risk management as a fundamental part of their corporate governance and their reporting externally to their shareholders and to the world. We should do the same and Government agencies should report externally about what they are doing with risk management.
>
> By turning it from an internal management practice into external reporting issue it focusses the mind on it quite clearly. It elevates it to the executive level somewhat more and I think that by those mechanisms we could then see better audit committees pick this up and address it more vigorously than they have done in the past.
>
> **CHAIR:** …Do you think you would need amendments to public sector legislation, or Premier's memorandum, or what do you think would be the appropriate way to try to address that?
>
> **Mr SENDT:** Certainly legislation would be one way to approach it. The danger with that is that techniques, expectations, can change over time. I this it is probably preferable to have a central agency, Premier's Department or Treasury, driving the change. It could be by way of Premier's memorandum, Treasurer's direction, Treasury circulars, but I think that whichever central agency takes up the role if that does happen, they can give far stronger guidance as to their expectations and what good risk management means and what good reporting risk management means.
>
> I think that the advantage of approaching it from the reporting end is that while it may be the end point of good governance or good risk management, it does give that very public focus and very strong expectation that behind the reporting there would be substance to the risk management.[38]

3.51 Any changes to legislation need to stand the test of time and remain relevant. This means the more detailed requirements should be included in guidelines, directions, circulars and/or memorandums from central agencies. However, there is still a role for legislation especially in strengthening the reporting requirements. Currently, there is no public sector legislative or other requirements that compel all agencies to implement an effective enterprise-wide risk management framework.[39] The main drivers of change are the management teams within the various agencies. The Committee considers there is a role for central agencies to take responsibility for guiding and encouraging all agencies to move towards best practice.

[38] Transcript of Hearing, 24 June 2005, pg 7-8.

[39] OH&S and other legislation require risk management in specific areas, but not an enterprise-wide approach that covers both insurable and non-insurable risks.

CURRENT POLICIES AND GUIDELINES

Financial Management Framework

3.52 Treasury issued the *Financial Management Framework for the General Government Sector* in December 2000. The Framework's purpose is to improve the outcomes from Government programs and service delivery to ensure taxpayers receive value for money.[40] It highlights five principles that are central to this process: clarity of objectives; proper allocation of responsibility and accountability; appropriate, comprehensive incentive structures; performance management and integrity of information.[41]

3.53 One of the key strategies, to ensure taxpayers receive value for money, is to help agencies build strategic risk analysis capabilities that are integrated with their business processes. The initial pilot program required the 11 largest General Government Sector (GGS) agencies to establish Service and Resource Allocation Agreements (SRAAs) with their Ministers. 2004-05 was the final financial year for SRAAs. The lessons learned during this pilot program have assisted with the development of the RSPs.[42]

3.54 As stated in the Treasury submission:

> As part of the 2004-05 Budget process, a streamlined funding plan approach was extended to all General Government budget dependent agencies through the Results and Services Plan (RSP). The RSP process is now the principle vehicle that Treasury employs to promote better risk management.
>
> The RSP is a high-level business plan that demonstrates the relationship the services that an agency delivers and the results that it is working towards, and sets out how resources will be deployed to achieve those results and services. It is prepared by agencies specifically to support decision-making by Budget Committee.[43]

3.55 Part 6 of the RSP requires the agency to identify risks, assess the potential impact on results and outline the strategies for managing those risks. The guidelines to assist with completion of this part are based on *AS/NZS 4360:1999* and *HB 143:1999 Guidelines for Managing Risk in the Australian and New Zealand Public Sector.*[44] Both of these publications have been superseded.

3.56 RSPs do not encompass all risks faced by the organisation. The Committee heard in evidence that:

> **Mr RONSISVALLE:** The results and services plans provide an incentive to actually consider risk management as a key part of an agency's operations. The results and services plan does not deal with all risks. It tends to more deal with service delivery risks.[45]

3.57 Furthermore, an agency could complete the risk section of their RSP without having a risk management policy, formal treatment plan, business continuity plan or other components of best practice risk management. Hence, having a RSP does not equate to the agency having effective risk management practices.

---

[40] Value for Money means resource allocation that is efficient, effective and appropriate.
[41] TPP 00-4 *Financial Management Framework for the General Government Sector,* December 2000, pg 1.
[42] Submission No. 33, NSW Treasury, pg 4.
[43] ibid
[44] Treasury Policy and Guidelines Paper TPP04-4, *What You Do and Why: An Agency Guide to Defining Results and Services,* October 2004.
[45] Mark Ronsisvalle, NSW Treasury, Transcript of Hearing, 24 June 2005, pg 18.

3.58 During the hearings, agencies made the following comments in relation to RSPs:

- It has helped us to understand and define what our business is about;
- It has assisted us in defining and ranking our risks;
- It forms the basis for identifying risks or impediments to service delivery; and
- It assisted with embedding our objectives and strategies into business planning.

3.59 Currently, the RSPs are confidential documents between Treasury and the budget dependent agency. Some agencies have elected to structure their corporate plan using the same key result areas and performance measures. A few agencies have taken the next step to report on some of those measures in their annual reports. The corporate plans and annual reports are publicly available. The Commissioner for Children and Young People provided the following evidence:

> **CHAIR:** …In your survey response you claim to be effective in both the development of your key performance indicators to measure success of strategies and emerging issues and the monitoring of strategies against key performance indicators. Are you able to show the Committee any evidence to support that response?
>
> **Ms CALVERT:** Yes, we use the results and services framework, which has been developed by Treasury, which sets out what the results of the organisation are, what the intermediate results are, how we might measure those intermediate results and then what are the service groups that underpin and feed into those results. Each of the intermediate results and the service group have performance indicators that are reported on either quarterly to the executive or annually through our annual report, which is then oversighted by the Joint Parliamentary Committee on Children and Young People.[46]

3.60 It is Treasury's intention that aspects of the RSPs be published in the future:

> **Mr RONSISVALLE:** In the longer term what we would like to try and do is connect together the results and services plan, what appears in budget papers and what gets reported in annual reports. That is the sort of the linkage we would like to establish.
>
> **Mr MCLEAY:** Are we at the beginning of stage one of that process?
>
> **Mr RONSISVALLE:** You will find that the budget papers are evolving over time to start picking up the things that are in the results and services plan. For 2006/07 we are intending to modify some of the layout of the budget papers to pick up a montage from the results and services plan framework and …also…the indicator is reported in an annual report so there is some accountability.[47]

3.61 The key component of the Financial Management Framework is the RSPs. In relation to risk management the following issues remain:

- Not all risks will be addressed as the primary focus is on service delivery risks;
- Preparation of the RSP is not evidence that the agency has implemented effective risk management practices;
- External communication of risks and risk management, as required by best practice standards, is only marginally enhanced. Treasury is only one of the external stakeholders that may be interested in this information; and
- The guidelines are based on standards that are not current best practice.

[46] Gillian Calvert, Transcript of Hearing, 10 June 2005, pg 4.
[47] Mark Ronsisvalle, Transcript of Hearing, 24 June 2005, pg 26.

RECOMMENDATION 1: The guidelines for preparation of the Results and Services Plans (RSPs) need to be updated to incorporate current best practice standards. Treasury should continue to assist agencies with developing their Results and Services Plans. Additionally, external reporting of risks and risk management should be enhanced for example, annual reports to include performance indicators from the RSPs.

Commercial Policy Framework

3.62 The framework is a collection of policies and guidelines that aim to ensure that government businesses operate efficiently and in accordance with commercial best practice. The main documents within the framework that relate to risk management include:

- *Statement of Corporate Intent/Business Intent (SCI/SBI) Guidelines*
- *Treasury Management Policy; and*
- *Total Asset Management Manual.*

3.63 All Public Trading Enterprise Sector (PTES) agencies are required to prepare either a SCI or SBI detailing their objectives and strategic direction of the business. One component of this document is the Annual Risk Management Statement which includes:

- How the planning and implementation of risk management fits within their business operations;
- An overview of the risk management plan;
- The relationship between major risks and the value drivers including indicators to track their performance;
- An analysis of major risks including the likelihood and consequences; and
- Quantification of the potential impact on value drivers for major risks including strategies to manage those risks.

3.64 Government businesses are required to report to Treasury each quarter on their performance against risk indicators and any developments in relation to major risks. Treasury uses these reports and information from the SCI/SBI to monitor risk management within agencies and then report any significant issues to the Treasurer on a quarterly basis.[48]

3.65 The results of the survey show that 60 per cent of PTES agencies rate their risk management practice at the lower end of the scale. They have identified weaknesses in the identification, treatment and monitoring of risks. This would obviously impair the quality and completeness of the information reported in their Annual Risk Management Statements. Consequently, Treasury may not be aware of all of the significant issues.

3.66 The *Treasury Management Policy* requires all agencies to establish policies and procedures to identify, quantify, assess and actively manage financial risk. The responsibility vests with the Board or, where there is no Board, the highest level of

[48] Submission No 33, NSW Treasury, pg 13

management. The quarterly SCI/SBI reports must include performance benchmarking of the treasury management function.

3.67 The *Total Asset Management Manual* contains significant risk management guidelines in relation to physical assets. These guidelines are based on *AS/NZS 4360:2004*. Agencies, other than state owned corporations, are required to have a systematic process for identification of asset related risks, perform analysis and develop ongoing measures to manage them. The *Total Asset Management (TAM) Policy* requires agencies to annually prepare and submit their TAM plans to Treasury. It is a key component of the annual budget allocation process. However, having sound risk management processes for assets does not necessarily mean an effective enterprise-wide risk management framework has been established.

Toolkit

3.68 In September 1997, Treasury issued the *Risk Management and Internal Control Toolkit.* It was designed to assist agencies in implementing their risk management and internal control frameworks. It was based on the *Internal Control – Integrated Framework* (COSO I) developed in the US by the Sponsoring Organizations of the Treadway Commission (COSO). In 2004, the *Enterprise Risk Management – Integrated Framework* (COSO II) was published. It incorporates both the internal control framework and provides a robust enterprise-wide framework for identifying, assessing and managing risks.

3.69 The Toolkit specifically refers to Treasury Policy and Guidance Papers[49] on best practice standards for internal control and commits to review and revise these documents as new information becomes available. These documents have not been updated even though best practice in this area has changed significantly over the past 10 years.

3.70 The submission from the Audit Office states:

> The Treasury Toolkit is now out of date and does not reflect current best practice, given that it is based upon COSO I which has since been significantly updated. If the Treasury guidelines and Toolkit are intended to be 'the standard' for NSW public sector agencies, they need to be updated now and on an on-going basis.[50]

3.71 Treasury agreed with the Auditor-General that the Toolkit needs to be updated, but their resources are currently being utilised in developing RSPs:

> **Mr RONSISVALLE:** It does need some updating. There have been a few standards that need to be updated. It needs to be integrated with the other documents we have put out since then.[51]

3.72 The results of the survey for this inquiry found that 65 per cent of agencies in the GGS and 20 per cent in the PTES have used the Toolkit, but the use was primarily in the past. The respondents made the following comments concerning the Toolkit:

- Overly complex approach that can limit risk identification to a low level that may not result in the best use of resources;

[49] TPP95a *Statement of Best Practice- Internal Control and Internal Audit* and TPP95b *Internal Control Assessment*

[50] Submission No 11, Audit Office of New South Wales, p4

[51] Mark Ronsisvalle, Transcript of Hearing, 24 June 2005, pg 18.

- Too complex and lacks practical application;
- Does not address identification of opportunities or communication strategies;
- Useful high level document;
- The case studies should be reviewed and modernised; and
- Needs to be updated to reflect best practice standards and recent corporate governance reforms.

3.73 The Toolkit is still a useful tool that can assist agencies in assessing and enhancing their internal control systems. COSO II was developed, as COSO I did not provide a robust framework for identifying, assessing and managing risk. As the Toolkit is based on COSO I, the same need for improvement exists.

RECOMMENDATION 2: The Toolkit either needs to be updated to reflect current best practice standards for risk management or be identified as purely an internal control tool. If the Toolkit is updated it should include sample policies, procedures and templates that agencies could adopt.

Other Treasury Publications

3.74 The responsibility for setting policies and procedures for whole-of-government procurement and asset management was transferred to the Treasurer in June 2003. In July 2004, the *NSW Government Procurement Policy* was issued as the framework for all government procurement.[52] These policies and procedures apply to all government departments, statutory authorities, trusts and other government authorities, but not to state owned corporations. All procurement that is high risk or requires funding of at least $10 million ($5 million for information technology) is subject to a Gateway review.[53] Risk management for the project is one of the key factors that will be assessed by this review.

3.75 Another Treasury publication is the *Working with Government: Guidelines for Privately Financed Projects*. It provides guidelines for performing risk analysis for all privately funded projects. This document also contains a sample risk table outlining the description, consequence, mitigation strategy and preferred allocation basis for each key risk category.

3.76 More recently, the *TMF Guide to Risk Management – the RCCC Approach* was published. This guide was developed as a joint initiative between the TMF Risk Management Unit and the Public Sector Risk Management Association. The purpose of the guide is to provide government managers and personnel with broad guidance and a framework for managing risk in the NSW public sector.[54] It brings together the myriad of public sector requirements and better practice standards. It also provides source documents, sample case studies and directions to available resources. The Department of Health has distributed the guide to health services across NSW.[55]

[52] Treasury Circular NSWTC 04/07 *Procurement Policy Reform* contains further information.
[53] The Government Procurement Services Unit of the Department of Commerce has been engaged to conduct these reviews at no cost to the agencies. They will assess whether appropriate levels of discipline have been applied at key stages in the procurement process, without diminishing agency responsibility.
[54] Submission No. 33, NSW Treasury, Attachment 3, pg3.
[55] Submission No. 32, Minister for Health, pg 14.

3.77 Currently the *TMF Guide* is available through a password protected site for agencies that have their insurance maintained by the TMF, but other agencies can obtain a copy on request. Treasury has informed the Committee that it will make this document more widely available by placing it on Treasury's general website, www.treasury.nsw.gov.au.[56]

3.78 When Treasury was asked about the role of this guide, Treasury officials gave the following response:

> **Mr NEALE:** It is guidance to agencies that assists them in managing their risk. The aim of the Treasury is to offer incentives to them to do better, particularly with their insurable risks.
>
> **CHAIR:** What sort of incentives?
>
> **Mr NEALE:** Monetary incentives basically. When agencies join the fund we assess their risk and how much they should pay in premiums and we set premiums having regard to benchmarking from other states, where that is possible. The bigger departments certainly are influenced by the performance of other states and we set a benchmark premium for them. At the end of the day what they actually pay to the TMF for their insurance cover depends on their actual performance. If they do badly they will pay more and if they do well they get rewards. The Department of Health on a regular basis does well on managing its insurable risk, the primary one being worker's compensation.[57]

3.79 The guide covers both insurable and non-insurable risks, but as the TMF's focus is insurance the incentives are linked to insurable risks.

E-Government

3.80 The NSW Government is committed to electronic service delivery. The *Information Management and Technology Blueprint for NSW - A Well-Connected Future* shows how the NSW Government proposes to effectively use information management and technology to create accessible and responsive government services and deliver them to the community using a seamless communications network linking homes, workplaces and public institutions. Part of the strategy includes a public sector wide approach to avoid duplication and promote consistency. The policies and guidelines that support the e-government strategy clearly provide a strong risk management framework for managing projects and information security.

3.81 The following risk management documents were issued by the Government Chief Information Office (GCIO) to enable agencies to use, manage and plan information technology that is consistent with whole-of-government directions:

- *Project Risk Management Guideline:* defines risk, outlines issues to be considered, details the key roles and responsibilities and provides a step-by-step risk management process in accordance with *AS/NZS 4360:2004; and*
- *Information Security Guidelines for NSW Government – Risk Management:* provides direction for information security risk management.

3.82 These guidelines are meant to form part of the overall risk management approach of the agency and are consistent with best practice requirements. It should be noted that the guidelines do not apply to state owned corporations.

[56] Correspondence from Mark Ronsisvalle, 2 August 2005, pg 2.
[57] Ian Neale, Transcript of Hearing, 24 June 2005, pg 23.

CONCLUSION

3.83 The Committee notes that there is no legislation or other requirements that direct agencies to have an effective risk management framework. The executives of individual agencies have been the main impetus behind development of risk management practices. The Treasury Managed Fund has developed the *TMF Guide to Risk Management* to encourage a more consistent and improved approach. However, this guide is not mandatory and its current use is not widespread.

RECOMMENDATION 3: The Government should provide public sector agencies with a risk management framework that supports an enterprise-wide approach. The guidelines, directions, circulars or memorandums should require the following:

- All agencies to have a risk management policy and risk treatment plan;
- All agencies to have business continuity and disaster recovery plans;
- Communication and consultation that is two-way and involves both internal and external stakeholders;
- Responsibilities for risk management to be included in performance agreements and linked to performance appraisals;
- Independent assessment of the appropriateness and effectiveness of identifying and managing risks; and
- Improved reporting of risk management strategies in annual reports.

RECOMMENDATION 4: The risk management framework should be supported by changes to the NSW financial and annual reporting legislation. These changes should include:

- Defining risk management;
- Assigning the overall responsibility for risk management; and
- Updating the annual reporting regulations to specify the minimum reporting requirements.

Chapter Four - Developments and Challenges

4.1 This Chapter outlines how recent developments have been managed and the future challenges that face the NSW public sector.

OTHER DEVELOPMENTS

Business Continuity Management

4.2 A business continuity plan is an enterprise-wide plan to maintain and/or restore business operations in the event of a disaster at a level and within a time frame that is acceptable to management. Previous Auditor-General's reports have highlighted this area as a key control weakness for a significant number of agencies.

4.3 The *Information Security Guidelines for NSW Government* provides information on how to develop and maintain effective business continuity management. Agencies are required to report to the Government Chief Information Office (GCIO) on their progress in implementing information security requirements. The survey results in Chapter Five show that not all agencies have completed their information security requirements, including the development of a business continuity plan.

4.4 The Committee heard the following evidence on the importance of business continuity plans:

> **Ms BEREJIKLIAN:** ...How important do you regard business continuity plans and what component of your overall risk strategy does that play? ...
>
> **Mr MARTIN:** In response to that I would like to say that EnergyAustralia is committed to business continuity management. We have been down the path now for about two years. We try and link it back in to risk management by the risks that general managers identify through their operational risks linked to the strategic risks, which are married together. We find there are areas, which are vital to the business which would bring us undone, if we lost our data agency, our billing, we would be in trouble, if we lost our contact centre where we communicate with people. So we link those risks together and in the risk management documentation it says how is it managed or what is the strength of that risk and it is linked back through the business continuity plan and we have a network incident plan, we have a corporate incident management plan, we have data agency disaster recovery plans and information technology business impact analysis. They are all carried out to ensure that as the identification of the risk cascades out to the line of business, where the effect of that line of business is there should be a continuity plan in place and a disaster recovery to get us back up.[1]

Records Management

4.5 The use of email by NSW public sector agencies has increased dramatically over the last few years. It is an efficient mechanism for communicating across government and with external stakeholders. There is an increased risk that e-mails may not be managed in accordance with the legislative requirements of the *State Records Act 1998.*

4.6 State Records have issued policies, templates and guidelines to assist agencies with managing electronic messages.

[1] Francis Martin, EnergyAustralia, Transcript of Hearing, 10 June 2005, pg 19

Intellectual Property

4.7 There have been many documented cases in Australia of intellectual property (IP) being lost to the private sector or even to other countries due to inadequate management. ICAC has identified research by employees or contractors at universities and health services as high-risk areas for possible misuse of IP. In both sectors, the individuals may use IP owned by public sector agencies to further their own business interests. Another concern is that commercial arrangements may be entered into without the public sector receiving appropriate ownership or benefits from the products or services developed.

4.8 In 2001, the Auditor-General's performance audit on *Management of Intellectual Property* found that agencies had limited knowledge of IP and were not managing their IP assets effectively. The risks and benefits associated with IP were not being assessed and this may have resulted in private companies benefiting from public sector IP.[2] The Audit Office issued the *Better Practice Guide: Management of Intellectual Property* to assist agencies in developing policies and procedures for the efficient and effective management of IP. NSW Agriculture (now part of the Department of Primary Industries) and TAFE NSW (within the Department of Education and Training) were identified as frontrunners in managing IP.

4.9 In response to the performance audit, an inter-agency working group was formed to develop an IP management framework based on a risk management approach. In February 2005, the Premier's Department issued the *Intellectual Property Management Framework for the NSW Public Sector.* The principles of this framework are mandatory for all GGS agencies and are recommended for the PTES. The Institute of Public Administration Australia NSW (IPAA) ran a training course, *Intellectual property: a risk management approach,* in February and July 2005.

4.10 The Auditor-General released a follow-up audit in March 2005. The audit found that some agencies had taken the initiative to develop policies and practices for managing IP. The report acknowledged the framework developed by the Premier's Department, but also highlighted the challenge of implementation.[3]

4.11 Eleven per cent of the agencies surveyed are not considering the loss of intellectual property during their risk assessment process. It is understandable that agencies would still be in the process of implementing the framework and management of IP should improve by 2006.

Information Security

4.12 As reliance on information technology increases so does the exposure to risk of computer crime including fraud. ICAC has emphasised the need for better information security to minimise this risk. GCIO and ICAC have issued publications and developed training programs to assist agencies in improving security over government information. The approach being undertaken to strengthen information security is a risk based approach and will become one of the components of an enterprise-wide risk management framework.

[2] The Audit Office of New South Wales, *Performance Audit: Management of Intellectual Property,* October 2001
[3] The Audit Office of New South Wales, *Follow-up Performance Audit: Management of Intellectual Property,* March 2005, pg 2.

4.13 Premier's Circular 2001-46 requires that all agencies safeguard their electronic information and obtain certification to the Australian and New Zealand Standard *AS/NZS 7799 Information Security Management*. The critical steps to certification are to establish a security framework comprising:

- a document outlining the context;
- a policy;
- a risk assessment; and
- a Statement of Applicability that describes how *AS/NZS 7799* controls will be applied as a result of the risk assessment.

4.14 The Auditor-General recently conducted a compliance review on information security that included a review of agency progress towards certification. He found that agencies had achieved various levels of progress towards meeting the deadlines set by the Government. Part of the process requires a full risk assessment to ensure that the necessary controls are in place to cover all risks. It is interesting to note that almost half of the agencies reviewed had not performed this risk assessment to the satisfaction of the independent auditors.[4]

FUTURE CHALLENGES

Risk Management Expertise

4.15 As mentioned in Chapter Two, the risk management knowledge of the directors, audit committee members and executives of an organisation will have a significant impact on the strength of their framework. The number of people with the necessary skills is finite and many private sector companies are utilising a high proportion of these resources to comply with *Sarbanes-Oxley*, ASX listing rules, Corporations Law and other requirements. As a result, not all public sector agencies may be able to obtain the necessary expertise to improve their risk management practices.

4.16 Some agencies are addressing this issue by hiring consultants, but they must ensure the knowledge is maintained by the agency after the consultant has completed the engagement. Other agencies are obtaining the expertise by inviting representatives from IAB Services, private sector internal audit providers or the Audit Office to be members of their audit committees. Training courses can also assist in developing the risk management skills within the public sector.

Fraud

4.17 The Auditor-General has estimated that the potential risk of fraud in the NSW public sector is between $1.2 billion and $3.0 billion annually.[5] The report recommends that Treasury initiate a minor amend to legislation to provide a legislative basis for fraud control and extend the application of fraud control requirements to non-budget sector agencies. Amongst other recommendations, agencies were encouraged to adopt or enhance the regularity and robustness of fraud risk assessments. The audit found that the results of the self-assessments performed by the university, health and the non-budget sector were worse than the overall ratings for the NSW public sector.

[4] The Audit Office of NSW, *Auditor-General's Report to Parliament 2004 Volume Four,* pg 14-17.
[5] The Audit Office of NSW, *Performance Audit Report Fraud Control: Current Progress and Future Directions,* February 2005, pg 2.

4.18 Australian standards on governance cover fraud control and corruption prevention. Auditing standards have also been revised to increase the focus on fraud control and require management representations that systems and procedures are in place to effectively deal with fraud. These requirements are applicable to both the private and public sectors and should result in management dedicating time and resources to this area.

4.19 This shows that fraud is an increasing risk, but currently in NSW there is no formal process to monitor implementation of fraud control and there is no legislative backing. In other jurisdictions, such as the Commonwealth public sector, there is legislation to support their fraud control framework.

E-Government

4.20 The public sector utilises information technology to communicate, to assist with business processes and to delivery public services. As the use of information technology such as email and the internet increases so does the risk that criminals will attempt to access personal information to commit fraud. Information security needs to continually evolve to minimise the risk and ensure business objectives continue to be achieved.

4.21 Computer viruses and other threats will become more prevalent. To minimise the risk of business disruptions causes by viruses and other threats, business continuity planning is vital.

4.22 Delivering services via the internet helps to meet the growing demand for 24 hour service, but exposes the agency to new risks. "Phishing" has emerged as a major problem on the internet. The object of phishing is usually to obtain information about people in order to commit fraud. The number of new unique phishing emails has grown from 107 in December 2003 to 13,142 in February 2005.[6] Email is only one of the ways that phishing can be performed.

4.23 The current guidelines on managing information technology in the NSW public sector and the requirement for agencies to be certified against *AS/NZS 7799 Information Security Management* will help to minimise these risks.

Management of Major Projects and Outsourcing Arrangements

4.24 In the NSW public sector there have been major infrastructure and software projects that have exceeded the budget, not been completed in accordance with planned deadlines and/or not met expectations. There have also been outsourcing arrangements that have failed to delivery expected outcomes. One of the contributing factors would be inadequate risk assessment and ineffective management of those risks.

4.25 There is an increase in the level of private sector involvement in the delivery of government services, for example the construction of major infrastructure. One benefit is the ability to transfer the risk to the private sector, but obviously, the cost will be built into the arrangement. Where the risk is not allocated appropriately or the arrangement is more favourable to the private sector partner, the government may incur additional unforeseen costs. These arrangements also create challenges for accountability and transparency. Auditors-General, public agencies, Ministers and

[6] Australian Institute of Criminology, High Tech Crime Brief 2005/09, *Phishing*.

Parliament access to information they require to perform their responsibilities may be restricted.

4.26 To ensure accountability and transparency is maintained, it is important that public sector executives have the necessary skills to negotiate and manage contracts. This includes the ability to identify and manage the underlying risks within and outside the public sector. There is the potential for significant liabilities to be passed onto the government due to the wording of the contract. For example, the receivers for the failed Airport Link Company are seeking compensation from the NSW public sector.[7]

IFRS

4.27 The accounting and auditing landscape is undergoing change with the adoption of international financial reporting standards (IFRS). Organisations were required to restate their opening balances as at the 1 July 2004 from Australian generally accepted accounting principles to the new harmonised standards. Due to the delay in the release of Standards from the AASB, the number of changes that are still occurring and the delay in guidance from central agencies, the restatement of opening balances is not completely finalised.

4.28 There are many risks associated with adoption of IFRS. Some examples include the risk that:

- Financial reporting deadlines will not be met;
- Financial statements will be qualified for incorrect or incomplete application of accounting standards;
- Budgets may be misstated resulting in possible cash flow issues for budget dependent agencies;
- Inaccurate profit estimates of state owned corporations could reduce estimates for dividends and taxation; and

4.29 Agencies may not identify the need to modify or replace application systems. This may result in additional costly manual procedures to overcome the deficiencies of the computer environment.

[7] The Audit Office of NSW, *The Auditor-General's Report to Parliament 2004 Volume Four,* pg 282.

Chapter Five - Progress Towards Best Practice

5.1 This Chapter discusses enterprise-wide risk management and highlights some of the experiences and the progress that has been made by NSW public sector agencies. The evidence of agency progress has been obtained during hearings and from submissions.

ENTERPRISE-WIDE RISK MANAGEMENT

5.2 Enterprise-wide risk management can:

- be a tool that supports decision-making;
- improve management reporting;
- identify and manage areas of concern;
- improve allocation and prioritisation of resources; and
- help an organisation achieve their objectives and strategies through more robust corporate planning.[1]

5.3 Effective risk management requires a robust framework to effectively identify, assess and manage risk at a strategic level across an enterprise. As stated by the previous Commonwealth Auditor-General:

> a measure of maturity of risk management in the Australian public sector is the extent to which entities have embraced organisation-wide risk management, sometimes known as enterprise risk management, and integrated it with their strategic objectives and operational culture.[2]

5.4 The Australian National Audit Office has found that while progress has been made, there is still more to be done before all public sector organisations have risk management as a central element of their day-to-day management approach.[3] This observation is relevant for the NSW public sector, which is still in the process of moving from the traditional silo approach of risk management towards an enterprise-wide risk management framework.

5.5 Similarly, many private sector studies have also found that companies also have a way to go before they are managing risk on an enterprise-wide basis. It is seen as a daunting, but necessary task. *AS/NZS 4360:2004* is seen as an effective tool in establishing sound risk management practices. Felix Klomen, a leading US risk management expert, stated that:

> AS/NZS 4360:2004 was and still remains the clearest and most concise guideline yet published. Its text, only 28 pages, is a model of brevity. It is expressed in simple and basic English, free from business jargon. Because its approach is generic, it applies to all forms of organizations.[4]

5.6 The Audit Office has observed that both public and private organisations in Australia are adopting *AS/NZS 4360:2004*. This opinion is supported by the results of the

[1] CPA Australia, *Enterprise-Wide Risk Management Better Practice Guide for the Public Sector,* 2002, pg 12.
[2] ANAO Audit Report No.58, *Control Structures as part of the Audit of Financial Statements of Major Australian Government Entities for the Year Ending 30 June 2004,* 26 June 2004, pg 49.
[3] Pat Barrett, *Future Challenges for Risk Management in the Australian Public Sector (APS),* Speech at RMIA ACT Chapter Conference, Canberra, 7 April 2005, pg 6.
[4] Felix Kloman, *Risk Management Reports,* November 2004, Volume 31, No. 11.

Committee's survey, submissions received by this inquiry and evidence provided at the public hearings. The Auditor-General stated in his submission:

> As the external auditor for the NSW public sector, we place great importance on agencies embracing risk management in a meaningful, practical way. We see some signs of this happening. But we think that it needs further stimulation, and a consistent approach in the sector would be desirable.[5]

5.7 There is some assistance available to help agencies develop enterprise-wide risk management. A useful feature of the *TMF Guide to Risk Management* is the inclusion of a reference list of other publications and resources that may assist agencies in developing their risk management practices.

5.8 In addition, CPA Australia issued a better practice guide to assist government agencies in understanding risk management and to provide a framework to encourage full integration with strategic planning and operations.[6] EnergyAustralia and the NSW Police Service are included in the case studies that support this better practice guide. However, none of the agencies surveyed have specifically mentioned that they have utilised this document in developing their risk management practices.

PROGRESS OF AGENCIES

5.9 The adoption of enterprise-wide risk management in the NSW public sector is varied. The Committee heard in evidence:

> **CHAIR:** In your opinion how widespread is the adoption of an enterprise-wide risk management approach across the public sector?
>
> **Mr O'TOOLE:** It is at various stages, some agencies have adopted it wholeheartedly, other agencies would not have a great awareness of it. Usually the larger agencies with the more commercial focus have embraced and it is part of their business. The smaller more traditional public service departments, depending on their size, it is very mixed, their adoption of it.[7]

5.10 Submissions were received from established agencies that are currently working towards improving their risk management practices. Some of the positive steps being taken by these agencies are outlined below.

5.11 The risk management framework in the NSW Rural Fire Service is primarily decentralised with the strongest area being their *Bush Fire Risk Management Plans* for each Rural Fire District. The Service acknowledges the need for an overarching policy, but the current model was designed to mirror the nature of their operations. The Service uses specific software to standardise business planning and management. The program uses a risk management approach to identify issues and potential areas for improvement. To assist with risk identification, standard documents are used to assess the internal and external environment. The Service is currently completing an organisational risk assessment, which will be used to develop an enterprise wide risk management policy and 2006-07 strategic plan.[8]

5.12 NSW Fire Brigades current policies and procedures are based on *AS/NZS 4360:2004* and advice from the TMF. The formal risk assessment process that has been

[5] Submission No.11, The Audit Office of NSW, pg 4.
[6] CPA Australia, *Enterprise-Wide Risk Management Better Practice Guide for the Public Sector,* 2002.
[7] Phillip O'Toole, Transcript of Hearing, 10 June 2005, pg 23.
[8] Submission No.12, NSW Rural Fire Service

developed includes risk types, consequence and likelihood matrices and captures opportunities. The plan is to have an enterprise-wide risk management framework, but there are still some development needs, for example moving from individual risk registers to an organisation wide risk register. NSW Fire Brigades are making progress beyond the organisation through facilitating multi-agency risk assessments. It has been a challenge to develop risk criteria that are satisfactory to all agencies.[9]

5.13 The Auditor-General's report on risk management and *AS/NZS 4360* influenced Workcover to perform risk assessments for several major activities, for example relocating to Gosford. In 2003, their Risk Management Committee performed a high level risk assessment, evaluated risks, developed treatment plans and established a risk register. A consultant was then engaged to expand on the internal review and provide the basis for audit planning. From 2006, the CEO and the Board will be providing attestations in relation to risk management.[10]

5.14 The Department of Gaming and Racing plans to engage IAB Services to provide an independent risk management assessment, which includes development of recommendations that can used to prepare the risk management plan.[11] The department has identified that there is room for improvement and decided to source expert assistance.

5.15 EnergyAustralia implemented business risk management in the early 1990s as a direct result of commercialisation and the appointment of a commercially run board. Representatives from EnergyAustralia believe that their risk management system complies with best practice requirements. The following evidence was heard:

> **Mr KEAN:** ...Today we believe we have in place a formal systematic approach to identifying managing and monitoring risks. Our system applies to both strategic and operational risks. We have integrated our processes into our culture and our risk assessments as part of our everyday decision making process. We obtain sign offs at the highest levels regarding the management of risks. Risk management is an essential component of EA's governance and management practices.
>
> In respect of the terms of reference for this inquiry, EnergyAustralia is satisfied that it fully complies with the principles of the 2002 Auditor General's report to Parliament; the requirements of the risk management standard and we believe we are operating at best practice levels in regard to risk management.[12]

5.16 EnergyAustralia's internal procedures require risk management attestations from all managers prior to finalisation of the budget and annual accounts processes.

Impact of Restructures

5.17 More than 25 per cent of the surveyed agencies were either recently established through amalgamation of other agencies or have undergone a restructure. It is understandable that their risk management frameworks have not been fully developed or integrated across the organisation. However, they have comprehensive plans for the development of their risk management frameworks. Some positive examples of these plans are outlined below.

[9] Submission No.21, NSW Fire Brigades, pg 1-2
[10] Submission No.24, Workcover New South Wales, pg 1-2
[11] Submission No.15, Department of Gaming and Racing
[12] Noel Kean, EnergyAustralia, Transcript of Hearing, 10 June 2005, pg 15.

5.18 During the initial restructuring phase, the Department of Environment and Conservation continued to operate on the basis of risk assessments performed by its foundation agencies. Relying on the past experience of the amalgamated agencies allowed the department to maintain its risk management framework without requiring additional resources. It has now begun to develop an integrated and improved framework based on *AS/NZS 4360:2004*.[13]

5.19 The Department of Commerce explained how the restructure impacted on its risk management framework:

> **CHAIR:** You have had a major restructure of your department. How does that impact on your risk management framework?
>
> **Mr M TURNER:** Significantly, in a word. In 2003 Commerce was brought about, in about April I think it was formed. Prior to that New South Wales Commerce was a Department of Public Works and Services and had undertaken a facilitated series of workshops with PriceWaterhouseCoopers in order to identify organisational risk. Part of the challenge that was then thrown to what was then Commerce, was to determine the risk management framework across the board. Broadly, the approach that we have taken within Commerce is to have a look at *AS/NZS 4360:2004* which is the risk management standard and that is the policy that was then endorsed by the risk and audit committee in December of last year and promulgated thereafter. On that basis, we have then been developing the principles and model, which was put before the risk development committee in April of 2005.
>
> The intention behind those things was, rather than take a fragmented approach, to ensure that there was a consistent approach, so to deal with some of those management type issues. We feel that this is important because unless there is a consistent understanding of not only the framework but also the definition and identification of risk, you can end up with an inconsistency of treatment. From that perspective what we are trying to do is to ensure that risks across the State are mitigated in terms of Commerce's ability to have an influence over the management of those risks, whether it is in a construction arm or whether it is in procurement, in making arrangements for broad based contracts for goods or services across the State, but also as it pertains to the workplace relations through the Office of Industrial Relations and also to fair and equitable trading with consumers and between businesses through the Office of Fair Trading.[14]

5.20 In response to the Auditor-General's findings on risk management, the Department of Education and Training established a steering committee to implement its risk management framework. Progress was delayed due to the restructure in 2003. In March 2004, the Director-General initiated an enterprise-wide review of corporate governance, which included risk management. Action is currently being taken to address the issues identified by this review. Their recently developed policies and procedures for risk management are based on *AS/NZS 4360:2004*.[15]

5.21 On 1 July 2004, the Department of Primary Industries was formed through a combination of four agencies. It is currently in the process of developing an integrated and comprehensive risk management strategy in accordance with the requirements of *AS/NZS 4360:2004.* As part of this process, the risk management systems of the former agencies were reviewed and the positive aspects formed the

[13] Submission No.17, Department of Environment and Conservation
[14] Marcus Turner, Department of Commerce, Transcript of Hearing, 24 June 2005, pg 30.
[15] Submission No.26, Department of Education and Training

basis of risk management for the new organisation.[16] A lot of work still needs to be carried out before effective enterprise-wide risk management is achieved.

5.22 On 1 January 2005, 17 Area Health Services were amalgamated to form eight new entities. Some of the new entities adopted the risk management practices of the former Area Health Services, but others have started over. The Committee heard the following evidence:

> **Mr WHAN:** Do all area health services have a risk management plan of some kind or another? …
>
> **Mr McGREGOR:** No, all area health services have risk management plans. As part of our review of corporate governance, which we undertook in late 2004 and early 2005, it was clear to us, and the Auditor-General has commented on this before, that the implementation had been variable. That is not surprising given the very significant changes that occurred in September, with the removal of the boards, the change in structure and the creation of the new eight area health services. Some of the new areas, rather than going through the process from January to now, have adopted the risk management plans of the former areas. They now have to go back and redo the whole exercise, and we hope to be able to give them a common framework across the system to assist them to do that.
>
> **Mr WHAN:** What is your timeframe on doing that?
>
> **Mr McGREGOR:** We hope to have the corporate governance and risk management plans in place in the next two to three months. We hope that by the end of the year the area health services will have a very clear framework to go forward with fairly uniform risk management frameworks.[17]

5.23 NSW Health has developed *Corporate Governance Guidelines for Chief Executives of Area Health Services.* These guidelines include risk management as one of the key areas of accountability. Chief Executives and internal auditors are required to conduct governance reviews for submission to the Director-General and the Department of Health. These reviews include an assessment of the risk management plan. In addition, the Chief Executives need to include a Corporate Governance Statement in their annual reports. Among other things, this Statement attests to the fact that the Chief Executive is responsible for risk management and has established a risk management plan.[18]

5.24 The Department of Health will shortly establish a Corporate Governance and Risk Management Branch. One of its tasks will be to develop a standard NSW Health risk management procedure as recommended by their internal auditors.[19] This will enable enterprise-wide risk management, which should lead to a more efficient and consistent approach.

5.25 It is evident that agencies that have undergone a restructure have experienced delays in establishing effective risk management practices that are integrated across the organisation. However, in some cases restructuring has been a good opportunity to integrate risk management into the strategic and operational plans of the new entity.

[16] Submission No. 27, Department of Primary Industries
[17] Robert McGregor, NSW Health Department, Transcript of Hearing, 10 June 2005, pg 25-26.
[18] Submission No. 32, Minister for Health.
[19] ibid, pg 14.

The new entity will also benefit from the strengths of the former agencies, including an increased knowledge base.

CONCLUSION

5.26 The Committee has found that NSW public sector agencies have made some positive steps towards meeting best practice requirements for risk management. All agencies that gave evidence at the hearings acknowledged the importance of risk management in strengthening their overall corporate governance framework.

Chapter Six - Survey Results

6.1 The survey was sent to 29 agencies from the General Government and Public Trading Enterprise Sectors. The response rate was 93 per cent (27 agencies). The survey comprised of a series of questions about the way the agencies manage risks. The questions covered the requirements under *AS/NZS 4360:2004* and included questions previously asked by the Audit Office to enable an assessment of progress that has been made since 2002. Appendix 4 contains a copy of the questionnaire.

6.2 As with all surveys, the findings do not necessarily apply to all participants or reflect on risk management practice across all agencies in the NSW public sector. When interpreting the results, allowances should be made for the subjective nature of self-assessment and respondents' varying degrees of familiarity with best practice requirements.

6.3 The responses to the survey outlined below are prefaced by a key element of better practice from the Standard. Where possible, comparisons have been made with the results of the survey conducted by the Auditor-General in 2002. It is important to bear in mind that the current requirements of are more comprehensive than the previous standard and agencies that are more familiar with these new requirements may be more critical in their self-assessment.

6.4 Eighty-nine per cent of respondents to the survey agreed that *AS/NZS 4360:2004* had significantly contributed to the development and implementation of risk management within their organisation. Over 70 per cent of respondents recognised that the Auditor-General's findings from the performance audit had influenced their risk management policies, procedures and practices.

COMMUNICATE AND CONSULT

> ***Key element:*** *Communicate and consult with internal and external stakeholders at each stage of the risk management process and concerning the process as a whole. A communication plan should be developed that addresses issues relating to both the risk itself and the process to manage it.*

6.5 Before communication processes can be established, stakeholders need to be identified. Severny-six per cent of the agencies surveyed in GGS and 90 per cent in PTES have identified their stakeholders, but less than 50 per cent have performed a stakeholder analysis.

6.6 Seventy-one per cent of respondents in the GGS and 40 per cent in the PTES do not have a communication and consultation plan. This represents an improvement from 2002 when the Auditor-General reported that 92 per cent of GGS agencies and 73 per cent of PTES were without a plan. These results are supported by research findings that public sector agencies do not effectively communicate their risk management policies and practices with external stakeholders.[1]

6.7 One-way communication can be achieved through the Internet, intranet, annual reports and newsletters. The alternative is a two-way consultation process. The advantages of two-way communication include:

[1] CPA Australia, *Public Sector Risk Management: A State of Play,* 2002, pg 13.

- Involving various parties helps to establish improved culture and embed risk management in the day-to-day business environment;
- Creating a value adding opportunity by partnering with other agencies with common risks;
- Transparency builds trust with internal and external stakeholders;
- Involving stakeholder can enhance the risk assessment process and assist with selecting the most appropriate risk treatment; and
- Stakeholders are more accepting of decisions when they understand the process and feel that their input is being valued.

6.8 The majority of agencies in both sectors are mainly using one-way communication methods and the primary focus is on internal stakeholders. Some of the positive examples of two-way communication in the NSW public sector include:

- NSW Rural Fire Service provides executive support to Bush Fire Management Committees. The co-ordination of fire fighting and bush fire mitigation involves continual information exchange between government and non-government organisations.[2]
- NSW Fire Brigades is moving towards multi-agency risk assessments within the emergency services sector. This will involve collaboration with a number of agencies.[3]
- The Commission for Children and Young People is continually interacting with its stakeholders to ensure that NSW is a better place for children and young people.[4] This mutual collaboration is required under their enabling legislation.

6.9 There are NSW public sector agencies whose functions are interrelated and transcend portfolio boundaries. These and other agencies have common stakeholders and may have common risks. The Committee considers that there is scope for collaboration between these agencies. Such strategies could improve the efficiency and effectiveness of identifying, assessing and managing risks.

RECOMMENDATION 5: Agencies should consider whether collaborating with other agencies with interrelated functions and common stakeholders would be beneficial to their risk management processes. For example, there may be an opportunity to perform multi-agency risk assessments or manage risks in partnership.

6.10 A KPMG survey found that the most common method of communicating risk management policies and processes was the annual report. The annual reports of NSW public sector agencies have various levels of risk management reporting. These include:

- Having no information on risk management;
- Reporting on only insurable risks; or

[2] Submission No.12, NSW Rural Fire Service.
[3] Submission No. 21, NSW Fire Brigades, pg 2.
[4] Gillian Calvert, Transcript of hearing 10 June 2005, pg2

- In best cases, identifying major risks, describing risk management policies and procedures, disclosing the activities they have undertaken to manage risks and the outcomes of these processes. [5]

6.11 The Audit Office and IAB Services both support the need for improved reporting on risk management. The following evidence was heard:

> **CHAIR:** What areas have you found need improvement in the public sector?
>
> **Mr O'TOOLE:** ....I think there could be more scope for greater reporting on risk management. I believe it should be enshrined into manager's personal performance agreements about what they are doing in terms of implementing strategies to mitigate risk, ensure that the accountability for management of risk is made clear, to develop a stronger risk awareness culture within the organisation and to involve external providers or external stakeholders in the process rather than just looking within the department because a lot of departments have relationships with a lot of private and other organisations.[6]

6.12 Recommendations for improved annual reporting requirements have been discussed in Chapter Three.

ESTABLISH THE CONTEXT

> ***Key element:*** *Define the basic parameters within which risks must be managed and set the scope for the rest of the risk management process. The context includes both the internal and external environment.*

6.13 Over 65 per cent of GGS and 90 per cent of PTES respondents have examined and documented their strategic, organisational and risk management context. These results are consistent with similar surveys performed by the NSW Auditor-General in 2002 and the Victorian Auditor-General in 2003.

6.14 In most cases, the strategic and organisational context would be integrated into existing corporate governance processes. This is the approach taken by the Department of Education and Training. Under its guidelines, the risk management context is documented on a standard form.[7] The guidelines of other agencies explain what steps are to be undertaken, but do not specify how this process should be documented.

6.15 Evaluating the external environment may require a cultural shift. The Managing Director of the Sydney Catchment Authority provided the following insight:

> **Mr HEAD:** I think it is part of the job of public sector executive teams to be aware of not just what is happening in your own agency but aware of improvement processes that are being implemented across government. So clearly I am involved in a range of collegiate processes with other executives in the public sector. It is part of my job to communicate to the SCA that those initiatives are happening and what we need to do to make sure we are responsible.
>
> What you are trying to achieve there is a culture within the organisation that is not just looking inward but is also looking outward and looking outward for our organisation means looking at what is happening in the catchment, looking at what other water

[5] KPMG, *Strategic Risk Management Survey,* November 2004, pg 7.
[6] Phillip O'Toole, Transcript of Hearing, 10 June 2005, pg 23.
[7] Submission No. 26, Department of Education and Training, pg 9.

> utilities are doing to continuously improve but also looking at whole of government improvement processes....[8]

6.16 The internal environment includes the allocation of roles and responsibilities for the risk management process.

Roles and Responsibilities

6.17 It is clearly legislated in the private sector that the board of directors are ultimately responsible and accountable for managing risks. This is not as clearly defined by NSW public sector legislation, but we can assume it rests with the board of directors or the equivalent head of the agency. Typically, senior executives carry out these responsibilities and mechanisms need to be in place to measure their performance. The key way of ensuring accountability is by having performance agreements that specifically define their responsibilities and include criteria to assess performance. Additionally, there needs to be an effective link between risk management and individual performance appraisals.

6.18 Seventy-six per cent of respondents in the GGS and 70 per cent in the PTES agree that their responsibilities for risk management are documented and communicated. Eighty-eight per cent in GGS and 60 per cent in PTES state that they are well understood. The results for PTES are consistent with other responses such as the provision of training, existence of a risk management policy and extent of internal communication. However, GGS percentages conflict with the following responses:

- Training of managers has only been provided in 47 per cent of agencies;
- Staff training has only been provided in 29 per cent of agencies;
- Only 65 per cent of agencies have a risk management policy; and
- Only 41 per cent have a risk management treatment plan.

6.19 Fifty-three per cent of respondents in GGS and 70 per cent in PTES claimed that performance agreements for executives cover their risk management responsibilities. Ministry of Transport is introducing this requirement in 2005-06. EnergyAustralia was the only agency in either sector to claim that the linkage between risk management and individual performance appraisals was effective.

IDENTIFY RISKS

> ***Key element:*** *Comprehensive identification of risks and events using a well-structured systematic process. The aim is to identify what, where, when, why and how events could prevent, degrade, delay or enhance achievement of the objectives.*

6.20 Sixty-five per cent of respondents in the GGS and 70 per cent in the PTES claimed that they carry out comprehensive and systematic identification of risks relating to each of their objectives. GGS has improved since the 2002 survey, whilst PTES has remained steady. Generally, the agencies that responded in the negative were not considering all risk types and relied on brainstorming, judgement and past experience to identify risks. The majority of respondents in both sectors are involving all staff in the risk identification process through focus sessions and interviews.

[8] Graeme Head, Transcript of Hearing, 10 June 2005, pg 13-14.

6.21 The risk assessment service provided by IAB Services includes the identification of key risks. This has been performed for approximately 30 agencies in the last two years. Other agencies have engaged external consultants to assist with their risk identification process.

6.22 The *Guidelines* that support *AS/NZS 4360:*2004 recommend that a risk register contain a description of the risk, an outline of existing controls, an assessment of consequences and likelihood, a risk rating and the priority. Over 65 per cent of all respondents have a risk register, which is a significant improvement for the GGS. The Committee heard in evidence:

> **Mr O'TOOLE:** …I believe that the risk register which has developed as a result of a risk assessment and then the resultant internal audit plan should be reported on at least twice a year to the audit committee as to the progress of implementing recommendations from it and as I said before, there should be a mandate that the risk register be refreshed every three years and the audit committee should definitely be the organisation responsible for monitoring that implementation.[9]

6.23 Another benefit of having a documented history of risk management was heard in evidence:

> **Mr M TURNER:** …my personal view is that risk management has available to it a whole range of benefits, including knowledge management, which typically is not handled very well across most sectors, including the private sector. The reason I say this is because if you go through a process where you identify what can go wrong and what can assist you to achieve objectives, you assess them and then record even just briefly what actions you undertake to either mitigate those risks where there is an adverse effect, or augment them where you have got an opportunity. In the absence of recording that information, you can repeat the same mistakes or miss capitalising on opportunities.[10]

6.24 The revised standard places a greater emphasis on identifying opportunities and managing potential gains. However, 15 per cent of respondents are only viewing risk as a threat to achieving their organisational objectives and not considering the opportunities for positive outcomes.

ANALYSE RISKS

> ***Key element:*** *Develop an understanding of risk to assist with making decisions on whether the risks need to be treated and the most appropriate and cost-effective treatment strategies.*

6.25 Risk analysis should be consistent with the risk evaluation criteria developed as part of establishing the context. Risk analysis can either be qualitative, semi-quantitative or quantitative depending on the risk, purpose of analysis and the information available. There are various methods used for measurement, various types of consequences and likelihood tables and various ways of presenting results. The Committee was provided with examples of the tools that agencies use to analyse their risks. They are predominately using consequence and likelihood matrices to determine the level of risk and how much management attention is required. These matrices are based on *AS/NZS 4360:2004*, but have been modified by each agency in line with their particular risk evaluation criteria.

[9] Phillip O'Toole, Transcript of Hearing, 10 June 2005, pg 24.
[10] Marcus Turner, Transcript of Hearing, 24 June 2005, pg 34.

6.26 NSW Health uses a standardised assessment tool for clinical risk management, being the NSW Severity Assessment Code risk matrix. Some of the area health services have designed their corporate risk matrix to align with this tool, but others are using a separate matrix for risk management outside the clinical domain.[11]

6.27 29 per cent of respondents in the GGS and 70 per cent in the PTES claim that they effectively analyse risks. The results for both sectors are lower than the 2002 survey. This is expected as the respondents have a better understanding of the requirements under *AS/NZS 4360:2004* and have conservatively rated their agencies as partially effective.

6.28 All respondents claimed to evaluate existing controls as part of the risk analysis process. Internal auditors play a significant role in exercising this function on behalf of the audit committees and/or risk committees. All respondents claimed to be prioritising and selecting the risks that require active management. During this process, 35 per cent of GGS and 60 per cent in PTES respondents use at least semi-quantitative methods of analysis for major risks.

6.29 There is a difference in level of risk analysis that needs to be performed by GGS and PTES agencies for reporting to Treasury. RSPs of budget dependent agencies only require qualitative analysis, but SBI/SCI for public trading enterprises require the potential impact for major risks to be quantified.

6.30 Risk Shield Pty Ltd recommends that all agencies adopt a standard risk matrix for qualitative risk assessment to enable whole-of-government comparisons. They also suggest that all major risks should be assessed using semi-quantitative models.[12] The witnesses had varied opinions on the feasibility of a standard risk matrix. The following evidence was supportive of a standard risk matrix:

> **Mr KEAN:** I have a view that I think, depending on who the Government body is, be it Treasury, be it the Government, be it Parliament, that it is important that that senior body should be able to measure risk across the whole of the State environment, so if they were based on the same matrix they would be able to compare the level of our risks with the level of risks in health, State Rail, what have you, and then be able to make a decision as to where best to place its resources…[13]

> **Mr M TURNER:** I would like to see one for the whole public sector….I do not believe that it needs to be unwieldy. One of the elements that we are trying to deal with in Commerce is a microcosm of what you are talking about. We have a diversity of operations from construction through to industrial relations and through to fair trading and procurement across the State, so the types of activities we are undertaking is something we have sought to address in setting our risk at the time.[14]

6.31 Other witnesses could see the benefits, but argued that it may not be feasible:

> **Mr O'TOOLE:** …It would assist in benchmarking the risks across the sector but I suppose the downside or the difficulty of having a generic risk matrix would be it would be very difficult because a lot of the risks are related to the particular operations of the organisation. So there could be the potential for kindred industries or operations being combined. The entire process of risk assessment is very subjective and what someone

[11] Robert McGregor, Transcript of Hearing, 10 June 2005, pg 27.
[12] Submission No.5, Risk Shield Pty Ltd, pg 1.
[13] Noel Kean, Transcript of Hearing, 10 June 2005, pg 18.
[14] Marcus Turner, Transcript of Hearing, 24 June 2005, pg 30-31.

classifies as extreme or high, moderate or whatever may not necessarily be the same as what another agency would necessarily do...[15]

Mr LUCAS: I don't think that there is a benefit in having a Government wide matrix because the risks and the impact or the consequences of those risks are probably unique to the business. Whether there is some benefit in having a sector area, so a natural resources or a planning type area or whatever, a transport sector, an electricity sector, there may be some merit in that....[16]

Mr SENDT: ....I think specifying there has to be a particular approach and that particular risks would apply across all the public sector. I think it is not the best approach. There may be some risks that are indeed common across most public sector agencies, but to prescribe those either in legislation or in some central agency direction runs the risk that agencies would concentrate perhaps on those and ignore other risks that are more specific to their organisation. My preference would be it should be an agency by agency approach and the agency then takes responsibility for the risks it identifies.[17]

EVALUATE RISKS

Key element: *Compare estimated levels of risk against pre-established criteria and consider the balance between potential benefits and adverse outcomes. This purpose is to prioritise the level of risk and consider the extent of any opportunities that may eventuate.*

6.32 The results of the risk analysis are used to complete this step in the process. The criteria used in the evaluation must be consistent with the objectives of the agency. While not all risks can be treated and not all opportunities can be taken advantage of, decisions need to be about which areas should be given priority by management.

6.33 Eighty-five per cent of respondents believe their criteria for evaluating risks is at least partially effective.

TREAT RISKS

Key element: *Identify and assess the range of options for treating risks including avoiding, preventing, mitigating, transferring or retaining the risk. Develop and implement treatment plans that increase potential benefits and reduce potential costs.*

6.34 The public sector does not always have the option of avoiding the risk by not undertaking the activity. The main risk treatment methods used by the agencies surveyed are to reduce the risk, for example, through increasing controls; or to transfer the risk, for example, by taking out insurance.

6.35 Business continuity plans and disaster recovery plans are strategies that mitigate and/or reduce the potential cost of major risks. Seventy-one per cent of respondents in the GGS and 90 per cent in the PTES have a disaster recovery plan. Sixty-five per cent of GGS and 70 per cent of PTES respondents in have a business continuity plan. Some of the delays are as a result of restructured agencies needing to work through a lot of operational issues before the plans can be finalised, for example, the integration of various information systems.

6.36 Eighty-eight per cent of respondents in the GGS and 90 per cent in the PTES are assessing the costs and benefits of treatment options before selecting the appropriate

[15] Phillip O'Toole, Transcript of Hearing, 10 June 2005, pg 24.
[16] Peter Lucas, DIPNR, Transcript of Hearing, 24 June 2005, pg 3-4.
[17] RJ Sendt, Transcript of Hearing, 24 June 2005, pg 9.

strategy. It is important that the treatment method corresponds with the potential impact of the problem. A simple low-cost solution may be the best option. When treatment options have been selected, they should be documented in a risk treatment plan. Only 41 per cent of respondents in the GGS and 60 per cent in the PTES have prepared and implemented risk treatment plans.

6.37 All respondents in the PTES claim that they have developed and implemented risk management strategies that are at least partially effective. Twelve per cent of respondents in the GGS have do not have appropriate strategies in place. This is a 24 per cent improvement on the 2002 survey results. However, without a documented risk treatment plan it is questionable how these agencies have made this assessment.

MONITOR AND REVIEW

Key element: *Regular monitoring and review is essential to ensure that risk treatment plans remain relevant and performance of the risk management process is measured. This process will also encourage continuous improvement.*

6.38 As reported above, 59 per cent of GGS agencies and 40 per cent of PTES agencies responding to the survey do not have risk management plans. This impairs their ability to effectively monitor and report on performance of the risk management system.

6.39 Thirty-five per cent of respondents in GGS and 50 per cent in PTES claimed that the effectiveness of risk management is regularly captured within routine management reporting. A similar percentage of agencies claimed that key risk performance indicators (KPIs) are routinely used to monitor levels of risk and outcomes of risk treatment measures. Of these agencies, only one assessed both their development of KPIs to measure success of strategies and emerging issues and their monitoring of strategies against KPIs as effective.

6.40 Forty-seven per cent of respondents in GGS and 50 per cent in PTES are monitoring and reviewing the risk management process on a regular basis. In addition, 70 per cent of all respondents claim that their risk management processes are subject to an independent audit on an annual basis. This figure may be overstated due to some agencies confusing a financial audit with a review of risk management processes.

OBSTABLES TO EFFECTIVE RISK MANAGEMENT

6.41 Seventeen per cent of respondents claimed to have no major obstacles to implementing effective risk management. The remaining respondents reported the following obstacles:

- Difficulty in developing a culture that is more supportive of risk management practice as an ongoing responsibility;
- Maintaining a high profile for risk management as a management responsibility;
- Lack of understanding of how risk management can provide opportunities for improvement and positive outcomes;
- Lack of resources;
- No documentation of key risk performance indicators;

- Not having a risk management policy hinders effective risk management;
- Risk management is isolated within asset management and not being developed on an enterprise wide basis;
- Risk management is seen as a static process rather than a management tool;
- Requirement of smaller agencies to have dedicated senior staff to maintain effective risk management;
- Lack of training in risk identification;
- Changes to the size and responsibilities of agencies through amalgamations and/or restructuring have impacted on their planned development and implementation of an effective risk management framework;
- Increased diversity of risks being managed by one agency;
- The geographical spread of staff hinders effective communication and training.
- Shortage of in-house expertise and limited funds to engage experts; and
- The lack of an integrated NSW framework that consolidates various guidelines and standards that are produced by various agencies.

6.42 John Bushell Value Management Pty Limited has recommended the following steps to maximising effectiveness of risk management with limited resources:

- Identify broad risk categories for the agency;
- Target the areas that senior management believe are the most hazardous to the agency and its customers;
- Use existing data wherever possible;
- Understand present risks before identifying risks related to changed circumstances;
- Initially target areas for risk reduction or elimination before developing strategies to manage remaining risks;
- Follow up on the outcomes to ensure benefits have been realised; and
- Look for the most cost effective solution.[18]

6.43 The Commissioner for Children and Young People has found that being a small and relatively new organisation has been an advantage:

> **Ms CALVERT:** …In a way the Commission is lucky in that we are quite a young organisation, so we do not have a whole history and culture that we have to turn around. When we set the organisation up we made a decision to be results focussed and then Treasury brought in this results and services framework, which reinforced what we had chosen to do anyway. The other thing that was fortunate about being a new organisation is that we were dealing with the content. We came out of the risk business, if you like, which was about child protection and we have a child protection function in the Commission. So we are very attuned to the notion of risk and we have to place risk at the centre of the organisation, and we have been able to do that because we are a new organisation. So from the beginning we have had a results focus and we have had an awareness of risk that other organisations maybe do not have.

[18] Submission No.9, John Bushell Value Management Pty Limited, Pg 2-5.

> **Mr McLEAY:** Or would be envious of. Do you find the fact that you are small also assists you to quickly with your outcomes?
>
> **Ms CALVERT:** Yes, I think that is true, we are a small organisation so we are much more flexible and responsive. The other thing about the Commission is that we have a much younger profile of our staff than the public sector generally and there are a lot of people who are new to the public service. That is both, in a sense, positive, because you have got people who think in fresh ways. However, it is also a risk, in that you have got people who do not understand the need for some of the accountability that you have to have in a public sector organisation.[19]

6.44 Larger agencies with a diverse range of services and existing culture will typically take longer to implement an enterprise-wide risk management system. On their own additional resources are not enough to fast track the process because modifying the culture and developing policies and procedures that can be applied to various services takes time.

CONCLUSION

6.45 The results of the surveys show that progress has been made since the Auditor-General's performance audit. However, the following key areas need to be strengthened:

- Communication and consultation needs to be a formal two way process that involves both internal and external stakeholders;
- All agencies should have a risk management policy and treatment plan;
- All agencies should have a business continuity plan and disaster recovery plan;
- Training in risk management needs to be more widespread and develop skills in how to identify and manage opportunities;
- Responsibilities for risk management need to be included in performance agreements and linked to appraisals; and
- The monitoring and review processes need to be enhanced.

[19] Gillian Calvert, Transcript of Hearing, 10 June 2005, pg 5-6.

Appendix 1 - List of Agencies Surveyed

General Government Sector (19)	**Public Trading Enterprise Sector (10)**
Casino Control Authority	Delta Electricity
Commission for Children and Young People	Department of Housing – t/as NSW Land and Housing Corporation
Department of Ageing, Disability and Homecare	EnergyAustralia
Department of Commerce	Hunter Water Corporation
Department of Community Services	Newcastle Port Corporation
Department of Education and Training	New South Wales Lotteries Corporation
Department of Energy, Utilities and Sustainability	Rail Corporation New South Wales
Department of Environment and Conservation	Sydney Catchment Authority
Department of Gaming and Racing	Waste Service NSW
Department of Health	Workcover Authority
Department of Infrastructure, Planning and Natural Resources	
Department of Juvenile Justice	
Department of Lands	
Department of Local Government	
Department of Primary Industries	
Legal Aid Commission of NSW	
Ministry of Transport	
NSW Rural Fire Service	
Roads and Traffic Authority	

Appendix 2 – List of Submissions

1. Recovre Pty Ltd
2. RailCorp
3. WSN Environmental Solutions
4. NSW Casino Control Authority
5. Risk Shield Pty Ltd
6. Hunter Water Corporation
7. NSW Commission for Children and Young People
8. NSW Lotteries Corporation
9. John Bushell Value Management Pty Ltd.
10. NSW Department of Housing
11. Audit Office of NSW
12. NSW Rural Fire Service
13. IAB Services
14. Delta Electricity
15. Department of Gaming and Racing
16. NSW Attorney-General
17. Minister for the Environment
18. Minister for Rural Affairs, Minister for Local Government, Minister for Emergency Services and Minister for Lands
19. EnergyAustralia
20. Newcastle Port Corporation
21. NSW Fire Brigades
22. Minister for Transport
23. Department of Local Government

24. Special Minister for State, Minister for Commerce, Minister for Industrial Relations, Minister for Ageing, Minister for Disability Services and Assistant Treasurer and Vice President of the Executive Council

25. Minister for Energy and Utilities, Minister for Science and Medical Research, Minister Assisting the Minister for Health (Cancer) and Minister Assisting the Premier on the Arts

26. Minister for Education and Training

27. Minister for Primary Industries

28. Minister for Infrastructure & Planning and Minister for Natural Resources

29. Minister for Regional Development, Minister for the Illawarra and Minister for Small Business

30. Roads and Traffic Authority

31. Minister for Juvenile Justice, Minister for Western Sydney and Minister Assisting the Minister for Infrastructure and Planning (Planning Administrator)

32. Minister for Health

33. NSW Treasury

Appendix 3 – List of Witnesses

10 June 2005, Parliament House

Organisation	Representatives
NSW Commission for Children and Young People	**Ms Gillian Calvert,** Commissioner for Children and Young People
Sydney Catchment Authority	**Mr Graeme Head,** Managing Director **Mr Graham Begg,** Manager Business Planning
EnergyAustralia	**Mr Noel Kean,** Chief Internal Auditor **Mr Frank Martin,** Audit Manager
Internal Audit Bureau Services	**Mr Phillip O'Toole,** Director Risk Management & Consulting Services
NSW Health	**Mr Robert McGregor,** Deputy Director General, NSW Health Department **Mr Terry Clout,** Chief Executive, Hunter New England Area Health Service **Dr Margaret Halliday,** Risk Manager, Sydney South West Area Health Service **Dr Michael Smith,** Director Clinical Governance, Sydney West Area Health Service

24 June 2005, Parliament House

Organisation	Representatives
Department of Infrastructure, Planning and Natural Resources	**Mr Damian Furlong,** Acting Executive Director, Corporate Services **Mr Peter Lucas,** Chief Financial Officer
The Audit Office of NSW	**Mr Robert Sendt,** NSW Auditor-General **Mr Anthony Whitfield,** NSW Deputy Auditor-General **Mr Stephen Horne,** Assistant Auditor-General
NSW Treasury	**Mr Mark Ronsisvalle,** Deputy Secretary **Mr Ian Neale,** Executive Director **Mr Mark Pellowe,** Acting Senior Director
Department of Commerce	**Mr Alistair Hunter,** Chief Financial Officer **Mr Marcus Turner,** Manager Corporate Risk Services

Appendix 4 – Copy of Questionnaire

PUBLIC ACCOUNTS COMMITTEE'S INQUIRY INTO RISK MANAGEMENT
QUESTIONNAIRE FOR SELECTED AGENCIES

This inquiry is a follow-up to the *Auditor-General's Performance Audit - Managing Risk in the NSW Public Sector June 2002*. This questionnaire is predominately based upon the requirements of the Australian/New Zealand Standard *AS/NZS 4360:2004, Risk Management (*the *Standard*).

If you have any queries, please contact the Committee secretariat on 9230 2363.

Please complete this survey by 29 April 2005 and fax to the Committee on 9230 3052 or post to:

The Committee Manager
Public Accounts Committee
Parliament of New South Wales
Macquarie St
Sydney NSW 2000

NSW Public Sector Framework

The following have significantly contributed to the development and implementation of risk management within your organisation: [*Circle your response]*	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
• AS/NZS 4360:2004 Risk Management Standard	1	2	3	4	5
• Legislation	1	2	3	4	5
• Policies, directives and guidelines from central agencies	1	2	3	4	5
• Policies, directives and guidelines from non central agencies	1	2	3	4	5
• Internal Audit	1	2	3	4	5
• External Audit	1	2	3	4	5
• Private sector risk management consultants	1	2	3	4	5
• Other [*please specify below*]	1	2	3	4	5

_____

_____

Is your organisation aware of the Risk Management and Internal Control Guidelines and Self-assessment Toolkit, issued by NSW Treasury in September 1997 (NSW Treasury TPP97-3)?	YES	NO
Has your organisation used the Toolkit to improve its risk management processes?	YES	NO
Did Treasury or any other agency provide assistance with implementing the Toolkit?	YES	NO
If your agency used the Toolkit, was an enterprise wide risk management plan developed based on the results of the Toolkit?	YES	NO

Does your organisation have any comments or recommendations about the Toolkit?

_____

_____

Does your organisation's most recent Annual Report include:

• A description of the risks faced by your organisation?	YES	NO
• A description of risk management activities performed by your organisation?	YES	NO
• A risk management declaration by the Board and/or CEO?	YES	NO

What other information does your agency provide on risk management to external organisations?

_____

_____

Performance Audit Findings

Did the Auditor-General's findings in the Performance Audit report influence changes to your risk management policies, procedures and practices? If yes, briefly explain.

_____

_____

The *Standard*

What impact, if any, did the revised risk management standard have on your policies, procedures and practices?

_____

_____

Risk Management Process

Does your organisation have a risk management policy? YES NO
Who approved the policy? _____
When was the policy last reviewed and/or revised? _____
How is the policy communicated throughout the organisation (to both internal and external stakeholders)?

_____

Have your internal and external stakeholders been identified? YES NO
Has a stakeholder analysis been performed? YES NO
Do you have a communication and consultation plan (formal document or checklist)? YES NO

	Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Effective risk management is important to the achievement of your organisation's objectives.	1	2	3	4	5
Our risk management practice is well developed.	1	2	3	4	5
Our policies, procedures, systems and internal controls for risk management are defined and communicated.	1	2	3	4	5
Our organisation has appropriate resources to support risk management policy and practice.	1	2	3	4	5
In applying risk management processes and developing related plans, the following have been examined and documented:					
• strategic context: the relationship with the environment [SWOT analysis],	1	2	3	4	5
• organisational context: capabilities, goals and objectives, and	1	2	3	4	5
• risk management context: scope and boundaries for application of the risk management process.	1	2	3	4	5
Risk management is integrated into the following processes in your organisation:					
• corporate/strategic planning	1	2	3	4	5
• annual planning	1	2	3	4	5

• business unit planning	1	2	3	4	5
• project planning	1	2	3	4	5
• audit planning	1	2	3	4	5
• annual budgeting	1	2	3	4	5
• business unit budgeting	1	2	3	4	5
• management reporting	1	2	3	4	5
• external reporting	1	2	3	4	5
• Board reporting *(NA if no Board)*	1	2	3	4	5
• project reporting	1	2	3	4	5
• performance evaluation	1	2	3	4	5

Does your organisation carry out a comprehensive and systematic identification of its risks relating to each of its objectives? YES NO

Does your organisation consider the following types of risk:

- political YES NO
- opportunity [risk of missing opportunities to improve on delivery of the organisation's objectives] YES NO
- environmental YES NO
- alliance [risk of working with partnering organisations] YES NO
- loss of intellectual property YES NO
- reputation YES NO
- financial YES NO
- project YES NO
- compliance YES NO
- public liability YES NO
- natural hazard YES NO
- technological YES NO
- human YES NO
- security YES NO
- other (please specify below) YES NO

_____

_____

Who is responsible for risk identification? _____

_____

_____

Does your organisation:

- Have a risk register/database? YES NO
- Make use of computer software for risk management? YES NO

What tools and techniques are used by your organisation for identifying risks:

- Audits YES NO
- brainstorming YES NO
- examination of local/overseas experience YES NO
- SWOT YES NO
- interview/focus groups YES NO
- judgement YES NO
- surveys/questionnaires YES NO
- scenario analysis YES NO
- operational modelling YES NO
- past experience YES NO
- process analysis YES NO
- other (please specify below) YES NO

_____

In pursuing its objectives, your organisation views risk as:

• a threat?	YES	NO
• an opportunity?	YES	NO
• other? (*please specify below)*	YES	NO

Who is responsible for analysing and prioritising the risks facing your organisation? _____

_____

Who decides how to address risks? _____

_____

You respond to analysed risks by:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
• evaluating the effectiveness of existing controls,	1	2	3	4	5
• assessing the costs and benefits of addressing risks,	1	2	3	4	5
• prioritising and selecting the risks that need active management,	1	2	3	4	5
• prioritising risk treatment where there are resource constraints.	1	2	3	4	5

To what extent is the organisation's risk assessed by using:	**Never**		**Sometimes**		**Very Often**
• qualitative analysis methods [e.g. high, moderate, low]?	1	2	3	4	5
• quantitative analysis methods?	1	2	3	4	5
To what extent does your organisation use the risk treatment of:					
• accepting / retaining the risk?	1	2	3	4	5
• avoiding the risk e.g. not proceeding with the activity?	1	2	3	4	5
• reducing the risk e.g. internal control?	1	2	3	4	5
• transferring the risk e.g. insurance?	1	2	3	4	5
To what extent is effectiveness of risk management captured within routine management reporting?	1	2	3	4	5
To what extent are key indicators used to routinely monitor the:					
• levels of risk?	1	2	3	4	5
• application of risk treatment measures?	1	2	3	4	5
• effectiveness of risk treatments?	1	2	3	4	5

Does you organisation have an up to date:

• business continuity plan?	YES	NO
• disaster recovery plan?	YES	NO
• risk management plan?	YES	NO
Are risk management processes subject to audit?	YES	NO

Who reviews and monitors:

- risks faced? _____
- application / effectiveness of risk treatments? _____
- opportunities? _____

How often is review and monitoring undertaken? _____

In the last five years the level of risk faced by your organisation has:

Increased / Decreased / Not Changed / Don't Know

How regularly do you review your insurance coverage? _____

Does your organisation have a Risk Management Committee?	YES	NO
If no, does your organisation have an Audit Committee and is the risk management and internal control framework covered in the Charter?	YES	NO
The responsibility for risk management within your organisation is:		
• documented and communicated?	YES	NO
• understood?	YES	NO
Do performance agreements for executives cover their risk management responsibilities?	YES	NO
Have key performance indicators (KPIs) been developed to monitor whether executives are meeting their risk management objectives?	YES	NO
Has risk management training been provided to management?	YES	NO
Has risk management training been provided to staff?	YES	NO

Effective Risk Management

Which of the following components of risk management are effective in your organisation:	**Effective**	**Partially Effective**	**Ineffective**	**NA**	**Not in place**
• Executive sponsorship, support and focus	1	2	3	4	5
• Line management ownership of risk management	1	2	3	4	5
• Effective culture and organisation	1	2	3	4	5
• Defined and communicated policies, procedures, systems and internal controls	1	2	3	4	5
• Linkage between risks and corporate aims and objectives	1	2	3	4	5
• Level of understanding of risk and risk management across the organisation	1	2	3	4	5
• Specification of the organisation's risk environment, including articulation of the organisation's objectives	1	2	3	4	5
• Linkage between risk management and individual performance appraisals	1	2	3	4	5
• Establishment of risk appetite, risk tolerance and risk treatment measures	1	2	3	4	5
• Establishment of criteria to evaluate risks	1	2	3	4	5
• Identification of risks	1	2	3	4	5
• Recording of risks	1	2	3	4	5
• Analysis of risks	1	2	3	4	5
• Prioritising of risks	1	2	3	4	5
• Development and implementation of risk management strategies	1	2	3	4	5
• Resourcing of risk management strategies and processes	1	2	3	4	5
• Development of KPIs to measure success of strategies and emerging issues	1	2	3	4	5
• Monitoring strategies against KPIs	1	2	3	4	5
• Performance benchmarking	1	2	3	4	5
• Continuous review/feedback on risk management strategies and performance	1	2	3	4	5
• Regular reporting to senior management	1	2	3	4	5

Overall, at what stage of risk management practice development does your organisation consider itself to be? (Either best practice, well developed, reasonably well developed, basic or not started)

_____

What are the main obstacles to effective risk management in your organisation?

Please attach any further comments you would like to make, including additional responses to any of the questions.