CONTENTS

Overview .................................................................................. 2
Mandatory requirements ......................................................... 5
Principles .................................................................................. 6
Risk management ..................................................................... 8
Risk governance ..................................................................... 14
Risk process ........................................................................... 22

Resources .............................................................................. 33
Insurance ................................................................................. 34
Glossary .................................................................................. 36
Appendices .............................................................................. 39
Templates ................................................................................ 48
The community expects Government to be vigilant – to be alert and respond to the full range of potential harms that comprise the safety, security and wellbeing of Victorians.

In order to meet this expectation and achieve its strategic objectives, Government must be prepared for risk. It needs its public sector to be productive, innovative and efficient, anticipating and managing the risks that could affect the delivery of its policy agenda.

**Message from the CEO**

It’s a privilege to work with the Victorian public sector and provide the education, insight, advice and support needed to help you effectively manage risk to confidently deliver on the Government’s agenda.

Victorians expect their government to be vigilant and controlling the range of harms that could compromise either their safety, security and wellbeing. As a result, the Victorian Government must be prepared for risk. It needs its public sector to be productive, innovative and efficient and tackling the risk-related issues that affect its ability to deliver the services needed.

Risk management, done well, will prevent harm or reduce its impact. This guide is a practical tool to help you plan for and engage with risk, both in your agency and across the public sector. Using this guide will help you:

- Navigate the Victorian Government Risk Management Framework
- Understand your agency’s risk profile
- Be confident the measures you take reflect sound planning
- Reinforce an organisational culture improving outcomes for Victorians
- Improve your agency’s risk maturity over time.

We welcome your feedback and experience in using the guide.

Risk management is the combination of culture, systems and processes undertaken by an agency to coordinate the identification and management of risk. Risk management activities inform decision making, support the achievement of objectives and the prevention of harm.

Government requires:

- awareness and evidence to make informed decisions on its appetite for risk
- a clear line of sight across inter-agency and State significant risks over the medium to long term.

Government needs to have confidence that the public sector can deliver services to the community and:

- understands and manages the risks it is exposed to
- receives support and advice from experts in risk management
- employs value-for-money risk solutions.

This guide has been developed to support the framework and help agencies meet their risk obligations and accountabilities including attesting that risks are being managed effectively and efficiently.
Using this guide

This guide aims to provide a practical explanation of key risk management concepts and practical tips to improve your capability.

You can adapt this guide to suit your agency.

Visit our website for further resources www.vmia.vic.gov.au

Navigation

**What must be done**
- Mandatory requirements page 5

**How to deliver**
- Principles pages 6-7
- Risk management pages 8-13
- Risk governance pages 14-21
- Risk process pages 22-32

**Where to look for help**
- Resources page 33
- Insurance pages 34-35
- Glossary pages 36-38
- Appendices pages 39-47
- Templates page 48
Our support

Our work is to help public sector agencies be prepared for risk and to do so effectively and efficiently.

VMIA can provide you with risk advice, thought leadership and a coordination point for risk prevention, recovery and assurance.

We provide services and advice to enhance your risk management and insurance arrangements.

We can work with you to embed enterprise and insurable risk management into your organisational practices.

Our work is about:

- **Education**
  Building the skills and capabilities of your team to better respond to risks.

- **Advice**
  Providing expert advice and consulting services to assist you in tackling your issues, guiding action and decision making.

- **Insight**
  Helping you turn information into knowledge, to know what's important and guide your action.

- **Learn**
  Reflecting what's gone wrong to make changes for the future.

Risk Management principles and guidelines

There are a number of standards that provide general guidance on best practice risk management. Government has adopted the [Australian and New Zealand Standard](#). This Standard is important because it helps to guide you on risk, what's important and what to do about it.

The framework requires you to act consistently with the Australian and New Zealand Standard. Consider it a ‘baseline’. Doing more will reflect your agency’s maturity.

The Standard has three central concepts and these are reflected in the guide.

There are a range of other Standards this guide draws on.
Government requires your agency to comply with the framework. Your senior officers must attest to your agency’s compliance with the framework and Victorian law.

### Risk management

Your agency must be satisfied that risk management is adequately resourced and that its risk management framework:

- Is consistent with the Australian and New Zealand Standard.
- Supports the development of a positive risk culture
- Is reviewed annually.
- Includes processes that effectively manage risk.
- Makes it clear who is responsible for managing each risk.
- Addresses the management of inter-agency risks and State significant risks.
- Demonstrates that business planning activities incorporate risk management.

### Insurance

Your agency must arrange all of its insurance with VMIA (unless exempted) and as part of your annual insurance renewal process:

- Consult with VMIA to determine appropriate insurance levels.
- Maintain a register of insurance and indemnities.
- Provide information on claims management capability, resources, structures and processes for any self-insured risks.

For self-managed claims your agency needs to maintain adequate claims management capability and processes and provide self-managed claims data to VMIA.

### Risk, insurance and attestation

We have summarised the risk and insurance requirements. Please refer to the Department of Treasury and Finance for the [Victorian Government Risk Management Framework](#).
This section outlines the 11 principles of the Standard and how they have been defined. This guide has been designed to ensure that it reflects the intent of the principles.

Risk management principles are not compliance-focused. They provide a set of statements to guide and assist in the design, implementation and oversight of your risk management framework. Reference to decision making, human behaviour and cultural factors includes ensuring risk management is operating as intended and contributes to improved performance and outcomes.

<table>
<thead>
<tr>
<th>Risk management</th>
<th>How is it applied?</th>
<th>Why is it important?</th>
</tr>
</thead>
</table>
| 1. Creates and protects value | • incorporated into governance framework  
• considered as part of organisational culture | • contributes to the achievement of objectives  
• assists to improve performance  
• protects community interests |
| 2. Is an integral part of an agency planning and management process | • integrated into strategic and business planning  
• informs delegations  
• part of change management processes | • avoids duplication  
• guides prioritisation  
• clarifies responsibilities |
| 3. Is part of decision making | • built into approval processes  
• explicitly incorporated into projects, system design and changes and resource allocation  
• part of all contractual agreements  
• part of staff recruitment and employment arrangements | • assists decision makers to make informed choices  
• assists to prioritise actions  
• distinguishes among alternative courses of action |
| 4. Explicitly addresses uncertainty | • used to develop descriptions for risk rating criteria (i.e. likelihood and consequence)  
• linked to assessing objectives | • explicitly identifies uncertainty in the agency’s internal and external contexts  
• promotes a shared view of risks and risk appetite  
• identifies vulnerabilities |
| 5. Is systematic, structured and timely | • incorporated into the design of all systems rather than a stand-alone process  
• consistently applied through clear guidance  
• measured and reported | • contributes to a consistent and efficient approach  
• facilitates comparability of results and benchmarking  
• promotes consistent understanding |
<table>
<thead>
<tr>
<th>Risk management</th>
<th>How is it applied?</th>
<th>Why is it important?</th>
</tr>
</thead>
</table>
| **6. Is based on best available information** | • advice and support for risk management is available  
  • specifies the functional requirements of risk management systems  
  • used to accurately define uncertainty and ensure treatments are relevant | • stakeholders require accurate and reliable data to manage risk  
  • risk attestation is supported  
  • evaluates the effectiveness of controls  
  • develops risk monitoring and reporting  
  • risk management information systems are fit-for-purpose |
| **7. Is tailored** | • the risk framework is designed and operated to fit with the agency's context and capabilities | • aligns with agency's external and internal context and risk profile  
  • consistent with agency's culture  
  • adequate resources are allocated  
  • comply with legal obligations |
| **8. Takes human and cultural factors into account** | • the risk framework considers how people and cultures interact with its functions and how to monitor risk culture and behaviour | • aligns the capabilities and intentions of stakeholders with the organisation's objectives  
  • ensures consistency between culture and behaviour |
| **9. Is transparent and inclusive** | • identifies scope and method for risk monitoring and reporting to stakeholders  
  • identifies elements required in the risk criteria  
  • identifies the role of stakeholders in the risk management process | • promotes line-of-sight of risks between all levels of the agency  
  • facilitates appropriate and timely involvement of stakeholders  
  • ensures that risk management strategy remains relevant and up to date |
| **10. Is dynamic, iterative and responsive to change** | • incorporated into change management strategies  
  • incorporated into strategic and business plans | • builds agency resilience  
  • ensures strategy takes account of emerging risks  
  • ensures the risk management framework is responsive to changes in context |
| **11. Facilitates continual improvement** | • risk management system is incorporated in continual improvement systems  
  • risk attestation and the results of internal audit are used to inform continual improvement  
  • stakeholder feedback is sought to influence the ongoing development of the risk framework | • improves agency risk maturity  
  • addresses stakeholder expectations to protect community interests  
  • assists agency to meet obligations |
There are a number of terms and concepts that are often used to describe activities relating to managing risk. Understanding these will help an agency manage risk more effectively.

The following are some of the key terms and concepts covered in this section:

- risk
- risk-based decision making
- risk management
- risk management framework
- risk maturity.

Risk

“Risk is the effect of uncertainty on objectives.”

AS/NZS ISO 31000:2009

The effect that uncertainty has on the achievement of an agency’s objective, gives rise to risk.

All agencies in the public sector are exposed to some level of risk, which all agencies have an obligation to manage.

An agency will be exposed to risk from many sources such as: political, economic, social, technological, regulatory or environmental. There are many different types of risk and multiple factors that influence risk. These may be global or localised and within the actual agency. Some factors will be beyond the agency’s ability to influence or control but the agency may still be impacted.

The positive aspect of risk is the “risk/reward” concept, where the benefits of taking a risk outweigh the potential negative impacts. Risk taking should be guided by an agency’s risk appetite and managed in accordance with its risk framework.

To manage risk, it is important to understand how uncertainty and objectives influence risk:
Uncertainty – There is no absolute certainty about the future but there is generally a level of predictability to outcomes and performance. Uncertainty reduces the predictability, in turn giving rise to risk.

As uncertainty changes, so does the risk. This means a risk is dynamic and needs to be monitored and reviewed on a regular basis.

Common sources of uncertainty are – When something is not available, unreliable or invalid; where the interaction or relationship is unknown, is variable or can be interpreted differently; when something is random, inconsistent; or has a range of possibilities and changes over time. Assumptions and presumptions are also common sources of uncertainty.

Objective – A clear understanding of the objective is important to risk identification. If there is a lack of clarity about what the agency is trying to achieve, it can result in a risk being identified that is not an actual risk. This can have flow-on consequences, such as unnecessary investment in controls and resources and underlying exposures left unidentified and unmanaged.

There are many ways to express an objective – An objective can be a personal objective, daily objective or an objective that relates to the outcomes the agency wants to achieve. The objectives of the agency are the expression of intent and purpose that generally relates to enabling legislation, strategy and vision.

Business objectives are often described as SMART –
- **S**pecific
- **M**easurable
- **A**ttainable
- **R**elevant
- **T**ime-bound.

In most agencies there will be multiple strategic, operational and project objectives. Executive and senior managers have a role to manage conflict or dependencies between objectives and find ways to address any uncertainties.

When considering risk:
- identify what event or situation would cause you to not achieve the objective
- consider the potential impact(s) to the objective
- describe the risk as a clear concise meaningful statement
- undertake an assessment of the risk
- decide what action should be taken.

Practical tips

For risk management:
- define the objective to determine the risk(s)
- consider the objective in a future context (either short, medium or long term)
- identify what is uncertain about the objective
- formulate a view of what is important to achieve the objective
- identify and manage through the risk management process (see process section)
- consider resources required to manage risks
- assess future requirements as priorities change.
**Risk-based decision making**

Decisions are often made based on incomplete information and where the outcome is uncertain. For example, they may be based on the best available information at the time, and a reliance on assumptions, research, evidence or past experience.

Risk-based decisions however, are where risk management as a discipline is applied to the decision making process.

This means taking into account the uncertainties of potential choices and considering the effects and impact of action before making a decision.

Understanding how much risk the agency is prepared to take is a useful way to help make a risk-based decision. If there is limited tolerance for a risk, it provides good guidance on what decisions cannot be made. Conversely, where the agency is prepared to take some risk within its mandate and legislative obligations, it provides decision makers with more confidence.

There are essentially two types of risk based decisions:

- **Informal** – where there are conversations and discussions involving routine day to day activities of the agency.
- **Formal** – is generally applied for key activities and objectives with a defined process and approach. This would involve a clear audit trail that may include: a brief, submission, report, documentation and supporting evidence.

---

**Case study on risk-based decision-making**

It is forecast that the population will rise in regional centres by 25% over the next five years. To help plan for this, Agency A has agreed to the following.

**Objective:** Increase service delivery in rural areas by 15% by 2020.

**Proposed model**

An innovative service delivery model has been proposed and a decision is required to scope, plan and implement the model. The outcome of the model is uncertain as there is limited information available about the potential success of the model, although pilot studies have indicated favourable results. There has been research into this model but there is no past experience to determine its effectiveness. Assumptions have had to be made based on limited research and the pilot.

A key area of consideration is whether the community will embrace the proposed service model and the effect this may have on the objective if they don't.

**Uncertainty**

- Assumptions have been made about each region
- Community engagement has been difficult to achieve in the past
- Remote areas will be difficult to penetrate due to limited resources
- Funding might only be available for three years and it is dependent on other priorities
- Staff turnover has been an issue in the past and it is not clear whether key staff with the skills required can be retained.

**Risk-based decision**

Given the importance of this objective, a formal risk assessment should occur to explore what is uncertain and identify potential risks to the objective. It may be possible to mitigate some of the risk(s) to an acceptable level.

Decision makers can then consider the benefits of introducing the service model, the risks that are not acceptable and what remains uncertain. Based on this information options can be formulated that detail uncertainties, assumptions, dependencies and the pros and cons.

The final decision maker can then make an informed decision based the available information at the time and determine if Agency A should proceed with the service model.
Risk management

“Coordinated activities to direct and control an organisation with regard to risk.”

AS/NZS ISO 31000:2009

Risk management is used to describe the activities undertaken by an agency to identify, assess and manage its risk. Risk management is fundamental to improving performance and achieving outcomes. When routinely applied, informed decisions can be made with more confidence.

Risk management is most effective when:

“every person thinks about risk and manages risk as part of their job.”

Risk management cannot prevent every risk from occurring due to the uncertain nature of some risks.

Risk management will:
- develop a discipline to avoid or reduce the likelihood and potential impact(s) of a risk
- provide a level of comfort that informed decisions are being made
- ensure the Victorian public sector is doing all it reasonably can to manage its risk.

Risk management supports an assessment and decision regarding:
- what risks to avoid
- why some risks can be taken
- how risks must be managed.

The benefits of risk management

Risk management includes the approach, process and activities undertaken to ensure that:
- adequate oversight, reporting, monitoring and assurance occurs
- risks are identified, assessed and action is taken
- controls are identified, assessed and sufficient investment occurs
- people have the right capability and skills to manage risk.

Risk management applied as a discipline within the agency's prescribed risk management framework will:
- support successful execution of strategy, business plans and projects
- increase the chance of achieving objectives
- improve culture
- provide confidence to Government and the community
- promote the efficient allocation of resources
- reduce negative perceptions and impact on reputation
- empower people to make decisions with confidence
- determine how much risk can be taken and tolerated
- inspire others to follow examples and work collaboratively.
Risk management framework

A risk management framework is the:

“Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.”

AS/NZS ISO 31000:2009

A framework is the term used to describe the totality of all processes, procedures, documents, policies, resources, governance, and arrangements it has in place that contribute to risk management.

An agency will already have many frameworks in place, designed to deliver its services and undertake activities. Some examples include: compliance framework, safety framework and governance framework.

A framework is essential to ensure there is an agreed approach to manage risk. It is required as part of overall governance arrangements and will also complement and support other frameworks.

The Standard sets out the components of a risk management framework. While an agency will have processes and approaches in common with other agencies, all agencies are different due to their mandate and requirements. This means their approach to risk management should be developed and tailored to suit their specific requirements.

Developing an effective risk management framework

The following can be considered:

**Risk governance**

The agency will:

- develop a risk management strategy and improvement plan
- ensure roles and responsibilities are well defined and included in position descriptions
- commit to improving, monitoring and measuring risk culture
- assess its risk appetite and incorporate it into decision making and corporate planning
- develop an approach that provides assurance to the Responsible Body risks are being managed.

**Process**

The agency will:

- establish and communicate its process
- develop appropriate tools and templates
- ensure people have adequate skills and capability
- develop escalation protocols
- ensure risk appetite is defined in its risk criteria
- identify State significant and inter-agency risks
- invest in control assessment and management
- align internal auditing to monitoring risk.

**Resources**

The agency will:

- invest adequate resources into the function
- support independence and escalation of risks
- assess capability requirements and link it to development plans
- create opportunities for people to champion risk
- provide adequate training and learning opportunities.
Risk profile review

This is a formal process where the agency’s risk profile is reviewed periodically and annually.

This could involve a requirement to:

- collect evidence of the identification, evaluation and review of risks and their controls
- assess effectiveness that is supported by audit activities and data to provide assurance.
- review and sign-off of the process by risk owners
- escalate any deficiencies and failures in systems or processes with recommendations for further actions
- assess that the process has been adopted and implemented
- check that there is evidence of:
  - governance, systems and reporting
  - risk identification and understanding of the agency’s risk profile and management plan
  - assurance activities
  - failures and deficiencies identified and escalated for further actions
  - continuous improvement in managing risks which are dynamic and changes as the operating environment changes.

Risk maturity

Risk maturity describes the capability and level of maturity an agency operates at in terms of its risk framework. Risk maturity is linked to an agency’s performance and achievement of outcomes.

Risk maturity typically encompasses all elements of the risk management framework. There may be varying levels of risk maturity across different elements within the framework.

Risk maturity is not a static concept and is susceptible to internal and external factors and drivers over time. As an agency and its context changes, risk management also needs to evolve to ensure that it continues to support the achievement of objectives.

The desired level of risk maturity should be considered by the Responsible Body aligned to achieving strategic objectives and managing its risk profile. The desired risk maturity should be reflected in the agency’s risk management strategy to influence risk improvement activities.

An agency should consider developing and implementing strategies to improve its risk maturity (or maintain it at the desired level).

Continual improvement is a fundamental element for effective risk management. An agency will need to develop its approach to risk management over time and invest adequate time and resources to achieve its desired rating.

Risk maturity goes beyond the structural elements of ensuring a framework is in place. It also requires an agency to determine if it is effective. This means an agency would need to assess whether:

- risk management is contributing to its overall performance
- risk management function is operating as expected
- outcomes are being achieved.

Risk maturity assessment

An assessment of risk maturity enables the agency to assess the performance of the risk management framework and to determine whether it is meeting expectations. An assessment provides a roadmap for improvement through identifying opportunities to mature the framework to the desired level. An agency may choose to undertake a self-assessment of its risk maturity using an internally developed methodology or an established model such as that defined in AS/NZS ISO 31000 or the VMIA risk management assessment methodology.

Further guidance, tools and templates are available on VMIA’s website at www.vmia.vic.gov.au
This section outlines the inter-dependence of good risk governance and effective risk management. It provides guidance on how to improve risk governance, and assess its effectiveness.

**Risk Governance**

Risk governance refers to the culture and arrangements developed by an agency to manage the uncertainties to achieving its objectives. It includes the leadership, accountabilities and oversight that builds and improves the risk management approach.

Risk governance is an essential part of an agency's overall governance responsibilities.

Effective risk governance supports an agency to improve performance and achieve desired outcomes as it will:

- guide required risk management behaviours
- establish consistent processes
- drive informed decision making.

**Practical tip**

For a risk management framework to be effective:

- Alignment of corporate planning to the risk management framework is an essential component of good governance.

Many agencies adopt a **three lines of defence** model. Three lines-of-defence is most effective when there is active support and guidance from the Responsible Body and senior management.

Each of these three lines has a distinct role in an agency’s governance and oversight. The Responsible Body, committees and senior managers are considered the primary stakeholders that are served by the established lines. This means they are in a position to ensure that the three lines of defence are reflected, enacted and reviewed as part of the agency’s risk management control processes.
The following diagram depicts the three lines of defence and the risk and control environment:

**Corporate and business planning**

Corporate and business planning refers to the annual planning an agency undertakes at all levels to determine its objectives and develop supporting plans.

Risk management must be incorporated into corporate and business planning processes as a mandatory requirement.

Incorporating risk management provides value to decision makers as it will:

- identify what could impact the agency’s objective(s)
- provide an opportunity to develop strategies to minimise the impact
- support decisions on how much risk can be taken to achieve an objective.

If risk management is not incorporated it essentially means decisions are made that have not considered what is uncertain and the possible resulting effects, implications and dependencies.

Investment decisions also require some consideration of risk, as an agency has finite resources and could find it will allocate resources inefficiently.

Risk management in corporate and business planning would include the identification and validation of key risks to strategic objectives and risks associated with business or divisional plans.

Risk management should also be undertaken for projects, policy development and as part of delivery of programs and services. This will ensure there is a comprehensive, consistent and integrated approach across the agency. Failure to do this could result in gaps and unexpected exposures.

Each agency will need to determine the best approach to incorporate risk management and this should be documented in its risk management plan.

The risk process section (page 22) provides guidance on how to undertake strategic risk identification.

---

Adapted from ECIA/FERMA Guidance on the 8th EU Company Law Directive, article 41

See Appendix B for three lines of defence model.
The following is an example of how risk management can be embedded into corporate activities:

**Quarter 4 Activities**
- Corporate plan finalised
- Annual risk reporting
- Insurance Attestation

**Checklist**
- Review Risk Register
- Audit & Risk Mgt Committee
- Risk reporting

**Quarter 3 Activities**
- Insurance questionnaire
- Review insurance cover
- Annual review (risk framework, risk appetite and tolerance)

**Checklist**
- Review Risk Register
- Audit & Risk Mgt Committee
- Risk reporting

**Quarter 2 Activities**
- Pre-budget insurance premium advice
- Corporate strategy workshop
- Strategic Risk Identification

**Checklist**
- Review Risk Register
- Audit & Risk Mgt Committee
- Risk reporting

**Quarter 1 Activities**
- Corporate plan roll out
- Annual Report (including attestations)

**Checklist**
- Review Risk Register
- Audit & Risk Mgt Committee
- Risk reporting

---

**Risk management policy**

A risk management policy outlines the intent of the agency with respect to risk management and describes the governance arrangements and expectations.

It provides guidance and is fundamental to establishing a positive risk culture in an agency by clarifying expectations regarding the attitude, awareness and accountabilities related to risk management.

The policy should be endorsed and approved by the Responsible Body and reviewed annually or when there is significant change.

A template is provided with this guide.
Risk management strategy

A risk management strategy describes an agency's future vision, direction and objectives for risk management. It incorporates key activities designed to achieve these objectives and the plan to build risk management capability and maturity.

The risk management strategy ensures the agency's Responsible Body and management have a common and clear view of the purpose of risk management, the activities to be pursued to enhance the framework and the capability building requirements to achieve this.

An effective risk management strategy ensures the risk management framework is suitable to the context of the agency. It enables an agency to:

- prioritise monitoring activities (such as risk maturity assessments)
- assist in the direction of resources to support gaps in risk management capability
- strengthen its approach to continual improvement.

An agency should consider its risk management strategy development in line with its corporate planning cycle. A structured approach which involves a clearly documented plan, endorsed by the Responsible Body, should be adopted.

Developing a risk management strategy will:

- provide a common view of context, risk management capability and maturity
- define the vision, objectives and future direction of risk management
- ensure risk management is aligned to the context and corporate objectives
- establish a plan to address risk management capability gaps
- assist with prioritising the risk framework monitoring and assurance activities
- align to the continual improvement approach.

Practical tips

In establishing a risk management strategy an agency should:

- Establish the context for risk management – review the function of risk management and define its value, future role and objectives in the agency.
- Develop risk management strategy – identify strategies to achieve risk management objectives.
- Develop improvement plan – assess capability gaps and establish activities to build capability to achieve the strategy.
- Communicate – consult with key stakeholders throughout the strategy development, ensure the strategy is endorsed by the Responsible Body and communicate outcomes throughout the agency.
Risk culture

Risk culture refers to the behaviours that lead to how every person thinks about and manages risk. Risk culture is a component of the overall culture of an agency. The risk management framework must support the development of a positive risk culture within the agency.

The Responsible Body and the executive are responsible for setting the ‘tone at the top.’ They play a key role in influencing and articulating the desired risk culture.

Developing a positive risk culture is essential to developing risk maturity and building capability. It is important because it will:

- create the tone and set expectations
- modify behaviour to what is expected within the agency’s values and behaviours
- underpin risk-based decision making.

Developing a positive risk culture requires a continuous improvement approach. This will ensure people are provided with opportunities to grow and improve their risk management capability and knowledge. It will also support consistent and appropriate risk decisions.

Risk culture encompasses how risk management is embodied and includes:

- **Accountability** – the way in which accountabilities are communicated and managed.
- **Awareness** – how aware people are of the risk management framework.
- **Attitudes** – the attitude towards risk management and its value proposition.

Combined, these characteristics reflect the behaviour of an agency towards risk management.

It is possible to assess risk culture and align the outcomes to the risk improvement plan.

Many agencies now include risk culture as part of their annual staff engagement survey or undertake a separate risk culture survey.

The results are reported through to the Responsible Body and relevant governance committee and aligned to the risk improvement opportunities and development plans.
The following provide guidance on the three components for developing a positive risk culture:

<table>
<thead>
<tr>
<th>Accountability</th>
<th>Awareness</th>
<th>Attitudes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Responsible Body and executive take leadership responsibility for risk management.</strong></td>
<td><strong>Risk management is at the front-end of decision making and aligned to objectives.</strong></td>
<td><strong>Risk management is viewed as everyone’s responsibility.</strong></td>
</tr>
<tr>
<td>• obligations, delegations and accountabilities are documented and communicated</td>
<td>• risk management policy and procedures are readily available</td>
<td>• risk management function has influence</td>
</tr>
<tr>
<td>• commitment and ‘tone from the top’ are widely understood and consistently applied</td>
<td>• integrated into corporate and business planning cycle</td>
<td>• value is expressed through discussions, actions and activities</td>
</tr>
<tr>
<td>• intent is reflected in values and behaviours and are consistently applied</td>
<td>• applied as part of day-to-day decision making and activities</td>
<td>• ongoing learning supports improvement initiatives</td>
</tr>
<tr>
<td>• reporting is transparent and timely</td>
<td>• standard approaches and access to supporting documents and tools</td>
<td>• people feel free to challenge and escalate</td>
</tr>
<tr>
<td>• performance mechanisms support and reward positive risk behaviour</td>
<td>• common vocabulary is developed and understood</td>
<td>• people operate within delegations</td>
</tr>
<tr>
<td>• roles, responsibilities and ownership are documented and communicated</td>
<td>• obligations, delegations and accountabilities are understood and applied</td>
<td>• agency values are evident in people’s behaviour</td>
</tr>
<tr>
<td>• risk culture is evaluated and aligned to the risk improvement plan.</td>
<td>• roles, responsibilities and ownership are understood and accepted.</td>
<td>• ethics and integrity underpin activities.</td>
</tr>
</tbody>
</table>

**Practical tips**

To develop a positive risk culture an agency should:

- ensure the message is communicated by the Responsible Body and the executive
- assess whether staff understand the message
- determine how risk culture is reflected in day-to-day practice
- assess how a positive attitude towards risk management is modelled through line managers
- develop a safe environment to report and escalate risk
- determine whether action to occur for risk taking is outside an individual’s delegated authority or scope.
Examples of where risk culture would be evident are:

- mission and values statements
- board orientation program
- by-laws and charters
- delegation authorities
- policies and procedures
- position description
- staff induction programs
- performance review templates
- audit reports
- incident/hazard/reporting, near misses
- quality improvement plans
- posters and brochures
- feedback from suggestion boxes
- minutes of meetings
- staff engagement surveys
- stakeholder feedback
- complaints
- learning and development programs
- standard templates and tools.

Case study of a positive risk culture

A Victorian public sector agency's board made a strong commitment to risk management and expressed a desire for it to be a relevant, sustainable and an effective part of its organisational culture.

Key points

- There is strong board and management commitment for risk management.
- Risk culture is positive and is assessed annually and benchmarked.
- A common and shared understanding of organisational purpose is evident.
- The value and role of risk management in decision making is well understood and applied.
- Staff are encouraged and supported to identify and escalate risks.

Overview

To assess its culture, the agency included specific questions on risk management in its staff opinion survey. These surveys are conducted annually. The commitment to measuring and reporting risk culture, together with a desire to use the information to benchmark against other agencies, supports an organisation’s culture described by one employee as ‘risk intelligent’.

The agency requested we conduct a risk maturity assessment to further understand its risk maturity, including its risk culture. The review was able to validate:

- a shared and common understanding of the agency's purpose, key functions, programs and improvement initiative
- a shared view that risk management is an important discipline and management tool used in planning and decision making throughout the agency
- that staff reported they were encouraged and supported to identify and raise risks
- that a central risk team supported the risk management function
- evidence of continuous and rigorous risk discussion by the executive and directors.

To further develop its risk culture, the agency also invested in a Risk Champion Model. Risk champions are mid-level managers selected across the organisation to be conduits for the business by informing and managing the risk profile.
Risk appetite

Risk appetite refers to the type and amount of risk that an agency is prepared to accept or avoid. It encourages the consideration of risk in strategic and tactical decisions by asking: “Is this course of action compatible with our risk appetite?”

In the case of Government an agency’s risk appetite statement is the shared view of the Responsible Body and executive management on the nature and amount of risk it will retain or accept to achieve its strategic objectives.

The risk appetite statement influences and guides decision making, clarifies strategic intent and ensures choices align with the capacities and capabilities of the agency. It supports a shared understanding of:

- opportunities and uncertainties
- what type of risk to pursue
- how much risk to accept
- what risk can be tolerated
- investment required.

Mandate, legislative requirements and stakeholder expectations affect how much risk an agency can accept. Expectations should be set by the Responsible Body and agreed with the executive. The executive communicates expectations to ensure monitoring, reporting and reviewing occurs.

Defining risk appetite will:
- focus on what is important to the agency
- develop a shared view of risk
- promote risk-based decision making
- improve oversight and monitoring.

A risk appetite statement supports:
- defining new initiatives and project priorities
- corporate and business planning and reporting
- investment and resource allocation.

Steps in determining risk appetite

A statement can be a high-level statement or include expectations for particular risks.

1. See Appendix C and D for an example of a risk appetite statement and steps for determining one.

Practical tips

Things to consider for risk appetite:
- What does risk appetite mean for your agency?
- Why would risk appetite add value?
- Who needs to set the expectations and accountability?
- How can it be included into the governance, framework and process?
- When should decisions about risk appetite be made and communicated?

Develop
- design statement to suit the agency
- define against key strategic objectives
- clear statements for decision makers.

Communicate
- set the tone for risk management
- ensure risk criteria reflects risk appetite and tolerances.

Monitor
- include in risk reporting
- review and adjust as the internal and external environment changes
- incorporate into continuous improvement activities
- utilise internal audit to review.
The risk management process is a core component of the risk management framework. Having a documented risk management process is important as it will outline the steps about how to:

- establish the context
- understand what is uncertain and potential effects
- identify and assess what could happen
- make a decision about what needs to occur.

Key steps of a risk management process

Establish the context

This step is essential to determine:

- the objective(s) being achieved
- why and what type of risk assessment is required
- what information is required to understand the risk – both internal and external
- what subject matter experts should be consulted.

Practical tip

When undertaking the risk process an agency should:

- Make sure the establish the context step is not missed. This step provides value to the process as it is where the alignment, planning, understanding and preparation occur.
In practice, there are essentially two ways the risk process occurs in an agency:

<table>
<thead>
<tr>
<th>Informal risk management process</th>
<th>Formal risk management process</th>
</tr>
</thead>
<tbody>
<tr>
<td>A formal documented risk assessment process has not occurred but the risk is considered and some action may be taken. Informal risk management process may occur during day-to-day activities where there is some uncertainty that may affect what the agency is trying to achieve.</td>
<td>A coordinated approach where the steps of the risk management process are followed and applied. This can occur in a structured discussion, workshop or meeting and can often be facilitated. It will result in risk(s) being recorded and actioned with an owner, time frames, reporting and monitoring.</td>
</tr>
<tr>
<td>The following may occur:</td>
<td>A formal risk assessment may occur for:</td>
</tr>
<tr>
<td>• Discussions of potential future risks of concern are discussed either with a manager or colleague and this leads to a change to a work practice or process.</td>
<td>• defined objectives important to the successful execution of an agency's strategy and operations (included as part of the corporate and business planning activities)</td>
</tr>
<tr>
<td>• Discussions of a potential future risk of concern occur and specialist expertise is sought.</td>
<td>• projects</td>
</tr>
<tr>
<td>• Discussions occur where there has been a change in the context or environment and there may be heightened monitoring of the situation.</td>
<td>• new services and/or products</td>
</tr>
<tr>
<td>• A trend in incidents is identified and there may be a need to assess the potential for a risk to an objective emerging.</td>
<td>• Government initiatives or policy directives</td>
</tr>
<tr>
<td>• Discussion of an emerging issue or risk is escalated and considered for formal assessment.</td>
<td>• change in the agency's mandate or requirements</td>
</tr>
<tr>
<td>• A standard meeting agenda item could include identification of potential risks or emerging issues for discussion and/or action, which could include escalation.</td>
<td>• identified problems that require further assessment and/or analysis</td>
</tr>
<tr>
<td></td>
<td>• inter-agency matters, agreements or requirements</td>
</tr>
<tr>
<td></td>
<td>• State significant or whole-of-Government operations.</td>
</tr>
</tbody>
</table>
Risk assessment
This step includes:
• risk identification
• risk analysis
• risk evaluation.

Risk identification
Risk identification defines the “risk” problem and provides insight into “uncertainty” and the possible effect on the achievement of objectives.

A well-described risk is important to provide context and meaning of the cause, event and impact for management and oversight. Key reasons are that it will:
• assist to direct controls assessments and treatment planning
• provide meaningful information for reporting and oversight
• reduce over or under investment in unnecessary controls
• align the uncertainty to an objective(s).

Risk will have a source and the following are the three key elements of a risk:

<table>
<thead>
<tr>
<th>Option 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cause</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event</strong></td>
</tr>
</tbody>
</table>

Describing a risk can be challenging and may take multiple attempts and a lot of discussion to agree on the risk.

Breaking the risk up into three elements helps to:
- Identify the cause of the event to help determine what controls would be required
- understand the “something” that could happen to consider the possible impact
- explore the potential impacts of the event to inform what decision is required.

Some agencies also describe a risk as an “event”. When describing the risk as an event it is helpful to consider how a post-event analysis would be conducted for the risk being described.

Practical tips
For describing risks:
- It is helpful to test the risk description with a person who is not the risk owner. This will help to ensure it can be understood and that it is describing the actual problem.

See Appendix F for a sample risk description and informal assessment example.

Common pitfalls
There are some common pitfalls in relation to describing a risk. For example an agency may:

- **Identify risks as broad statements.** Broad statements are less informative and difficult to manage at both an operational strategic level.

- **Identify risks as a cause.** A cause contributes to a risk event occurring, rather than the risk itself. Articulating risks in this manner hinders the effectiveness of monitoring and measurement activities.

- **Identify risks as incidents.** Incidents are risks that have materialised. Treatment plans would be focused on managing the incident rather than preventing the incident from occurring again.

- **Identify risk as consequences.** Consequences may be measurable but cannot be managed effectively as they do not represent a specific “risk event”.

- **Identify a risk as a “type” of risk.** For example Occupational Health and Safety or Information Technology.

*The term “impact” has been used to simplify guidance for risk identification. It is referred to as “consequence” in AS/NZS ISO 31000.
Risk analysis and evaluation
These are separate steps in the process but are usually undertaken together.

Analyse to:
- identify source and cause
- assess current controls, effectiveness and determine gaps
- consider how likely are/what are the impact(s)
- determine the risk rating = likelihood x impact (consequence).

Evaluate to:
- escalate to necessary reporting levels
- prioritise risks
- consider options
- decide what action is required
- identify resources required.

Practical tips
For risk identification:
- Ensure there has been robust discussion about a risk. This is valuable particularly where some things are uncertain.
- Include someone with knowledge or expertise of the risk to reduce uncertainty.
- Refer to the objective to ensure there is a focus on what is important.
- Identify dependencies with other agencies as these can lead to identifying shared risks.
- Identify and consider the risks associated with not pursuing an opportunity.

For a risk analysis and evaluation:
- Rate the risk based on current controls and their effectiveness
- Analyse the risk against the range of risk categories to determine potential impacts
- Assess risk against all categories of risk to determine most appropriate rating
- Determine option – avoid, share, reduce, accept.

Controls
A control is:
"measure that is modifying risk – controls include any process, policy, device, practice or other actions which modify risk. Controls may not always exert the intended or assumed modifying effect."
AS/NZS ISO 31000:2009

Controls influence how a risk is rated. A risk may be rated too high or too low based on how the control is viewed, its effectiveness or in the absence of a control.

Understanding the control environment is an essential part of the risk process. The risk owner is the best person to provide a view of the control. Specialist expertise may be required to support and validate this view.

Controls are important because an agency cannot operate effectively without appropriate governance, structure, processes and procedures. Every agency will have controls to govern and guide the way it operates and delivers its services.
Some common controls include:

- legislation
- delegations
- committees
- reporting
- policies, procedures, guidance material
- qualifications
- credentialing
- insurance
- employment screening
- training and required learning
- OHS representatives, champions, other representatives
- position descriptions
- values and behaviours, code of conduct
- audit, reviews, investigations
- equipment, devices, infrastructure
- checklists, templates.

A new agency would need to establish its governance and control environment and many of the controls would be established due to legislative or regulatory requirements. Controls are generally the responsibility of risk owners and would include their oversight and implementation.

When analysing and evaluating a risk, consideration is given to the specific controls that are currently in place that would modify the risk.

Considering both the design and operating effectiveness of controls is a critical aspect of the risk management process.

Multiple controls may exist and some will be more important or effective than others. Failure of controls could lead to an event.

Key fundamental questions to consider are:

- What are the current control(s) in place that would modify this risk?
- Why is this control important in modifying this risk?
- How effective is the control at modifying this risk?
- Who is going to assess whether the control is effective?

Where there are multiple controls, it is important to identify the important ones or the ones that are critical. This is important to help make a decision about what action is required or about additional investment.

Each agency should have its own control effectiveness rating approach to guide the process and how controls should be rated. This should be supported by an internal audit program that is aligned to the risk register and risk plan.

A simple approach is assessing whether the control is:

1. effective
2. partially effective
3. ineffective.

After the controls have been identified, assessed and rated, a decision can be made as to whether additional controls are required.
Practical tips
As a guide to controls consider the following:

- Controls that cannot be rated and are important should be assessed by a subject matter expert.
- Identifying key controls will prioritise risk treatments and support decisions on investment.
- Undertaking a cost benefit analysis of controls helps to identify over or under investment.
- Controls rated as effective do not guarantee the risk will not occur.
- Design of controls varies and they can be preventative, detective and/or monitoring.

Management assumptions about the strength of internal control can influence the risk profile. Assumptions should be tested to improve the design and/or effectiveness of internal control.

Risk treatment
Risk treatment is the action taken to manage the risk. A risk treatment is not required for every risk. It is a decision made during evaluation.

Treat to:
- reduce the likelihood and/or impact
- describe what action is required to modify controls or develop a new one
- determine target risk rating
- assign responsibility and ownership
- define timeframes and reporting.

Common issues with controls are:
- defects
- they deteriorate over time
- there is uncertainty with the assumption when the controls were designed
- changes in the environment in which the controls operate.

For risk treatment:
- Allocate a risk owner.
- Assess what additional controls are required to modify the risk.
- Ensure additional controls are operating as intended before re-assessing.
- Consider additional treatments if current ones are not effective.
- Document the treatment plan and progress.
Monitor and review
Monitor and review is an essential ongoing component of the risk process as it will:
• detect any changes to the internal and external context
• identify emerging risks
• measure performance of risk treatments
• provide oversight and governance of risks and treatments
• assess if the risk has changed and requires escalation, or is no longer valid and can be archived from the risk register.

Communicate and consult
Communicate and consult occurs throughout the process in various forms as it will:
• support stakeholder engagement and accountability in the process
• include the right people to help to reduce uncertainty
• provide information and reports to relevant stakeholders
• create opportunities to collaborate, advise and provide expertise to assist the process
• increase awareness of risk management and its value
• improve the decision-making process.

A template is provided with this guide.

Practical tips
For monitor and review:
► Develop an approach to identify and assess issues that may influence a risk.
► Ensure additional controls are operating as intended before re-assessing.
► Consider additional treatments if current ones are not effective.
► Seek feedback on the quality of risk reporting and adjust as required.
► Undertake cost benefit analysis of controls to ensure optimal investment is occurring.
► Identify risks that can be archived during the review process.
► Ensure appropriate linkage to continuous improvement and auditing systems for sustained monitoring and improvement.

Practical tips
For communicate and consult:
► Develop approach and document it.
► Decide what should be communicated and to whom.
► Create a stakeholder communication plan if relevant.
► Identify expertise required to provide advice about a risk.
► Nominate experts or owners to provide context on the risk.
► Advise outcomes and seek feedback.

Risk Categories
A risk category helps to classify a “type” of risk. This makes it easier to understand the context of the risk and develop a profile of risks of the agency. Each agency should decide what risk categories make sense to its context and operations.

Common risk categories are:
• Financial
• Safety
• People
• Legal and compliance or regulatory
• Reputation
• IT
• Governance
• Clinical.

These categories of risk are generally called “operational” risks.

Operational risks reflect day-to-day business activities.

Risk criteria
Risk criteria define appetite for categories of risk. Risk criteria should be used in the decision-making process to develop a shared understanding about how much risk, the type of risk and amount of risk an agency wants to accept for its objectives, projects or initiatives.
Risk profile

This is a term used to describe the nature and severity of risks the agency is facing. The profile may be:

- **Simple** – a summary of the risk categories.
- **Detailed** – a summary of the risk categories and detail of the risks in those categories.

Strategic risks

Strategic risks are generally risks that relate to the corporate objectives of the agency. They tend to be longer term and/or are of strategic importance and can impact the strategic intent of the agency. It is possible for some operational risks to be of strategic importance and be classified as strategic.

Strategic risk assessment

Given the mandatory requirement to incorporate risk management into corporate and business planning, an example of a three-phased approach to undertake a strategic risk assessment is provided.

The same approach can be adopted at the business and/or divisional level. The key difference is that stakeholders and risk categories may change. Business/divisional risks need to align to the strategic objectives.

Practical tips

As a guide to undertaking a strategic risk assessment:

- Ensure top down agreement for the approach.
- Incorporate it as part of the annual planning cycle.
- Develop necessary processes and procedures.
- Develop and communicate expectations to participants.
- Engage a person with relevant skills to facilitate it.
- Provide all pre-reading and information well in advance.
- Estimate time frames and develop a simple action plan to guide the process.
- Assign actions and follow up arrangements post session.
- Ensure risk owners are available to talk to their risk.
- Communicate outcomes and agreement.
- Consult effectively, particularly with key identified stakeholders.
- Report and monitor outcomes.
- Determine approach for survey and identify questions.

See Appendix E.

Risk register

A risk register is used to record risks and provide information to manage them. It can be a spreadsheet or form part of a software application. The following are the key elements that should be included in a risk register:

- risk number and description including the cause of the risk
- category
- controls
- effectiveness of controls
- likelihood rating
- impact (consequence) rating
- current rating
- change to previous risk rating
- responsible person/owner
- status of treatment plan.

Practical tips

For a risk register:

- describe risks so that they are meaningful
- review risks regularly and archive risks that no longer require active treatment
- consider how many risks can reasonably be managed by each risk owner
- determine which risks are really important
- manage access to maintain the integrity of the content.
Inter-agency and State significant risks

Some inter-agency risks could become State significant or have some Statewide implications.

Inter-agency and State significant risks are essentially a “category” of risk. The normal risk assessment approach should be applied. If the process has to be adapted differences may include:

- A higher degree of uncertainty due to the nature and complexity of the risk problem.
- Solutions may be required that involve multiple parties and entities.
- Time frames may be longer term particularly for State significant risks.
- Scale may be beyond normal thresholds and may require different consideration.
- Interdependencies may not be clear or change over time.

Inter-agency and State significant risks are typically shared by two or more agencies where a shared objective or a key dependency exists.

Formal or informal processes may be in place which could include executive forums, formalised partnerships and committees.

- Vulnerabilities may be different depending on service delivery requirements.
- Triggers may be different and require different management or indicators.
- Controls may be different depending on the context.
- Assurance arrangements and requirements may vary
- Escalation arrangements may extend beyond your agency.

These risks may to require an agency to:

- undertake detailed exploration and analysis
- seek support from an expert
- develop a specific approach to manage
- form a partnership and/or collaborate
- develop of a whole-of-Government response
- engage with private entities and the Commonwealth to develop strategies/solutions.
- establish joint monitoring and reporting
- gain consensus on the appropriate response
- determine ownership and accountability
- fund risk mitigation activities or treatments
- ensure agreed actions are undertaken by the respective agencies
- provide an aggregated summary of the risk to Government.

See Appendix G for key components to managing inter-agency and State significant risks.
Managing inter-agency risks

Practical tip
As a guide an agency should consider if further detailed analysis is required. Considerations include:
- source (drought, political, economic)
- likelihood (rare, unlikely, possible, likely, almost certain)
- threat to (biosecurity, infrastructure, life, social cohesion)
- triggers (endemic virus, rising water, increased incidents)
- vulnerabilities (vulnerable group of the population, assets, systems)
- dependencies (infrastructure, food source, industry, essential service)
- scale, range and dimension (breadth of effects, number agencies, whether confined to Victoria or interstate/international)
- speed of onset (whether it is emerging, imminent or longer term)
- stakeholders (agencies, community, sector, local Government).

Case study of an inter-agency response: a regional hospital and local TAFE
A regional hospital and local TAFE acknowledge a number of key inter-dependencies. These include reliance on:
- a critical workforce supply
- training opportunities
- collaborative funding initiatives.

A workshop is held to identify shared objectives and what actions each agency will take to manage the shared risk. A key action is the formation of a bi-monthly committee to discuss and monitor these risks. To support communication, a formal Memorandum of Understanding is documented to acknowledge interdependencies, maximise resources and to provide clarity of roles and responsibilities. To ensure governance and oversight, each agency reports the progress of the risk treatments to the bi-monthly committee and to their respective risk committees.
Managing State significant risks

Practical tips
As a guide an agency should consider if further detailed analysis or research is required before a decision is made where gaps in information or knowledge exist.

Other considerations include:
- Coordination and management of the response may require a lead agency or a whole-of-Government initiative. Collaboration with other agencies, local, community and national bodies could be required.
- Arrangements may need to be documented between respective agencies. Depending on the requirements this could take the form of an agreement, memorandum of understanding or joint plan. The following can be considered as a guide for inclusion:
  - roles, responsibilities and accountabilities
  - escalation protocols
  - actions required by respective agencies
  - monitoring and oversight arrangements
  - reporting including agency and aggregated reporting
  - oversight and assurance requirements
  - risk indicators and/or performance measures
  - funding arrangements and submissions for additional funding.
- Governance arrangements may need to outline escalation protocols to the appropriate Government body.

Case study of a Statewide response: Emergency Management Victoria

A statewide response is the creation of Emergency Management Victoria (EMV). EMV is the over-arching body which supports and enables the Emergency Management Commissioner (EMC) to fulfil his role.

EMV plays a key role in implementing the Government's emergency management reform agenda. This work will drive how Victoria's emergency services organisations train together, work to common operating standards, share the same operational picture, and use equipment and systems that work together.

Maximising the ability of the emergency management agencies to work together and share resources is a key function of EMV. This will occur through strengthening the working relationship between the Government and statutory response agencies without compromising their individual identities and strengths.

Managing risk is everyone’s responsibility. Effective risk management requires resources. It is now a mandatory requirement to allocate adequate resources to risk management. This means considering what is required to satisfy the agency’s obligations and accountabilities.

An agency will need to make a decision regarding what constitutes adequate investment based on its mandate, size, complexity, services and level of risk maturity.

An agency that does not have a dedicated resource for its risk management function will need to consider how it can effectively meet its obligations and deliver its services. It will need to determine who will be responsible at the executive and manager level for the risk management functions and how it will be monitored and improved.

The risk management function is most effective when it has independent oversight of the risk profile and risk management framework. The risk management function should:

- assist the Responsible Body, committees and senior management to develop and maintain the risk management framework
- tailor it to be the right size for the agency
- ensure there are reporting lines to conduct its risk management activities
- define roles, responsibilities and authorities
- ensure staff possess the appropriate experience and skill
- provide access to required areas of the agency
- require notification and escalation of matters of concern or that deviate from the agreed approach
- create a level of independence to support the three lines of defence and overall governance.

### Practical tips

As a guide to assessing resources an agency should consider whether:

- adequate resources are committed in budgets for its:
  - risk management framework
  - improvement plan activities
  - corporate and business planning
  - risk management function
  - risk culture development
  - people and tools
  - inter-agency and State significant risks
  - controls and assurance
- capability requirements are assessed and programs are established to support development
- role of the risk management function is well defined, has influence and supports improvement
- tools, templates, guidance and support is available and easily accessible.
INSURANCE

We provide insurance products specifically for Government – delivering broad cover at low cost – helping to protect important assets and services.

Departments or participating bodies must arrange all insurance with us unless:

- exempted by the Minister for part or all risks
- we have formally declined or cannot offer insurance for a specific risk.

An agency must have appropriate insurances in place that reflect its risk profile. Portfolio departments are accountable for providing oversight of their agencies.

Insurance does not prevent something from occurring. If something unexpected does happen insurance means an agency won’t have to fund the full cost of the loss. The community benefits from an agency being able to recover financially and it minimises the impact on consolidated revenue.

Not all risk can be covered by insurance as there are many risks that do not have a direct financial impact and alternative risk management strategies would be required.

Risk-based decisions can also be made not to insure a risk, where a cost benefit assessment determines insurance is not the best option.

We can help to determine appropriate insurance programs. Key factors to consider include:

- type, scale and nature of risk
- what risk the agency is prepared to accept
- availability of alternative risk management and mitigation strategies
- level of insurance required based on your objectives, risk profile and tolerance
- past claims experience
- availability and cost of cover.

Agencies are responsible for managing and funding any self-insured and under-deductible losses. This means an agency will need to determine:

- the loss the agency is able to manage and fund (often referred to as a deductible)
- the number of losses the agency is able to manage and fund any given policy year
- capability to manage claims and appropriately reserve for losses.

Important points to note:

Insurance may be a viable cost effective option to reduce the financial impact for the agency if the risk occurs. Insurance should not be the only option.

- Preventative or mitigating strategies should be considered to reduce the likelihood and/or impact.
- Provide a cost benefit analysis of potential actions.

Risks that cannot be insured should be included as part of the risk management framework.
A Responsible Body should:

- ensure the agency considers all insurable risks and is insured appropriately
- determine the appropriate level of insurance based on consideration of the agency's risk profile
- ensure that a current register of insurance and indemnities is maintained
- ensure that the financial impacts of any indemnities have been adequately assessed and align with the agency's risk appetite
- ensure that the valuation basis for valuation of self-insured retained losses is recorded
- be satisfied that adequate claims management capability is maintained where the agency manages below deductible claims
- ensure required below deductible claims data is provided to VMIA.

Claims management

- We can manage below deductible claims on your behalf.
- The default position is to use us to manage below deductible claims.
- When an agency manages its own claims, it should ensure it is appropriately resourced to manage them effectively.
- Below deductible claims have to be provided to us for self-managed claims greater than $10,000, related to third-party liability and employment claims (excluding WorkCover claims).

We cover:

- **Aviation**
  - Aircraft loss or damage and third party liability

- **Business Travel**
  - Covers employees on business trips

- **Construction Risk**
  - Damage and liability during construction projects

- **Cyber Liability**
  - Legal liability from actual or alleged breaches of an agency's data and corporate information

- **Director's & Officers Liability**
  - Claims against agencies' directors and officers

- **EmRePSS**
  - Emergency service providers

- **Fine Art Exhibitions**
  - Damage and loss of artworks and property

- **Industrial Special Risks**
  - Loss and damage of business property

- **Journey**
  - Cover for employees travelling between home and work

- **Medical Indemnity**
  - Covers healthcare providers and rural GPs

- **Motor Vehicle**
  - Damage to motor vehicles and third-party property

- **Personal Accident**
  - Cover for volunteers in agencies

- **Professional Indemnity**
  - Alleged breaches of professional duties

- **Public and Products**
  - Injury and property damage to third parties

Standing Direction of the Minister for Finance 4.5.5.1

Agencies required to insure with us must attest as part of the annual insurance renewal process.

- Claims data should be provided annually as part of the insurance attestation process.
- We may also request details of other self-managed claims which must be provided in our prescribed format.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable Officer</td>
<td>In relation to a department of public body, means the accountable officer for that department or public body as determined under section 42 of the Financial Management Act 1994.</td>
</tr>
<tr>
<td>Agency</td>
<td>Any department or public body as defined in the Financial Management Act 1994.</td>
</tr>
<tr>
<td>Agency required to insure with the VMIA</td>
<td>A Department or participating body as defined in section 3 of the Victorian Managed Insurance Authority Act 1996.</td>
</tr>
<tr>
<td>Agency-specific risks</td>
<td>Risks that can be managed entirely within a single agency's operations and can generally be well understood and effectively managed with straightforward risk management processes.</td>
</tr>
<tr>
<td>Audit committee</td>
<td>The Standing Directions of the Minister for Finance state that an audit committee is appointed to oversee and advise the department or agency on matters of accountability and internal control. The committee is a subset of the Responsible Body (or Board) which has been formulated to deal with issues of a specific nature.</td>
</tr>
<tr>
<td>Australian/New Zealand Risk Management Standard</td>
<td>AS/NZS ISO 31000:2009. The Standard provides principles and generic guidelines about risk management, and can be applied to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.</td>
</tr>
<tr>
<td>Consequence</td>
<td>Is the outcome of an event and has an effect on objectives.</td>
</tr>
<tr>
<td>Control</td>
<td>Measure that is modifying risk.</td>
</tr>
<tr>
<td>Formal risk management</td>
<td>Occurs where the steps of the risk management process are followed and applied.</td>
</tr>
<tr>
<td>Informal risk management</td>
<td>Occurs when a formal documented risk assessment process has not occurred but the risk is considered and some action may be taken.</td>
</tr>
<tr>
<td>Inter-agency risks</td>
<td>Risks shared by two or more agencies that require coordinated management by more than one agency and may include systemic risks. The responsibility for managing and inter-agency risk is shared by all the relevant agencies and will benefit from a coordinated response where one agency takes a lead role.</td>
</tr>
<tr>
<td>Responsible Body</td>
<td>For a department, the accountable officer is the Responsible Body. For other agencies, it is the board or the person or body with ultimate decision making authority.</td>
</tr>
</tbody>
</table>

1 Department of Treasury and Finance, Victorian Government Risk Management Framework – Definition page 22
2 Ibid
3 Department of Treasury and Finance, Victorian Government Risk Management Framework, page 16
4 Ibid
5 AS/NZS ISO 31000:2009
6 AS/NZS ISO 31000:2009
7 Ibid
8 Department of Treasury and Finance, Victorian Government Risk Management Framework – Definition page 22
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk appetite</td>
<td>Refers to the type and amount of risk that an agency is prepared to accept or avoid.</td>
<td>Department of Treasury and Finance, Victorian Government Risk Management Framework – Other risk terms page 19</td>
</tr>
<tr>
<td>Risk criteria</td>
<td>Terms of reference against which the significance of a risk is evaluated.[^10]</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk culture</td>
<td>Refers to the behaviours that lead to how every person thinks about and manages risk.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk evaluation</td>
<td>Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk governance</td>
<td>Refers to the culture and arrangements developed by an agency to manage the uncertainties to achieving its objectives.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk identification</td>
<td>Defines the ‘risk’ problem and provides insight into ‘uncertainty’ and the possible effect of this on what is trying to be achieved.</td>
<td>Department of Treasury and Finance, Victorian Government Risk Management Framework – Other risk terms page 19</td>
</tr>
<tr>
<td>Risk management</td>
<td>Coordinated activities to direct and control an organisation with regard to risk.[^11]</td>
<td>AS/NZS ISO 31000:2009</td>
</tr>
<tr>
<td>Risk management framework</td>
<td>Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk management plan</td>
<td>Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk management policy</td>
<td>Statement of the overall intentions and direction of an organisation related to risk management.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk management process</td>
<td>Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk management strategy</td>
<td>Describes an agency’s future vision, direction and objectives for risk management. It incorporates key activities designed to achieve these objectives and the plan to build risk management capability and maturity.</td>
<td>Ibid</td>
</tr>
<tr>
<td>Risk profile</td>
<td>A description of any set of risks. The set of risks can contain those that relate to the whole agency or part of the agency.</td>
<td>Department of Treasury and Finance, Victorian Government Risk Management Framework – Other risk terms page 19</td>
</tr>
</tbody>
</table>

[^9]: AS/NZS ISO 31000:2009
[^10]: Department of Treasury and Finance, Victorian Government Risk Management Framework – Other risk terms page 19
[^12]: Ibid
[^13]: Ibid
[^14]: Ibid
[^15]: Department of Treasury and Finance, Victorian Government Risk Management Framework – Other risk terms page 19
Risk register  
Record of information about identified risks.

Risk tolerance  
The agency’s readiness to bear the risk after risk treatment in order to achieve objectives. Risk tolerances are based on the maximum level of acceptable risk and may be expressed in various ways depending on the nature of the risk.\textsuperscript{16}

Risk treatment  
Process to modify risk, it can involve: avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk, taking or increasing the risk in order to pursue an opportunity, and/or removing the risk source.

Stakeholder  
Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.\textsuperscript{17}

State significant risks  
Risks where the potential consequences or impacts of the risk on the community, the Government and the private sector are so large as to be of State significance.\textsuperscript{18}

\textsuperscript{16} Department of Treasury and Finance, \textit{Victorian Government Risk Management Framework – Other risk terms} page 19
\textsuperscript{17} AS/NZS ISO 31000:2009
\textsuperscript{18} Department of Treasury and Finance, \textit{Victorian Government Risk Management Framework – Other risk terms} page 17
Appendix A | Risk management framework components

**Mandate and Commitment**

**What is it?**
It reflects the intent to ensure effective risk management.

**Why is it important?**
It provides the basis for a common and consistent approach.

**How is it evident?**
When commitment to risk management is strong and supports a positive risk culture.

**Typically this would be reflected in:**
- mission and values statements
- by-laws and/or charters
- policies
- position descriptions
- staff recognition programs
- continuous improvement plans.

**The agency would:**
- endorse the risk management policy
- ensure a positive attitude towards risk management
- review regularly the effectiveness of its risk management.

---

**Design**

**What is it?**
It reflects what is required and what should be included.

**Why is it important?**
It considers context, requirements, and components.

**How is it evident?**
Design of the framework enables a systematic and structured approach.

**Typically this would be reflected in:**
- risk management procedures
- governance structure
- risk management policy
- by-laws and/or charters
- terms of reference of committees
- communication and consultation plans.

**The design of the framework takes into account:**
- internal and external factors
- accountability and responsibility for managing risk
- integration into corporate and business planning
- communication and reporting mechanisms.
Appendix A | Risk management framework components

**Implementation**

**What is it?**
It reflects what actions are required to make it real.

**Why is it important?**
It ensures planned activities occur and are resourced.

**How is it evident?**
Implementation and integration the risk management framework supports risk-based decision making across the agency.

**Typically this would be reflected in:**
- risk management strategy
- project documentation
- risk management policy
- maps of the decision-making process
- corporate and business plans
- minutes of committee meetings
- budgeting and planning processes
- procedure manuals associated with management systems
- risk management training systems
- internal audit and assurance systems.

**The agency would:**
- develop a risk management strategy to support integration
- identify its requirements for building capability
- review its progress
- report outcomes
- re-assess post implementation.

**Monitor and review**

**What is it?**
It reflects the approach required to assess performance.

**Why is it important?**
It ensures effective and fit for purpose.

**How is it evident?**
Monitoring and reviewing the risk management framework continuously ensures it is effective and supports performance.

**Typically this would be reflected in:**
- control effectiveness assessments
- a risk treatment plan
- risk management policy
- terms of reference of committees
- performance templates
- risk management KPIs
- minutes of committee meetings
- internal and external audit plans.

**The agency would:**
- assess its risk management framework at least annually
- monitor progress against the risk management strategy
- implement enhancements as required.
Appendix A | Risk management framework components

**Continual improvement**

*What is it?*
It reflects the continual improvement process.

*Why is it important?*
It ensures it is dynamic and aligns to requirements.

*How is it evident?*
Implementing a risk management improvement plan continuously enhances risk management and risk.

Typically this would be reflected in:
- a risk management improvement plan
- a risk attestation statement
- risk management policy
- minutes of committee meetings
- an agency-wide quality improvement plan
- performance templates
- risk management KPIs
- control effectiveness assessment reports
- audit reports.

The agency would:
- develop a risk improvement plan
- incorporate improvement activities in its quality cycle
- measure improvement through monitoring and assurance.
## Appendix B | Three lines of defence model

<table>
<thead>
<tr>
<th>First line: Management control</th>
<th>Second line: Risk control and oversight functions established by management</th>
<th>Third line: Independent assurance</th>
</tr>
</thead>
</table>
| Controls are designed into systems and processes under managerial guidance. | Risk management function (and/or committee) facilitates and monitors the implementation of effective risk management practices in the following way:  
  - supports management policy  
  - monitors risk management and provides guidance and support  
  - assists risk owners and management  
  - identifies and alerts management to shifts and emerging issues  
  - monitors specific risks, adequacy of internal control, reporting, compliance  
  - assists in the development of processes and controls | Internal audit is established to provide the Responsible Body and senior management with assurance around:  
  - Effectiveness of governance and risk management  
  - Internal controls  
  - How first and second line of defence is operating  
  - Assessment of control objectives and plans. |
| Adequate managerial and supervisory controls are required to ensure compliance and to identify breakdowns or unexpected events. | Designed to ensure the first line of defence is operating as intended. | **External auditors, regulators and external bodies**  
Those entities outside the structure of the agency but who play an important role in the overall governance and control structure. |
| Operational managers are responsible for:  
  - owning and managing risk and guiding development of internal policies and procedures and ensuring activities consistent with objectives  
  - implementing corrective actions to address process and control deficiencies  
  - maintaining effective internal controls  
  - executing risk and control procedures on a day-to-day basis. |  
Mid-level managers design and implement detailed procedures that serve as controls and supervise execution of those procedures. |  
Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41 |
## Appendix C | Risk appetite statement – example

<table>
<thead>
<tr>
<th>Corporate objective</th>
<th>Risk category</th>
<th>Risk appetite statement</th>
<th>Benchmark</th>
<th>Risk tolerance range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure financial sustainability of the service</td>
<td>Financial</td>
<td>A <strong>low appetite</strong> for financial volatility and desire to carefully control costs. We operate within the approved budget expenditure limit of ≤5.0%.</td>
<td>Annual board-approved budget</td>
<td>1.0% – 2.5% 2.5% – 5.0% &gt;5.0%</td>
</tr>
<tr>
<td>Become an employer of choice in our sector</td>
<td>Human Resources</td>
<td>A <strong>moderate appetite</strong> for applying new approaches to ensure we remain an employer of choice in our sector, while maintaining safety and service levels. We will do this by: • maintaining an annualised staff turnover rate of 15% or less over a rolling 12-month period. • ensuring our rate of staff absenteeism remains at ≤3% in each month. • less than five accepted workers’ compensation claims annually.</td>
<td>Median staff initiated turnover rate for public sector agencies</td>
<td>≤15% 15% – 17% ≥17%</td>
</tr>
<tr>
<td>Provide services and products to enhance our clients’ capacity</td>
<td>Service Delivery</td>
<td>A <strong>low appetite</strong> to lose a valued position of trust with our clients. We will maintain a level of client engagement of at least 85%. A <strong>moderate appetite</strong> to innovate through projects and R&amp;D to benefit our clients. We accept that 10% of project effort may not result in immediate or direct client benefits as long as lessons are learned for future services and products.</td>
<td>Board-approved minimum level</td>
<td>≥85% 75% – 80% ≤75%</td>
</tr>
<tr>
<td></td>
<td>Projects</td>
<td></td>
<td>Annual board-approved budget</td>
<td>≥10% 10% – 20% &gt;20.0%</td>
</tr>
<tr>
<td>Maintain high levels of information governance, security and accountability</td>
<td>Information Management &amp; Legal Compliance</td>
<td>A <strong>very low appetite</strong> for information security breaches, frauds or proven ethical complaints. We maintain a zero tolerance for such events.</td>
<td>Government Information Security Policy Standard, Compliance Standard</td>
<td>0 instances 0 instances</td>
</tr>
</tbody>
</table>
## Appendix D | Steps in determining risk appetite

<table>
<thead>
<tr>
<th>Develop</th>
<th>Communicate</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify key stakeholders who need to contribute to the development of the risk appetite statement (e.g. Board, Executive, Risk Manager).</td>
<td>1. Identify key internal and external stakeholders who need to be aware and apply the risk appetite statement.</td>
<td>1. Confirm governance arrangements for oversight of the application and impact of the risk appetite statement.</td>
</tr>
<tr>
<td>2. Identify expectations of stakeholders and their general attitude to the risk profile and its capacity to bear the risks. Using surveys or event-based scenarios may assist with this.</td>
<td>2. Establish the preferred methods for communicating with each stakeholder group (e.g. memoranda, governance meetings, etc.).</td>
<td>2. Ensure adequate systems (technology) to facilitate monitoring, timely reporting and escalation when tolerances are exceeded.</td>
</tr>
<tr>
<td>3. Identify and agree on points in the business where key decision making is pivotal, so that risk appetite can be applied at those points (e.g. strategic planning, projects, organisational change, etc).</td>
<td>3. Establish the content and form of risk appetite communication (policy inclusion, memorandum, bulletin, poster, etc.).</td>
<td>3. Ensure corrective actions to address variations are identified and implemented and that progress is reported.</td>
</tr>
<tr>
<td>4. Identify how risk appetite performance will be monitored (e.g. key performance indicators).</td>
<td>4. Review risk criteria to ensure it reflects risk appetite and tolerances.</td>
<td></td>
</tr>
<tr>
<td>5. Identify the limits for each risk appetite statement (e.g. total annual loss is not to exceed 5% of budget or $50K).</td>
<td>5. Confirm that the performance of the risk appetite statement will be monitored by the Responsible Body.</td>
<td></td>
</tr>
<tr>
<td>6. Identify the thresholds for each risk statement, e.g. • acceptable = • tolerable = • unacceptable =</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Identify the specific events that will trigger a review of the risk appetite statement (e.g. breaches in limits, change in strategic direction, Government policy, legislative changes, etc).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix E | Strategic risk assessment

<table>
<thead>
<tr>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish the context</td>
<td>Risk identification</td>
<td>Assessment and treatment planning</td>
</tr>
</tbody>
</table>

### Review
- Risk management strategy and concepts to ensure there is shared understanding among stakeholders
- Review: Current risks to strategic objectives
- Review: Individual risks with risk owners

<table>
<thead>
<tr>
<th>Identify</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Strategic and operational priorities</td>
</tr>
<tr>
<td>- Emerging challenges</td>
</tr>
<tr>
<td>- Vulnerabilities and dependencies</td>
</tr>
</tbody>
</table>
- Gaps and additional risks
- Treatment options and establish a plan

<table>
<thead>
<tr>
<th>Agree</th>
</tr>
</thead>
</table>
- Roles and responsibilities for next phase
- Strategic risk profile
- Reporting and monitoring plan

### Key stakeholders include:
- Executive
- Risk team
- Possible board member

### Outcomes
- Context summary including a plan for phase 2
- Strategic risk profile for assessment and treatment planning in phase 3
- Validated strategic risks with treatment plans
Appendix F | Risk description examples

Example of a strategic risk
Objective: Supporting high-quality Government decision making and implementation

Risk description
An ineffective recruitment program (cause) leads to lack of policy expertise in key roles (event) resulting in sub-standard policy advice to Government (impact).

Example of an operational risk
Category: Human Resources
Objective: Improve staff capability to provide high-quality advice

Risk description
Poorly implemented learning management system (cause) leads to staff not completing required training (event) resulting in key skill gaps (impact).

Example of a project risk
Category: Information Management and Security
Objective: Upgrade learning management system to support increased capability requirements

Risk description
Ineffective subject matter expert identification (cause) leads to poor quality specification design for IM learning management system upgrade (event) resulting in product that doesn't meet user needs (impact).

Example of an informal risk assessment
Objective: What is it we are trying to achieve?
Provide new public infrastructure in a Melbourne growth corridor by the end of the year.

What would cause this risk to occur?
Late changes to specifications for the new infrastructure

What event would impact our ability to be successful in achieving our objective?
Designs and drawings are delayed

What potential impacts are there if the event occurred?
Delay in delivery of the new infrastructure and avoidable costs to the community

Example of a risk description:
Late changes to specifications for the new infrastructure (cause) leads to designs and drawings being delayed (event) resulting in delays in delivery of the new infrastructure and avoidable costs to the community (impact).
## Appendix G | Key components to managing inter-agency and State significant risks

<table>
<thead>
<tr>
<th>Governance</th>
<th>Framework</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequate governance to ensure clear accountability and oversight.</td>
<td>Integrate requirements into the risk management framework and supporting documentation.</td>
<td>Apply the risk process in consultation with relevant agencies.</td>
</tr>
<tr>
<td>This includes:</td>
<td>This includes:</td>
<td>This includes:</td>
</tr>
<tr>
<td>• Lead agency agreed</td>
<td>• Reflected in risk appetite statement</td>
<td>• Considered in environmental scanning for emerging issues/trends</td>
</tr>
<tr>
<td>• Roles, responsibilities are clearly defined and documented</td>
<td>• Documented in policies, procedure, templates</td>
<td>• Included as part of formal process for corporate and business planning</td>
</tr>
<tr>
<td>• Approvals/delegations, charters, committees are in place and reviewed</td>
<td>• Documented in risk escalation protocol</td>
<td>• Undertaken for projects or major initiatives</td>
</tr>
<tr>
<td>• Oversight, monitor, review, assurance established</td>
<td>• Defined in category of risks</td>
<td>• Discussed at meetings and minuted</td>
</tr>
<tr>
<td>• Reporting and escalation through to the Responsible Body are developed and applied</td>
<td>• Described in consequence table</td>
<td>• Defined in risk criteria</td>
</tr>
<tr>
<td>• Protocols, memorandum of understanding or agreements developed</td>
<td>• Included in treatment/action plans</td>
<td>• Described in consequence table</td>
</tr>
<tr>
<td>• Responsibility included in relevant position descriptions and featured in terms of reference for committee</td>
<td>• Included in risk improvement plans</td>
<td>• Included in treatment/action plans, initiatives</td>
</tr>
<tr>
<td>• Part of attestation process</td>
<td>• Escalation protocols developed and applied</td>
<td>• Developed treatment plans/action plans</td>
</tr>
<tr>
<td>• Ensuring agency can demonstrate how inter-agency and State significant risks are addressed</td>
<td>• Adequate resources allocated</td>
<td>• Demonstrated evidence of analysis assessment</td>
</tr>
<tr>
<td></td>
<td>• People have capability</td>
<td>• Communicating, collaborating, consulting</td>
</tr>
<tr>
<td></td>
<td>• Included in risk register, business continuity, incident register</td>
<td>• Monitoring, reviewing, reporting</td>
</tr>
<tr>
<td></td>
<td>• Agenda item and documented in minutes of meeting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Part of audit program and continual improvement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identified as part of research or data mining/analysis</td>
<td></td>
</tr>
</tbody>
</table>
Risk

- A1 Risk Management Glossary
- A2 Risk Management Policy Guide
- A3 Risk Management Communication Plan
- A4 Roles and Responsibilities
- A5 Risk Manager Role Description
- A6 Articulate Risk Appetite Tolerance
- A7 Risk Management – Board Reporting Template
- A8 Assurance Map Guide
- A9 Risk Management Attestation Checklist
- A10 Risk Management Strategy
- A11 Risk Register Guide
- A11 Risk Register Template
- B1 Categories of Risk
- B2 Risk Criteria Examples
- B3 Risk Assessment & Treatment Guide
- B4 Guide to monitoring and reviewing risks

Insurance

- Insurance register
- Indemnities register
- Incident and claims register
- Incident notification form
- Guide to managing indemnities