Australian Government
Comcover

Better Practice Guide

June 2008

Risk Management

COMCOVER

ISBN 1 921182 78 4 print

ISBN 1 921182 79 2 online

Department of Finance and Deregulation

Acknowledgements

Photographs taken by Steve Keough, Steve Keough Photography
Copyright: Department of Finance and Deregulation

Contents

Foreword

Risk management has evolved into a well-recognised management discipline and is now considered a key governance and management tool within the public and private sectors.

Risk management underpins an agency's[1] approach to achieving its objectives. An important responsibility for any government body is the effective and efficient use of Commonwealth resources. This aim can be aided by sound risk management practices. To increase the likelihood of achieving desired outcomes, informed decisions should be made based on evaluation of the associated risks.[2]

The successful achievement of outcomes by agencies can be inhibited by the risks that arise as a result of the environment we operate in. We must be constantly aware of the impact of our operating environment to ensure we identify opportunities that enable the development of policies and programs that meet stakeholders' expectations; demonstrate effective and efficient use of resources; and ensure the timely delivery of high quality services.

The Department of Finance and Deregulation, through the Comcover Fund, is responsible for promoting better practice risk management across the Australian Government sector. The Comcover Fund provides risk management and insurance services to over 160 agencies with a broad range of responsibilities. Fund members include General Government Sector entities governed by the *Financial Management and Accountability Act 1997* (FMA Act) or the *Commonwealth Authorities and Companies Act 1997* (CAC Act) and the High Court of Australia.

The current accountability frameworks created by the *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act 1997* provide chief executives, directors, their management and their staff with the building blocks to effectively manage risk.

Agencies that develop a robust risk management framework will be better placed to ensure the efficient, effective and ethical delivery of their outcomes across a wide range of policy and program areas.

This Guide provides a summary of the key principles and concepts of risk management as well as some practical tips to be considered when implementing or reviewing an agency's framework for managing risk. It also emphasises the importance of developing the right culture for managing risk.

1 In this Guide, the terms "agency" and "agencies" apply to all Australian Government sector entities, regardless of whether they are subject to the FMA Act or the CAC Act.

2 Australian Public Service Commission, *Building Better Governance*, APSC, Canberra, 2007, p.15.

The most effective approaches to managing risk have been developed where the culture of an agency regards the process of managing risk as essential and valuable. Agencies that develop a positive risk culture, supported by suitable frameworks and processes, promote an understanding of accepting appropriate risks as part of their every day decision-making processes.

As the successful management of risk requires a whole-of-government approach, this Guide has been developed to complement other key government publications. Agencies are encouraged to consider this Guide in the context of other better practice guidance material produced by the Department of Finance and Deregulation, Australian National Audit Office, Department of the Prime Minister and Cabinet, Attorney-General's Department, Comcare and the Australian Public Service Commission.

I J Watt
Secretary
Department of Finance and Deregulation
12 June 2008

Structure of the Guide

The Guide is divided into three sections.

Section one – The context for managing risk within the Australian Government

This section provides a summary of the key requirements and obligations relating to the management of risk contained within the Australian Government financial management framework. This includes legislation, policy and other related guidance material for Commonwealth entities.

Section two – The risk management framework – creating a foundation to effectively manage risk

This section contains an overview of the essential elements of effective risk management frameworks including:

- Policy and objectives;
- Accountability and responsibility;
- Integration;
- Review and evaluation; and
- Culture.

Section three – The risk management program – operationalising your risk management framework

This section details the key resources and processes required to implement risk management within agencies including:

- Resourcing;
- Communication and training;
- Risk assessment; and
- Risk profiling and reporting.

Introduction

What is risk management?

Risk is the possibility of an event or activity impacting adversely on an organisation, preventing it from achieving organisational outcomes. **Risk management** comprises the activities and actions taken to ensure that an organisation is conscious of the risks it faces, makes informed decisions in managing these risks, and identifies and harnesses potential opportunities. Managing risk well requires careful consideration of the key concepts of minimising loss, maximising opportunity and preparing for uncertainty.

Adopting a structured approach to managing risk and developing a culture of positive risk management are key considerations when developing an agency's risk management framework.

The benefits of adopting a structured approach to managing risk can include:

- improved accountability;
- improved stakeholder relationships and confidence;
- the development of a learning culture;
- improved financial management and performance;
- better resource allocation;
- improved compliance outcomes; and
- reduction in the potential for litigation.

Risk management can be used to help provide a strategic approach to decision-making, which can assist agencies improve performance and deliver key outcomes more effectively.

Purpose of this Guide

The purpose of this Guide is to provide advice to agencies on the development and implementation of an enterprise wide approach to managing risk.

A number of the concepts in the Guide reflect current legislative requirements and general government policy. Other concepts which are not mandated represent prudent contemporary governance practice and should be considered by agencies in developing and improving their approaches to managing risk.

In developing this Guide, Comcover has incorporated key findings, recommendations and practical examples relating to better practice risk management from:

- Joint Standards Australia / Standards New Zealand Committee, *Australia and New Zealand Standard 4360:2004 on Risk Management,* August 2004.
- International Organization for Standardization, *Draft International Standard, Risk Management – Principles and Guidelines on Implementation, ISO/DIS 31000,* 2008.
- Joint Management Advisory Board / Management Improvement Advisory Committee (MAB/MIAC) Report No.22, *Guidelines for Managing Risk in the Australian Public Service,* MAB/MIAC, Canberra, 1996.
- Australian National Audit Office Audit Report No.3 2003-2004, *Management of Risk and Insurance,* ANAO, Canberra, August 2003.
- Australian National Audit Office Better Practice Guide, *Public Sector Governance, Volume 1, Framework, Processes and Practices,* ANAO, Canberra, July 2003.
- Australian National Audit Office Better Practice Guide 2005, *Public Sector Audit Committees,* ANAO, Canberra, February 2005.
- ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations,* 2nd edition, 2007.
- *Comcover's Benchmarking Risk Management Program,* Comcover, Department of Finance and Deregulation, Canberra, 2001-2007.
- *Comcover's Awards for Excellence in Risk Management,* Comcover, Department of Finance and Deregulation, Canberra, 2003-2007.
- Comcover's *Risk Management Assessment Service,* Comcover, Department of Finance and Deregulation, Canberra, 2006-2008.

To support the concepts discussed in this Guide, Comcover will continue to develop and release a range of better practice guidance material, including case studies and fact sheets, which will provide further practical assistance examples that illustrate and promote good risk management within the public sector. We encourage agencies to continually review the range of guidance material available to help ensure that their risk management arrangements reflect the latest available advice.

Acknowledgements

Comcover would like to thank all organisations that generously contributed to the development of the *Risk Management Better Practice Guide*.

In particular, our thanks go to:

- Australian National Audit Office;
- Australian Maritime Safety Authority;
- National Gallery of Australia;
- Australian Securities and Investment Commission;
- Comcover Advisory Council; and
- Risk Management Institution of Australasia.

We would also like to thank Comcover Fund Member agencies for their dedication to continually improving risk management practices within the Australian Government sector.

Section one The context for managing risk within the Australian Government

one

The context for managing risk within the Australian Government

Chief executives of agencies governed by the *Financial Management and Accountability Act 1997* (FMA Act) and directors of bodies governed by the *Commonwealth Authorities and Companies Act 1997* (CAC Act) are accountable for the performance of their organisations.

This section provides a summary of the key requirements and obligations relating to the management of risk contained within the Australian Government financial management framework legislation and other related guidance material for public sector entities including:

- the *Financial Management and Accountability Act 1997* (FMA Act);
- the *Financial Management and Accountability Regulations 1997* (FMA Regulations);
- the *Financial Management and Accountability Orders 1997* (FMAOs);
- the *Commonwealth Authorities and Companies Act 1997*;
- the *Commonwealth Authorities and Companies Regulations 1997*;
- the *Commonwealth Authorities and Companies (Report of Operations) Orders 2005*;
- Chief Executive's Instructions (CEIs);
- *Commonwealth Procurement Guidelines* (CPGs); and
- other Australian Government policies and guidance material for Commonwealth entities.

In addition, under the *Auditor General Act 1997,* the Auditor-General is responsible for providing the Parliament with an independent assessment of selected areas of public administration, and assurance about public sector financial reporting, administration and accountability.

Risk management and the *Financial Management and Accountability Act 1997*

The main purpose of the FMA Act is to provide a framework for the proper management of public money and public property. The FMA Act seeks to mitigate risks for the Commonwealth by setting out requirements in relation to the collection, custody, recording and spending of public money and the custody and management of public property, as well as setting out the special responsibilities of chief executives and reporting and audit requirements.

In addition to the FMA Act, the financial management framework includes a range of policies which also have the purpose of mitigating risk to the Commonwealth. Two significant policies relate to contingent liabilities and the management of foreign exchange risk.

The *Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort*[3] seek to manage the risks surrounding contingent liabilities by providing guidance on entering these types of arrangements. It also reinforces the importance of sound risk management strategies and awareness regarding the use of such instruments.

The *Australian Government Foreign Exchange Risk Management Guidelines*[4] reduce the risk to the Commonwealth from foreign exchange movements and set out the government's overarching principle of prohibiting hedging.

Risk is further mitigated by reporting and audit requirements and a key component of this is the Certificate of Compliance process which seeks to ensure that agencies are complying with the framework. The certificate itself is prepared in the context of agencies' internal risk management processes, including internal reporting, internal audit and the operations of internal audit committees.

In addition to a chief executive's direct responsibilities under the FMA Act, all officials have an obligation to comply with the financial management framework in performing their duties. The financial management framework is therefore an important risk management tool in itself, as it regulates all officials' actions. However, to ensure compliance with the framework, internal risk controls also need to be established.

3 Department of Finance and Deregulation, *Finance Circular 2003/02: Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort*, Department of Finance and Deregulation, Canberra, 2003.

4 Department of Finance and Deregulation, *Finance Circular 2006/06: Australian Government Foreign Exchange Risk Management Guidelines*, Department of Finance and Deregulation, Canberra, 2006.

Sound risk management underpins the financial management framework and should inform any financial decision taken by chief executives and agency officials. An agency's risk management practices will be central to its activities, including but not limited to:

- determining policy direction and actions;
- considering spending proposals;
- considering issuing of an indemnity or entering into any other contingent liability as part of an agreement, arrangement or contract;
- meeting requirements under insurance policies;
- determining a suitable business continuity plan;
- issuing appropriate delegations and authorisations to officials; and
- ensuring correct payments are made to individuals or service providers.

Furthermore, some areas of the financial management framework explicitly refer to the agency's risk management arrangements, or anticipate the application of risk management within the agency. For example:

- **Part 7 of the FMA Act** places special responsibilities upon chief executives to manage their agency's affairs in a way that promotes the proper use of Commonwealth resources. In discharging this responsibility, chief executives need to consider the role of sound risk management practices as a means of promoting the efficient, effective and ethical use of Commonwealth resources.

- **Section 44 of the FMA Act** requires chief executives to manage the affairs of the agency in a way that promotes the proper use of Commonwealth resources. Proper use is defined as meaning efficient, effective and ethical use.

  An inherent function of this responsibility involves entering into contracts, arrangements and agreements binding the Commonwealth. Before a chief executive or their delegate can enter into a contract, the FMA Regulations, in particular FMA Regulations 9–13, must be complied with.

- **FMA Regulation 13** provides, in part, that a person must not enter into a contract, arrangement or agreement unless the corresponding spending proposal has been approved under FMA Regulation 9 and, if necessary, authorised in accordance with FMA Regulation 10.

- **FMA Regulation 9** provides approvers, as defined in FMA Regulation 3, with the function of approving spending proposals only where they are satisfied that the proposed expenditure will make efficient and effective use of the public money, and where it is in accordance with the policies of the Commonwealth, including procurement policy as outlined in FMA Regulation 8.

- **FMA Regulation 10** provides the Minister for Finance and Deregulation with the function of authorising the relevant approver to consider approving spending proposals which are not supported by sufficient uncommitted appropriation. This assists the government in managing the extent to which agencies enter into commitments to spend public money that has not yet been appropriated to them. FMA Regulation 10 has been delegated to chief executives in particular circumstances. The *Financial Management and Accountability (Finance Minister to Chief Executives) Delegation 2007 (No.2)* (the delegation) explains where a chief executive may exercise their delegation under FMA Regulation 10 and authorise officials to consider approving spending proposals. *Finance Circular 2007/01 – Regulation 10* provides details regarding the process for gaining FMA Regulation 10 authorisation.

- **Under section 45 of the FMA Act**, chief executives must implement a fraud control plan for their agency. As the management of fraud is an aspect of the overall management of risk within an agency, fraud control plans should not be considered in isolation from an agency's risk management plan and practices. FMA Regulation 20 requires officials to have regard to the Fraud Control Guidelines issued under FMA Regulation 19. FMAO 2.2 requires chief executives to provide a report on fraud control for their agency to the responsible minister at least every two years. The Fraud Control Guidelines specify that agencies are to conduct fraud risk assessments at least every two years and when an agency has undergone substantial change in structure or function.

- **Section 46 of the FMA Act** requires chief executives to establish and maintain an audit committee for the agency. The audit committee, whose minimum functions and responsibilities are outlined in FMAO 2.1, plays an integral role in assisting agencies to manage risk effectively.

- **FMA Regulation 6** authorises chief executives to issue instructions to their agencies on any matter necessary or convenient for carrying out or giving effect to the FMA Act or Regulations. Chief Executive's Instructions should be utilised to develop and promote sound risk management practices and internal control procedures. Officials should refer to *Finance Circular 2004/15 Chief Executive's Instructions*, which state that agencies should consider, amongst other things, outlining the roles and responsibilities of the chief executive, senior management and the audit committee, as well as the circumstances under which risk assessments should be undertaken.

- **Compliance reporting** – FMA Act agencies are required to report annually on the financial management and sustainability of their agency to their portfolio minister, with a copy provided to the Minister for Finance and Deregulation. The Certificate of Compliance provides a comprehensive overview of the agency's compliance with the Australian Government's financial management framework including adopting appropriate management strategies for all current known risks that may affect the financial sustainability of the agency.[5] A balanced risk-based approach to the compliance monitoring process is required to ensure that the chief executive is reasonably confident that all significant instances of non-compliance with the framework have been disclosed.

- **Sections 63 (2) and 70 (2) of the *Public Service Act 1999*** require the secretary of a department or the head of an executive agency to report to the responsible minister, for presentation to Parliament, on the department's activities during the year. This report must be prepared in accordance with guidelines approved on behalf of Parliament by the Joint Committee of Public Accounts and Audit. The annual report for FMA agencies and executive agencies must include a summary of the structures and processes that are in place to implement the principles and objectives of corporate governance. This is to include internal audit arrangements including the approach adopted to identify areas of significant operational or financial risk, and the arrangements in place to manage those risks.[6]

5 Department of Finance and Deregulation, *Finance Circular 2008/04: Certificate of Compliance – FMA Act agencies*, Department of Finance and Deregulation, Canberra, 2008.

6 Clause 12 of the *Requirements for Annual Reports for Departments, Executive Agencies and FMA Act bodies*, Department of the Prime Minister and Cabinet, Canberra, 2007.

Risk management and the *Commonwealth Authorities and Companies Act 1997*

The CAC Act specifies a number of financial, governance and accountability obligations of both Commonwealth authorities and Commonwealth companies. For Commonwealth authorities, it contains detailed financial reporting rules and deals with matters such as banking, investment and the conduct of officers. For Commonwealth companies, the CAC Act contains reporting and other governance requirements in addition to those in the Corporations Act 2001 (Corporations Act). Note that the Corporations Act does not apply to Commonwealth authorities under the CAC Act.

The governance arrangements and requirements for Commonwealth authorities will be determined by their legislative framework. At a minimum, this includes their enabling legislation and the CAC Act. Other legislation, in addition to the enabling legislation of the authority and the CAC Act, may impose additional obligations on the authority, which may have a bearing on its risk management framework.

Officers (including directors) of Commonwealth authorities are required to exercise their powers and discharge their duties with care and diligence, in good faith, in the best interests of the authority and for a proper purpose. Directors of companies are subject to equivalent requirements under the Corporations Act. In meeting these obligations, it is expected that the operations of the entity and the actions of its officers will be based on sound risk management.

There are several additional areas where the CAC Act and its subordinate legislation require CAC Act entities to address risk management.

Compliance reporting – Commonwealth authorities and Commonwealth companies in the General Government Sector are required to report on an annual basis to their responsible minister and the Minister for Finance and Deregulation, on their legislative compliance and financial sustainability. CAC Act bodies need to have implemented sufficient controls to monitor legislative compliance and financial performance and in doing so, be able to manage the risks associated with these issues. [7]

Commonwealth authorities

- **Section 17 of the CAC Act** requires a Commonwealth authority that is either a government business enterprise (GBE) or a statutory marketing authority to prepare a corporate plan. The corporate plan must include an analysis of factors that are likely to create significant financial risk for the authority or the Commonwealth.

- **Section 9 of the CAC Act** provides that the directors of a Commonwealth authority must prepare an annual report in accordance with Schedule 1 for each financial year. Clause 1 of Schedule 1 of the CAC Act provides that the annual report must include a report of operations, prepared by the directors in accordance with the Finance Minister's Orders.

- **Paragraph 10 (1)(b) of the *Commonwealth Authorities and Companies (Report of Operations) Orders*** requires the directors of a Commonwealth authority to include information in its annual report on operations on factors, events or trends influencing the authority's performance over the financial year and in the future, and on the risks and opportunities faced by the authority and the strategies it has adopted to manage these risks and opportunities.

- **Subsection 32(1) of the CAC Act** requires the directors of a Commonwealth authority to establish and maintain an audit committee. Functions should include, but are not limited to, helping the authority and its directors to comply with their obligations under the CAC Act; and providing a forum for communication between the directors, the senior managers and the auditors of the authority.

7 Department of Finance and Deregulation, *Finance Circular 2006/11: Compliance Reporting – CAC Act bodies*, Department of Finance and Deregulation, Canberra, 2006.

Wholly-owned Commonwealth companies

- **Section 42 of the CAC Act** requires a wholly-owned Commonwealth company that is a GBE to prepare a corporate plan. The corporate plan must include an analysis of factors that are likely to create significant financial risk for the company or the Commonwealth.

- **Subsection 44(1) of the CAC Act** requires the directors of a wholly-owned Commonwealth company to establish and maintain an audit committee. Functions should include, but are not limited to, helping the company and its directors to comply with their obligations under the CAC Act and the Corporations Act; and providing a forum for communication between the directors, the senior managers and the auditors of the company.

Further guidance from the Australian National Audit Office (ANAO) in relation to the management of risk within Australian Government agencies which agencies should also consider in implementing an appropriate risk management framework, is listed in the Reference section at the end of this Guide.

Section two The risk management framework – creating a foundation to effectively manage risk

The risk management framework – creating a foundation to effectively manage risk

To achieve an effective approach to managing risk, risk needs to be regarded as important to an agency's strategic planning, management and decision-making process. It is also important to consider an agency's operating environment and, with careful planning, how to integrate risk management with the agency's overarching governance arrangements.

Through the development and implementation of a risk management framework, an agency will be well-placed to achieve the objectives of its risk management policy and ensure risk management is consistently practiced across the agency.

There are five key elements which underpin an effective framework for managing risk within an agency.

1. Risk management policy and objectives

An agency's risk management policy defines the relationship between the agency's risk management philosophy, its risk appetite, accountabilities for managing risk, and the resources and processes dedicated to the management of risk. It should ideally include a set of objectives that guide and shape risk management activities, and outline how performance against these objectives will be measured.

2. Accountability and responsibility

Accountability for managing risk needs to be reflected in an agency's organisational chart and clearly defined in the role, charter and responsibilities of the agency's board and senior executive management team.

3. Integration

Integrating risk management into the governance, planning and management processes within an agency will provide purpose in applying the risk management process and relate risk back to the agency's core business. Specialist risks such as occupational health and safety, business continuity and security often have their own legislation, standards, system requirements and processes. Integrating specialist risk programs into the agency's overarching risk management framework supports more efficient use of resources and helps provide greater assurance that these risks are being appropriately managed.

4. Review and evaluation

Review and evaluation of both the risk management framework and the application of risk management practice needs to be scheduled at regular intervals. It is important for an agency to assess the level of compliance with its risk management framework, as well as measure the effectiveness and quality of risk practice within the agency.

5. Positive risk culture

An agency's commitment to managing risk is demonstrated by senior executives and reflected in the organisation's culture and processes. A positive risk culture reflects an emphasis on the benefits of risk management to achieving agency objectives.

THE FOLLOWING CHECKLIST PROVIDES KEY POINTS TO CONSIDER WHEN DEVELOPING A FRAMEWORK TO EFFECTIVELY MANAGE RISK

- ☑ How is the chief executive's or board's view of risk management determined and communicated across the agency?
- ☑ How does the agency ensure that the risks to be tolerated are acceptable and appropriate?
- ☑ How well is risk management integrated into the agency's strategic and business plans?
- ☑ How well does the agency's accountability framework map to the risks that are being managed and how is the responsibility for managing risk allocated across the agency?
- ☑ What strategy is in place for the agency to communicate risk both externally and internally?
- ☑ How are external changes and events, and their effects, monitored?
- ☑ Have sufficient resources been allocated to risk management?
- ☑ What training is provided to individuals within the agency to understand and manage risk at both the strategic and operational levels?
- ☑ How does the agency take advantage of its experiences in dealing with risks, crises, problems and successes?
- ☑ How does the chief executive or board monitor the agency's risk management practices and review their own performance and obligations?

Policy and objectives – Why is this element important?

An agency's risk management policy defines the relationship between the agency's risk management philosophy, process and procedures. Developing and communicating an agency's risk policy is an important step in ensuring that risk is managed effectively at all levels of an agency.

Key elements of an agency's risk management policy are:

- the objective and rationale for managing risk in the agency;
- clear links between the policy and the agency's strategic plans and business plan;
- an outline of the accountabilities for managing risk;
- guidance on the agency's risk tolerance or appetite for risk;
- details of the support and expertise available to help staff undertake effective risk management practices;
- a statement on how risk management performance will be measured and reported; and
- a commitment to the periodic review of the agency's risk management framework.

An agency's risk management policy can also provide guidance to staff on the agency's commitment to:

- integrating risk management principles into existing procedures and practices;
- communicating the agency's approach to managing risk;
- coordinating the interface between risk management, compliance and assurance programs within the agency;
- incorporating risk management training into internal staff development programs; and
- ensuring that internal review and evaluation programs consider risk management when developing annual audit plans.

POLICY AND OBJECTIVES – PRACTICAL TIPS

- ✓ Ensure the agency's risk management policy reflects linkages to organisational objectives, and provides clear direction to staff on where to seek support and expertise in identifying, evaluating and managing risk.
- ✓ Summarise the agency's risk management policy into a risk statement. Obtain senior executive endorsement and circulate the risk statement within the agency via the Intranet or as a staff publication.
- ✓ Ensure the risk appetite of the agency is documented, communicated and reviewed regularly.
- ✓ Develop risk tolerance guidelines and limits (including quantifiable limits where practicable) that support the agency's risk policy and appetite and are easily understood by all staff.
- ✓ Undertake periodic reviews of your agency's risk appetite in conjunction with its strategic planning process.[8]
- ✓ When publishing your agency's risk management policy on the Intranet, provide a link to procedures that provide advice to staff on how to identify, evaluate and prioritise risk considering the agency's risk tolerance or appetite for risk.
- ✓ Create a map of key documents of your risk management framework to make it easy to differentiate between policy/guidance and process documents. Avoid confusing risk policy documentation with procedural practices by adopting a structured hierarchy to policy development.

8 KPMG, *Risk management beyond compliance: A reflection on current issues and future directions from Australia's top chief risk officers*, KPMG Australia, November 2006, p.12.

ACCOUNTABILITY AND RESPONSIBILITY

Accountability and responsibility – Why is this element important?

Ultimate accountability and responsibility for an agency's performance lies with the chief executive or its directors. This includes accountability for an agency's overall management of risk.

While senior managers and executive are ultimately accountable for risk management, it is the responsibility of all managers and staff to manage risk. Roles and responsibilities for those charged with implementing the risk management function also need to be clearly articulated.

The successful integration of risk management with an agency's overarching governance, financial, assurance and compliance frameworks, is reliant on ensuring that the accountability and responsibility for risk management is clearly defined.

Accountability for risk management requires:

- governance arrangements for bodies, such as boards, executive committees and audit committees, to consider the risks facing an agency in its ongoing operations;
- promotion of active participation in risk management by all staff;[9] and
- senior management to support the establishment of appropriate processes and practices to manage all risks associated with an agency's operations.

Responsibility for managing specific policy, project and program risks generally rests with individual line managers across the agency.

Responsibility for the implementation of the agency's risk management framework rests with the risk manager or risk management team who have been appointed to sponsor or provide guidance to others on effectively managing risk.

9 Australian National Audit Office Better Practice Guide, *Public Sector Governance Vol 1, Framework, Processes and Practices,* ANAO, Canberra, July 2003, p.19.

The table below identifies suggested accountabilities and responsibilities for managing risk in an agency.

GROUP	ROLE IN RISK MANAGEMENT
CHIEF EXECUTIVE BOARD OF DIRECTORS	• Champion the agency's governance and risk management frameworks. • Determine the agency's risk appetite. • Accept the agency's strategic risk profile. • Confirm that the agency's risk management framework is continually maturing to reflect the changing environment. • Review recommendations from the agency's audit and risk committee(s) and determine future actions. • Ensure the risk management framework is implemented and adopted. • Endorse the current planning approach to managing significant and critical risk areas. • Set objectives and goals for the risk management program. • Report on the agency's key business and financial risks to the responsible minister.
SENIOR MANAGEMENT GROUP	• Develop the agency's strategic risk profile. • Review agency-wide and business unit risk profiles. • Review and assess the current and planned approach to managing significant and critical risk areas. • Review and monitor completion of risk profiles and action plans. • Ensure the risk management framework is implemented in individual business units.
AUDIT AND RISK COMMITTEES	• Oversee the risk management framework. • Review and approve risk profiles and action plans (collectively and for all business units). • Monitor the implementation of the risk management program against the endorsed implementation strategy or plan. *Depending on the structure of the agency, these activities may be undertaken at the board or executive level.*
MANAGERS AND SUPERVISORS	• Monitor the risks and risk profiles for their areas of responsibility. • Ensure staff are adopting the agency's risk management framework as developed and intended.
RISK MANAGER	• Coordinate the implementation of the risk management framework, risk profiles and action plans. • Evaluate risk management planning to ensure consistency and accuracy of practice. • Facilitate, challenge and drive risk management development within the agency. • Report to the senior management group, executive management team and audit committee or board at regular intervals.
INDIVIDUAL STAFF	• Recognise, communicate and respond to expected, emerging or changing risks. • Contribute to the process of developing risk profiles for their business unit or branch. • Implement risk plans within their area of responsibility.

Audit Committees

The role of an audit committee in the overall accountability structure for risk management is important. In situations where an audit committee's role includes risk management, its charter may reflect its responsibilities to:

- oversee an agency's internal control structures to ensure that all key controls are appropriate for achieving corporate goals and objectives and are operating effectively;
- review compliance with an agency's risk management policy and programs;
- provide advice to the chief executive and board to help them meet their external accountability obligations, including statutory and fiduciary duties; and
- oversee internal and external audit activities including the implementation of audit recommendations.

It is prudent to consider the benefits of including independent audit committee membership. Greater independence can help strengthen an audit committee's ability to seek explanations and information, and the objectivity of its understanding of the various accountability relationships, particularly on financial performance, risk and controls.[10]

Audit committees may also establish separate sub-committees to manage specific risk categories including:

- financial and business risks;
- business continuity plans, including the testing of disaster recovery plans;
- occupational health and safety plans;
- fraud control plans; and
- environmental and security plans.

10 Australian National Audit Office Better Practice Guide, *Public sector audit committees*, ANAO, Canberra, February 2005, p.5.

ACCOUNTABILITY AND RESPONSIBILITY – PRACTICAL TIPS

- ✓ The agency's risk management policy should clearly separate the lines of accountability for overall risk management outcomes and responsibility for implementing the risk management framework and processes.
- ✓ Accountability and responsibility for managing risk can be reflected in an agency's organisational chart and in individual duty statements and performance agreements.
- ✓ Ensure that the charter of the senior executive management team and the board clearly articulates their responsibilities for overseeing the agency's key strategic risks and their related treatment strategies.
- ✓ To demonstrate accountability and responsibility of the agency's risk management practices, have the chief executive or board endorse the agency's key risk management policies and procedures.[11]
- ✓ Ensure that senior management understand the key strategic risks of the agency and who has responsibility for managing them. Also ensure that middle managers and line managers understand their business risks and their responsibilities for managing these.[12]
- ✓ Recognise risk management as a key skill and responsibility of all staff. Incorporate it into duty statements, performance agreements and discuss it as part of annual performance reviews.

11 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003, p.28.

12 KPMG, *Risk management beyond compliance: A reflection on current issues and future directions from Australia's top chief risk officers*, KPMG Australia, November 2006, p.18.

Integration – Why is this element important?

Public sector governance aims to ensure that an agency achieves its overall outcomes in such a way as to enhance confidence in the agency, its decisions and its actions.[13] Risk management is a key element of effective governance and the framework for managing risk should ideally align and integrate with an agency's overarching governance framework.

Agencies with mature risk management frameworks recognise the value of integrating risk management activities into operational frameworks and processes.

The benefits of integration can include:

- more robust strategic planning;
- improved resource allocation and use;
- greater coordination across different areas of the agency;
- enhanced communication;
- improved management reporting; and
- reduced financial and operational volatility.

When integrating risk management, it is important to consider an agency's operating environment and, through deliberate planning, how risk management processes can be embedded into management activities such as business planning, decision making and reporting.

Successful integration helps ensure the efficient use of resources by reducing the likelihood of duplication of processes and individual risk treatments. Another key benefit of integration is that it helps ensure that the risk management process itself is appropriately resourced and remains relevant and effective.

Specialist risk categories

It is also important to examine the relationship between an agency's risk management framework and specialist risk categories. An agency can be exposed to further risk when these key areas are not considered as part of the overarching risk management program.

Some common specialist risk categories that may have their own programs and processes within an agency include:

- financial;
- business continuity planning and disaster recovery;
- fraud;
- occupational health and safety;
- purchasing and procurement; and
- security.

13 Australian National Audit Office Better Practice Guide, *Public Sector Governance, Volume 1, Framework, Processes and Practices*, ANAO, Canberra, July 2003, p.6.

Many specialist risk areas have their own legislation, standards and compliance requirements. Depending on the scope and depth of these requirements, a dedicated risk management program may be either required or desirable. Whilst implementing a dedicated program provides assurance that specialist risks are appropriately managed, it is important to examine the relationship between these areas and an agency's overarching risk management framework to ensure consistency in the approach to risk management process and practice.

INTEGRATION – PRACTICAL TIPS

- ✓ Risk management cannot be practiced in isolation. Ensure an agency's risk management framework and programs contribute to existing business planning, budgeting and reporting processes.
- ✓ Ensure the agency's risk management framework considers all risks of the agency including strategic, financial, reputation, operational and compliance, as well as cross-references specialist risk areas such as fraud control, business continuity and occupational health and safety risk management processes and reporting.
- ✓ Use the agency's chief executive instructions to articulate and document the links between the risk management framework and other strategic frameworks and processes.[14]
- ✓ Reflect the agency's risk appetite in the internal control framework through financial delegations, procurement delegations, human resource delegations and other key management processes including the determination of insurance arrangements.
- ✓ Update risk management frameworks in a timely manner to reflect restructures, changes of key personnel, or changes in external requirements.[15]
- ✓ Where a specialist risk program is implemented, incorporate review and reporting on this risk category into the agency's overall risk reporting framework.
- ✓ Include easy-to-use risk management tools and templates into strategic and business planning documentation and processes.
- ✓ Check that key risk issues for the agency are communicated to internal and external stakeholders through existing communication channels as part of established communication practice.

14 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003, p.27.

15 ibid.

Review and evaluation – Why is this element important?

Effective and mature risk management frameworks incorporate regular review and evaluation mechanisms, both formal and informal. This helps to determine whether the agency's approach to risk management is consistent with its organisational objectives, ensures that frameworks and programs are continuously improved, and that good risk management practice is recognised and rewarded.

Regular review and evaluation of an agency's risk management framework and program provides critical information to senior management on the effectiveness of the agency's approach to risk management. This reporting considers the alignment of the agency's risk management policy with organisational objectives, ensures that the agency's risk context is clearly established, its risk appetite is understood, and that the responsibilities for managing risk are clear and consistent with strategic directions.

When undertaking review and evaluation, it is important to assess both the risk management program's performance and the effectiveness of the management and treatment of risk. Performance indicators should:

- be easily measurable;
- measure both processes and outcomes;
- be presented in a format that is easily understood by key stakeholders; and
- contribute to improvement and learning within the agency.

Ongoing review and evaluation of an agency's risk management framework, program and practice occurs at three levels:

First level – review of risk information

The identification and assessment of risks can vary across an agency because some people are risk takers while others are risk averse. It is important that there is a process of moderation so that an agency-wide perspective on risk can be agreed. This will also help ensure that risk treatments are reviewed for their effectiveness and to ensure consistency. The focus of this review is an agency's risk register.

Relevant issues for consideration include:

- the degree of accuracy and completeness of the risk register;
- whether the risk register contains statements that clearly articulate specific risks and their treatments;
- whether the consequence and impact levels of individual risks are still relevant; and
- the effectiveness of current treatments.

If this review identifies changes in the nature of previously identified risks, including their treatments or controls, these changes can be reflected by updating the risk register and plans.

Second level – line management review

It is important that those responsible for implementing a specific policy, program or project, review their risk profiles to help ensure that no new risks have emerged and that treatment strategies are still appropriate and effective. It is important that regular reviews are scheduled and consideration is given to how they are undertaken. It may be appropriate to review a sample of risks across a business unit's range of activities. Where issues are identified, it is important to determine if they are associated with a particular risk or whether they are systemic in the risk management process. In either case, it is important to address the issue more thoroughly and to document any findings and corrective action.

Third level – third party audit

Auditing provides independent assurance to senior management that a comprehensive risk management framework is in place that identifies and manages the key risks of the agency. An audit helps identify where an agency's framework lacks alignment with its organisational objectives, provides opportunities for improvement in processes, and allows significant issues to be raised.

Audit findings generally identify systemic issues, so it is important to ensure corrective action is taken to provide sustainable solutions. Audits should also evaluate the appropriateness of existing controls. This will help ensure consistency across the agency and identify potential opportunities to effectively manage similar risks, or categories of risk, from an agency-wide perspective.

REVIEW AND EVALUATION – PRACTICAL TIPS

- ✓ Develop monitoring and review approaches to assess both performance of and compliance with the risk management framework.[16] Guard against audit approaches that only assess compliance rather than the quality of the risk program.
- ✓ Ensure there is a formal review of the agency's risk management framework and practice at least annually.[15]
- ✓ Ensure performance measures assess the effectiveness of treatments and controls and are sufficiently detailed, but not overwhelming, for the relevant audience.
- ✓ Integrate oversight of risk management with other governing bodies or committees, such as senior management committee, executive board or finance committee.
- ✓ Benchmark your agency's risk management performance against your peers.

16 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003, p.27.

Positive risk culture – Why is this element important?

One of the objectives of establishing a risk management framework is to support the development of an organisational culture where risk is appropriately identified, assessed, communicated and managed.

Risk is inherent in everything we do. By adopting a consistent approach to how risk is managed and communicated, a culture of sensible risk taking will emerge.

The individual elements that contribute to developing a positive risk culture are:

- **leadership**, which is articulated in a well considered policy modelled by all senior managers;
- **communicating** the benefits of risk management, and recognising and rewarding those who excel in managing risk in their day-to-day responsibilities; and
- **integrating** risk management with other organisational processes and systems so that the task of managing risk is not regarded as an additional responsibility or burden.

Developing a culture that ensures risk management is considered integral to an agency's strategic and operating environment is often challenging. A positive risk culture is one where understanding, managing and accepting appropriate risk is part of an agency's every day decision-making processes. This is in contrast to a negative risk culture where people are risk averse, ignorant of risk or overconfident with risk taking.

When an agency adopts a framework for managing risk, it helps create an environment that influences behaviour, and eventually shapes internal attitudes towards risk. In simple terms, it's about ensuring that its leadership, organisational structure, processes and systems are all sending the right signals in a consistent manner to the people doing the work to deliver agency outcomes.

It can take an agency three to five years to reach the point where a positive risk culture is visible. A positive risk culture can be attributed to the proactive implementation of a risk management framework.

POSITIVE RISK CULTURE – PRACTICAL TIPS

- ✓ Ensure that executive commitment to the benefits of risk management is communicated to all stakeholders.
- ✓ Encourage senior managers and line managers to demonstrate awareness of risk management when undertaking their day-to-day responsibilities, including by speaking with staff regularly about opportunities for managing risk well.
- ✓ Appoint a senior executive sponsor to lead and promote risk management within the agency and include responsibilities for this in their performance agreement.[17]
- ✓ Identify and lobby key people who can influence the culture (through their visibility and behaviour) and process change (through their positional authority).
- ✓ Reward and recognise those that manage risk well, both publicly and through the agency's performance assessment processes. Positive reinforcement of successful risk management approaches and outcomes will assist in maintaining momentum and mitigate against staff ambivalence towards the risk management program.
- ✓ Build measures of culture and attitude toward risk into staff surveys as part of overall risk management performance measurement.
- ✓ Promoting a positive risk culture does not necessarily require a change in current risk management practices. It requires all staff to value the benefit of risk management in their day-to-day responsibilities.[18]
- ✓ Don't recreate the wheel. It is more important to build a culture where everyone is committed to risk management rather than develop new policies and procedures.

17 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003, p.28.

18 KPMG, *Risk management beyond compliance: A reflection on current issues and future directions from Australia's top chief risk officers*, KPMG Australia, November 2006, p.13.

Section three The risk management program – operationalising your risk management framework

The risk management program – operationalising your risk management framework

An agency's risk management program underpins its risk management framework. It comprises both resources and processes that operate to manage risk exposure in accordance with the parameters reflected in the risk management policy of the agency.

The successful development and implementation of an agency's risk management program requires careful consideration of the following four elements:

1. Resourcing

To ensure the successful management of risk, sufficient resources need to be allocated to both the implementation of the agency's risk management framework and program, and to implement risk treatment strategies.

2. Communication and training

To develop skills and capability in risk management, agencies need to build a level of risk management awareness and knowledge through internal communication and training.

3. Risk assessment

Risk assessment is the process of applying risk management to the specific risks faced by an agency. Risk assessment supports the profiling and reporting of risk through a combination of processes, tools and templates used to establish the context, identify, analyse and treat specific risks.

4. Risk profiling and reporting

This element of the risk management program focuses on the preparation and presentation of risk information via profiles and reports. A risk profile is a high-level synopsis or picture of an agency's risk information developed in consultation with senior management. Risk profiles and risk reports provide information for stakeholders on the prioritisation of key risks and the significance of the risk treatment strategies that require implementation.

Resourcing – Why is this element important?

The successful implementation of a risk management program requires the allocation of both financial and human resources.

Agencies need to identify an appropriate level of resourcing that not only considers the implementation of its risk management program but also ensures sufficient resources are committed to the effective treatment of risk.

The cost of treating risk is not often considered in business planning or the initial stages of risk assessment. Failure to understand the impact of the potential cost of treating risks may lead to increased pressure on project or departmental budgets, failure to deliver key programs or services, and possible damage to an agency's reputation or credibility with key stakeholders.

It is also important to identify personnel to implement the agency's risk management program and to manage it on an ongoing basis. Agencies that demonstrate good risk management practices are those that have identified an individual or team to oversee the implementation and facilitation of the risk management program.

The role of the risk manager, or the risk management team, is to support senior executives by coordinating and providing clear and concise risk information that can be used in planning and decision-making. The risk manager, or risk management team, is also responsible for helping business units across the agency identify and evaluate risk to ensure a consistent approach is applied to the management of risk.

Risk managers require a well-developed understanding of the agency and its operations. This helps to identify opportunities to integrate risk management into existing practices, which in turn, can enhance efficiency and agency performance.

Key responsibilities of an agency's risk manager, or risk management team, include:

- ensuring there are easily accessible systems and processes in place to enable all staff to conveniently undertake risk management in their day-to-day work;
- ensuring risk management processes are applied consistently across the agency;
- developing and implementing an appropriate risk communication strategy;
- identifying the needs for skills development and specific training in risk management across the agency; and
- developing and maintaining a risk reporting framework to enable regular reporting of key risks, and the management of those risks, to senior management.

In implementing a risk management program, the allocation of resources is essential to support strategies such as training and communication. In some cases, there may also be a need for funding to develop new systems and processes to identify, analyse and treat a range of risks across the agency.

RESOURCING – PRACTICAL TIPS

- ✓ Build resource allocation for risk treatment strategies into business planning and budgeting processes. Check what proportion of an agency's budget is allocated to risk treatment strategies.
- ✓ Track risk management costs to assist in the development of future budgets for risk management activities.[19] Capture both direct and indirect costs in resource tracking and budgets.[20]
- ✓ Allocate a component of an agency's budget to ensure the agency's risk management program can be implemented effectively and the risk management function is adequately resourced.
- ✓ Regularly review the adequacy of risk management resourcing levels, including administrative support for reporting, recordkeeping and database maintenance.
- ✓ Establish the risk manager's role (or risk management team) at the right level and within the right area of the agency to facilitate organisational change. Ensure that the role or function grows at the same pace and maturity of the agency's uptake of risk processes and practice.
- ✓ Centralise and promote the risk management resources of the agency to minimise duplication and enhance efficiency.

19 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003, p.28.

20 Comcover *Risk Management Assessment Service Annual Report*, Department of Finance and Deregulation, Canberra, 2007.

COMMUNICATION AND TRAINING

Communication and training – Why is this element important?

Developing a level of risk management awareness and capability requires the implementation of well developed internal communication and training strategies.

Regular internal communication supports the development of a basic understanding of the principles of risk management. It helps ensure that staff develop a shared understanding of the risks that face an agency and supports the adoption of consistent approaches to managing risk across all areas of the agency. It also helps to promote greater understanding of how risk management contributes to achieving an agency's goals.

To understand and manage the risks that face an agency, a shared understanding of the agency's appetite for risk and its risk management process is required. Communicating the process of risk management internally helps clarify ambiguity or inconsistencies that may occur across the agency.

While not all staff are required to be risk professionals, it is important to ensure that those responsible for implementing an agency's risk management program have, or have access to, a high level of risk management competency. While formal qualifications or accreditation are not essential, they can be used to promote an individual's capabilities. They also provide individuals with the opportunity to continually develop skills and to remain aware of emerging issues and practices, which can be used to further improve internal processes.

It is important to ensure staff are educated or trained in accordance with their current level of awareness and the competency level required of their role. Where there is a requirement to educate staff on specific aspects of risk management, this may require specialised training. For example, on complex projects where detailed reporting can assist in communicating progress against objectives, specialised training may be required on developing risk and reporting processes.

It is the risk manager's responsibility when designing a risk training strategy to ensure a mix in the delivery of education or training techniques. For large agencies with decentralised structures, online learning may be appropriate. For smaller agencies, a series of tailored face-to-face sessions may be more effective.

To identify the most appropriate training program, the first step is to undertake a skills analysis to determine the level of current capability across the agency. From this, an understanding of the type of training requirements can be identified, as not all staff will require the same level of risk experience or knowledge to undertake their work responsibilities.

COMMUNICATION AND TRAINING – PRACTICAL TIPS

- ✓ Increase staff awareness of risk issues through a variety of information dissemination methods. Consider the use of newsletters, surveys and the Intranet.
- ✓ Conduct a training needs analysis to determine the risk management competencies required for the agency's staff.
- ✓ Provide appropriate risk management, insurance and risk-related awareness training to all staff, and ensure that staff receive periodic refresher courses after the initial training is held.[21]
- ✓ Ensure your agency's induction program includes an overview of its risk management framework.
- ✓ Encourage managers to develop knowledge and skills in risk management through training programs and self development.[22]
- ✓ Identify and train risk experts. These may be the agency's project management experts, finance professionals or other groups that the agency relies on as part of key management processes.
- ✓ Identify opportunities to develop skills through more informal learning methods, such as regular lunchtime discussion sessions or opportunities for people to learn through practical experience.

21 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance,* ANAO, Canberra, August 2003, p.29.

22 CPA Australia, *Enterprise-Wide Risk Management: Better Practice Guide for the Public Sector*, CPA Australia, Melbourne, 2002, p.36.

Risk assessment – Why is this element important?

Risk assessment is the process of applying risk management to the specific risks faced by an agency. This element includes the development of appropriate risk treatment strategies. The Australian New Zealand Risk Management Standard, AS/NZS 4360:2004 recommends the following steps as integral to the risk assessment process:

- Establish the internal, external and risk management context;
- Identify risks and opportunities that could impact on the achievement of objectives;
- Analyse the likelihood and consequence of identified risks, including the effectiveness of existing controls;
- Evaluate risks with reference to the agency's overall risk management policy and appetite;
- Develop treatment strategies as appropriate;
- Communicate and consult with stakeholders; and
- Monitor and review the effectiveness of both the overall risk assessment process and the agreed treatment strategies.[23]

Establish the context for managing risk

Establishing the context for managing risk is essential to effectively identifying, analysing and evaluating risk. This process will provide the level of understanding that is required to easily identify and document individual risks, while also ensuring the parameters which risks must be managed within are clearly articulated. To establish the context for managing individual risks, first consider the agency's internal and external operating environments. Next, determine the agency's objectives, whether a risk is acceptable and what controls and treatments may be required.

23 Joint Standards Australia / Standards New Zealand Committee, *Australia and New Zealand Standard, Risk Management, AS/NZS 4360:2004*, 3rd edition, August 2004.

Identify risks and opportunities

The identification of risk occurs at all levels of an agency, whether it is considering how best to achieve an agency's outcomes or ensuring the protection of agency assets. Good risk identification recognises the importance of examining all sources of risk to ensure that analysis considers the contribution of each source to the likelihood and consequence of individual risks.[24]

To ensure the most accurate identification of risks, it is important to make certain that staff undertaking the identification process are informed about the policy, project or process being reviewed and have access to quality risk information. This will help ensure a good understanding of the likelihood and consequence of individual risks.

When reviewing and evaluating the quality of risk information, it is important to consider a consistent use of terminology. Confusion around terms can lead to an inconsistent approach to managing risk. Clarity in defining risks is often one of the most difficult steps in risk identification. A common problem encountered is where a risk is articulated as a source of risk rather than a specific risk. This can make it difficult to clearly articulate the risk, and identify the correct controls and treatment strategies.

Analyse and evaluate risk

The purpose of this step is to analyse the likelihood of a risk occurring and its potential impact. This step needs to be undertaken for each identified risk in order to provide the basis for evaluating risks that require further treatment.

As well as considering the likelihood and impact of individual risks, an important step of risk analysis is reviewing existing controls or management strategies for each risk. This will provide clarity about:

- When the risk is likely to occur?
- What are the possible courses of action available to manage the risk?
- What pre-planning can be undertaken ahead of the risk occurring?
- Is it worthwhile developing a contingency plan to manage the risk?

Risk analysis tools are used to assist in measuring the level of risk associated with a particular risk. These tools often have three scales of measurement – consequence, likelihood and the risk level.

The most common risk analysis tool is a risk matrix, which provides qualitative or semi-quantitative scales to measure likelihood and consequence. A greater level of depth can be provided by the selection or use of a three-dimensional tool that can measure likelihood in greater detail by breaking down probability and exposure.

Once current controls and management strategies have been considered, risks can be reported in a risk matrix. This simple tool assists in determining whether the risk should be prioritised for further action.

24 Joint Management Advisory Board/Management Improvement Advisory Committee (MAB/MIAC) Report No.22, *Guidelines for Managing Risk in the Australian Public Service*, MAB/MIAC, Canberra, 1996, p.23.

Develop treatment strategies

Once risks have been analysed, evaluated and prioritised, agencies need to determine a strategy for the mitigation of each risk. In broad terms, a decision should be made to either:

- **Avoid or reduce the risk** by adopting alternative approaches to achieving an objective. For example, in the case of a project risk, the treatment strategy might involve identifying an alternative course of action such as revised timing, a different delivery model or a different resource mix. Each may reduce the risk likelihood to zero and thus avoid the risk.
- **Transfer the risk** through the use of contacts and insurance arrangements. Risk can be transferred to another party which has greater control over the risk situation, or is less susceptible to the impact of the risk factors. This is generally achieved through contractual or insurance arrangements, noting that responsibility for overseeing the risk cannot be transferred as ultimate accountability for the risk rests with the responsible officer or agency.
- **Accept the risk** and develop contingency plans to minimise the impact should the risk eventuate. For the risks we accept to manage, it is necessary to identify a person responsible for establishing a monitoring process that captures the likelihood of the risk occurring and the treatment strategies to be applied should the risk eventuate.

Communication and consultation

The communication of risk issues and risk information with key stakeholders is important to maintain high levels of confidence from stakeholders. External stakeholders such as ministers, industry, customers, suppliers and the broader community need to have the opportunity to communicate their views and feel involved in decision-making. A thorough communication and consultation process can provide useful feedback to be considered when identifying and evaluating risk. It will also enable you to take into account the current risk tolerances of key stakeholders at all stages of the risk assessment process. In some cases, it will also influence the choice, acceptance of, and in turn, the effectiveness of treatment strategies.

Monitoring and review

Due to the dynamic operating environment of agencies, the ongoing monitoring and review of individual risks is a necessary step in the risk assessment process. Regular monitoring and review should ensure the correct identification of risks as well as consider the most effective and appropriate strategies for the treatment of individual risks.

Factors such as changing policy or the need to reduce operating costs may impact the likelihood or consequence of risks. This can cause changes to individual risks and the level of impact of these risks.

When reviewing the status of individual risks, consider the effectiveness of current risk treatment strategies. This process of monitoring and review provides assurance to those responsible for managing risk and senior executive, that there are no surprises from new or emerging risks, and that risk treatment strategies continue to be cost effective and appropriate.

RISK ASSESSMENT – PRACTICAL TIPS

- ✓ Keep the risk identification and assessment process simple. As the agency matures refine this process to include quantitative and qualitative analysis where needed.
- ✓ To ensure the consistent application of risk management processes, develop a common risk language across the agency that is understood by all. A glossary of terms and key definitions (risk dictionary) can be easily maintained on an agency's Intranet.
- ✓ Create a common list of sources of risk for your agency to be included in your risk assessment documentation. Consider the following as possible sources of risk:
    - commercial or legal relationships;
    - financial market or economic environment;
    - business interruption;
    - human resources or planning;
    - natural events; and
    - environmental.
- ✓ Analyse sources of risk to identify common or shared risk drivers. This will support efficient resource allocation for treatments.
- ✓ Ensure the risk manager, or risk management team, responsible for overseeing the risk management process in your agency is available to assist in identifying risks, if required. Possible methods of identifying risk include conducting interviews or group discussions to workshop the identification of key risks.
- ✓ Develop a suite of document templates to support the risk assessment process including:
    - risk register;
    - incident log;
    - risk assessment;
    - risk profile; and
    - risk management and treatment plan.
- ✓ Develop strategies to manage stakeholder expectations by identifying the risks that might impact them.[25]
- ✓ Include controls and treatments in risk management plans for specific risks, as well as documenting who is responsible for the risk and the treatments.
- ✓ Recognise insurance, where appropriate, as a treatment in risk management and treatment plans.[26]
- ✓ Include timeframes for implementing treatment strategies in risk management plans, and monitor and report on both the timeliness and effectiveness of risk treatments.

25 CPA Australia, *Enterprise-Wide Risk Management: Better Practice Guide for the Public Sector*, CPA Australia, Melbourne, 2002, p.21.

26 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003, p.29.

Risk profiling and reporting – Why is this element important?

An agency's risk profiling and reporting processes provide for the collection, reporting and communication of risk information to internal and external stakeholders.

Risk profiling and reporting encourages regular review of program or project delivery, provides assurance on controls, and the opportunity for senior executive to review the agency's level of risk tolerance or risk appetite, and assess the effectiveness of risk treatments.

Appropriate sponsors for each risk area should be appointed to ensure action is taken to manage key risks. Risk profiles should link into an agency's governance framework to ensure that risks and the effectiveness of treatment strategies are regularly reviewed and reported, and accountability and responsibility for managing risks is clearly articulated.

Risk profiling

Risk profiling provides a high-level status report of an agency's risks. A risk profile is a key tool for informing senior management on the priorities and management of risk across the agency. A risk profile differs from the development of risk management plans or registers, as it uses data from a number of different sources such as operational, project and program risk reviews. An agency's risk profile will change over time as risk priorities change through changes in the agency's activities, changes in the external environment and as a result of the progressive implementation of treatment strategies.

Creating a risk profile for the agency:

- facilitates identification of risk priorities;
- captures the reasons for decisions made about what levels of risk exposure are acceptable;
- provides an overall picture of this risk profile of an agency and allows those responsible for the management of particular risks to see how their risks fit into the bigger picture; and
- facilitates review and monitoring of risks at the strategic level.[27]

Risk reporting

When developing a risk reporting framework, it is important to consider the external reporting required, such as compliance reporting in relation to financial sustainability or occupational health and safety, as well as internal management reporting requirements. To prevent duplication of processes, information provided in strategic reporting can be used to inform senior management and executive when completing annual compliance reporting tasks.

A strategic risk report needs to identify, assess and provide information on the monitoring of risks against the strategic objectives of the agency.

Operational risk reporting is also critical to ensure that the agency's risk management framework and program are consistently implemented across the agency. Operational reporting can occur each quarter with the resulting data considered when preparing strategic risk reports for senior management.

27 HM Treasury, *The Orange Book Management of Risk – Principles and Concepts*, United Kingdom, 2004, p.20.

Essential operational risk reports include:

- Risk registers – An agency's risk registers contain descriptions of individual risks, including their causes, impacts and existing controls. Regular review of risk registers:
  - helps to ensure that risks are correctly reflected, and are in line with an agency's risk management framework; and
  - ensures the correct priority and rating of individual risks has been identified (that is, those risks that are rated as high or extreme) and are brought to the attention of senior management as part of the strategic reporting process.
- Risk treatment plans – To reduce the cost of managing risk, risk treatment plans should be reviewed to ensure treatment strategies are consolidated and that there is no duplication in either resource allocation or in the monitoring of individual risks.

Risk data generally needs a level of translation and consolidation for it to be meaningful at the strategic level. To ensure that material provided for review by senior management is appropriate, consider the following key questions:

- What do they need to know?
- What is the most acceptable format when presenting information?
- What analysis has been undertaken to provide a level of robustness to the data?
- What follow up action do they need to undertake?

The documentation and reporting of risk information is important to develop and maintain corporate knowledge, and to promote an understanding of risk. Risk should be recorded to ensure compliance with regulatory and legislative requirements, and to demonstrate transparency and accountability.

RISK PROFILING AND REPORTING – PRACTICAL TIPS

- ✓ Develop a tailored risk profile for the agency, which translates operational risks into a strategic report that reflects the risk context and risk appetite of the agency. Ensure that the agency's risk profile is reviewed and monitored at least quarterly.
- ✓ Connect the operational risk reporting framework with the strategic reporting element of the risk management framework.
- ✓ Monitor and report on risk activities to senior management in accordance with the timeframes established in the risk management policies. Reporting on treatments for high risks should occur at least quarterly (and bi-annually for other risks) to assist management to monitor the appropriateness and effectiveness of risk treatment strategies.[28]
- ✓ Provide opportunities for senior management involvement in risk profiling and reporting, including analysing key strategic and operational risks and treatments, as this is essential to achieving successful outcomes.[29]

28 Australian National Audit Office Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003, p.30.

29 ibid., p.28.

References

Australian National Audit Office Audit Report No.3 2003-2004, *Management of Risk and Insurance*, ANAO, Canberra, August 2003.

Australian National Audit Office Better Practice Guide, *Public Sector Governance, Volume 1, Framework, Processes and Practices,* ANAO, Canberra, July 2003.

Australian National Audit Office Better Practice Guide, *Public Sector Audit Committees,* ANAO, Canberra, February 2005.

Australian Public Service Commission, *Building Better Governance,* APSC, Canberra, 2007.

ASX Corporate Governance Council, *Corporate Governance Principles and Recommendations,* 2nd edition, 2007.

Comcover, *Comcover's Awards for Excellence in Risk Management,* Comcover, Department of Finance and Deregulation, Canberra, 2003-2007.

Comcover, *Comcover's Benchmarking Risk Management Program,* Department of Finance and Deregulation, Canberra, 2001-2007.

Comcover, *Risk Management Assessment Service Annual Report*, Department of Finance and Deregulation, Canberra, September 2007.

CPA Australia, *Enterprise-Wide Risk Management: Better Practice Guide for the Public Sector,* CPA Australia, Melbourne, 2002.

Department of Finance and Deregulation, *Finance Circular 2008/04: Certificate of Compliance – FMA Act agencies*, Finance, Canberra, 2008.

Department of the Prime Minister and Cabinet, *Requirements for Annual Reports for Departments, Executive Agencies and FMA Act bodies,* PM&C, Canberra, 2007.

HM Treasury, *The Orange Book, Management of Risk – Principles and Concepts,* United Kingdom, October 2004.

International Organization for Standardization, *Draft International Standard, Risk Management – Principles and Guidelines on Implementation, ISO/DIS 31000,* 2008.

Joint Management Advisory Board / Management Improvement Advisory Committee (MAB/MIAC) Report No.22, *Guidelines for Managing Risk in the Australian Public Service,* 1996.

Joint Standards Australia / Standards New Zealand Committee, *Australia and New Zealand Standard, Risk Management, AS/NZS 4360:2004,* 3rd edition, August 2004.

Joint Standards Australia / Standards New Zealand Committee, *Handbook, Risk Management Guidelines Companion to AS/NZS 4360:2004, HB 436:2004,* 2004.

KPMG, *Risk management beyond compliance: A reflection on current issues and future directions from Australia's top chief risk officers,* KPMG Australia, November 2006.