Department of **Treasury and Finance**

Victorian Government Risk Management Framework

March 2015

State Government Victoria

The Secretary
Department of Treasury and Finance
1 Treasury Place
Melbourne Victoria 3002
Australia
Telephone: +61 3 9651 5111
Facsimile: +61 3 9651 2062
dtf.vic.gov.au

Authorised by the Victorian Government
1 Treasury Place, Melbourne, 3002

ISBN 978-1-922222-46-6
Published March 2015

If you would like to receive this publication in an accessible format please email information@dtf.vic.gov.au
This document is also available in Word and PDF format at dtf.vic.gov.au

Contents

Foreword

In order to achieve its strategic objectives, the Victorian Government must be prepared for risk. We need our public sector to be productive, innovative and efficient. Planning for and engaging with risk is essential to a well-functioning public sector. It is the responsibility of agency leaders and all staff to think about and manage risk as part of their roles. Working together, they will better understand their risk profile and ensure the measures they take reflect sound planning and are supported by robust policies, systems and processes. This will build capability and reinforce an organisational culture that is focused on improving outcomes for Victorian communities.

As our public sector moves towards a more sophisticated, whole of government approach to service delivery, it is essential for agencies to be willing and confident to work with each other to tackle not only their own risks, but inter-agency and state significant risks as well. This needs to be the hallmark of joined-up service delivery.

It is timely we release this update to the Victorian Government Risk Management Framework. Originally issued in 2007, it has been updated to improve clarity on expectations and to reflect better practice, Australasian standards and contemporary approaches to risk management. It sets the baseline for what is needed in the public sector to meet the Government's expectation of risk management. Over time, we will strengthen the standards and lift the benchmark to improve public sector capabilities and performance.

The updated framework acknowledges that individual agencies have different levels of risk maturity that will evolve and improve over time. The Victorian Managed Insurance Authority will work with public sector agencies and provide the education, insight, advice and support needed to help agencies effectively manage risk.

I encourage Victorian public sector agencies to continue improving their risk management.

Robin Scott MP

Minister for Finance

1. Introduction

Management of risk must be an integral part of an agency's culture, reflected in policies, systems and processes. This includes strategic business planning, performance management and overall governance to ensure sound financial management and efficient service delivery.

Risks may affect only one agency or multiple agencies. Agencies must consider and implement appropriate risk management strategies, including working with other agencies to manage risk.

A systematic approach to risk management is critical as the public sector moves to a more sophisticated approach to the development and delivery of services.

The Minister for Finance has issued risk management and insurance standing directions under the *Financial Management Act 1994.* Legislative requirements and Government policies and procedures related to risk management include:

- *Financial Management Act 1994;*
- *Standing Direction of the Minister for Finance 4.5.5 – Risk Management Framework and Processes);*
- Insurance requirements under the *Victorian Managed Insurance Authority Act 1996*;
- *Insurance Management Policy and Guidelines for General Government Sector – September 2007*; and
- *Government Policy and Guidelines: Indemnities and Immunities – June 2008.*

1.1 Purpose

The Victorian Government Risk Management Framework (VGRMF) describes the minimum risk management requirements agencies are required to meet to demonstrate that they are managing risk effectively, including inter-agency and state significant risk. It outlines the role and responsibilities of an agency's responsible body. The VGRMF adopts the *Australian and New Zealand Standard AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines* which provides a generic, internationally accepted basis for best practice risk management.

The VGRMF is mandated by the *Standing Direction of the Minister for Finance (Ministerial Standing Direction) 4.5.5 – Risk Management Framework and Processes* and provides high level information for agencies and the responsible body.

Detailed guidance, information and risk management support is available from the Victorian Managed Insurance Authority (VMIA). The VMIA has an important role in supporting agencies in the implementation of the VGRMF.

1.2 Coverage

Under *Ministerial Standing Direction 4.5.5 – Risk Management Framework and Processes*, the VGRMF applies to departments and public bodies covered by the *Financial Management Act 1994*. All other agencies are encouraged to adopt the VGRMF to enhance their risk management practices.

2. Roles and responsibilities

2.1 Entities with specific roles and responsibilities under the VGRMF

2.1.1 All agencies

All agencies must fully comply with the requirements of *Ministerial Standing Direction 4.5.5* and are responsible for appropriately identifying, assessing and managing all risks to which they are exposed. Agencies should establish and maintain effective risk governance that includes an appropriate internal management structure and oversight arrangements for managing risk. The responsible bodies are directly accountable for their organisations' risk management obligations.

Under section 13 A of the *Public Administration Act 2004*, the department head (Secretary) has responsibilities for advising the portfolio Minister on matters relating to relevant public entities (as defined in the *Public Administration Act 2004*) and for working with and providing guidance to these public entities. Consistent with this role, department heads are expected to advise the portfolio Minister on any significant risks relating to the relevant public entities.

2.1.2 Agency audit committee

Under *Ministerial Standing Direction 2.2 - Financial Governance*, agencies must, unless an exemption has been obtained, appoint an audit committee to oversee and advise the public sector agency on matters of accountability and internal control affecting the operations of the agencies.

In relation to risk management the responsibilities of a department or agency's audit committee may:

- consider the agency's risk profile and insurance arrangements;
- review and assess the effectiveness of the agency's risk management framework;
- review, monitor and verify compliance with *Ministerial Standing Direction 4.5.5*; and
- report to the responsible body on the level of compliance attained.

2.1.3 Department of Treasury and Finance

The Department of Treasury and Finance (DTF) advises the Government on policies relating to risk management and insurance. DTF is responsible for maintaining and updating the VGRMF to ensure that it continues to be aligned with best practice. DTF monitors compliance with *Ministerial Standing Direction 4.5.5* through the annual attestation process and provides additional guidance on the DTF website at www.dtf.vic.gov.au.

2.1.4 Victorian Managed Insurance Authority

Under the *Victorian Managed Insurance Authority Act 1996*, VMIA's functions include assisting agencies in establishing programs for the identification, quantification and management of risks and monitoring risk.

VMIA has a support role to play in the implementation of the VGRMF through assisting agencies with technical expertise and advice on risk management best practice and standards. VMIA has legislative responsibilities in relation to public sector agencies under the Act, including:

- assisting to establish programs to identify, quantify and manage risks;
- monitoring risk management maturity and capability;
- providing risk management advice and training;
- advising the government on risk management; and
- acting as an insurer.

VMIA guides and supports agencies to apply the VGRMF by providing risk guidelines, training and support, risk maturity assessments and learning and development strategies.

2.2 Other entities with roles and responsibilities in public sector management

2.2.1 Victorian Secretaries Board

The Victorian Secretaries Board has strategic oversight of public administration in Victoria including opportunities and risks faced by Victorian departments and public agencies. It also supports effective coordination, collaboration and communication between departments and public agencies.

2.2.2 The State Crisis and Resilience Council

The State Crisis and Resilience Council (SCRC) is the peak crisis and emergency management advisory body in Victoria responsible for advising the Minister for Police and Emergency Services in relation to whole of government emergency management policy, strategy and implementation. Chaired by the Secretary of the Department of Premier and Cabinet, the SCRC also comprises the secretaries of all departments plus the Chief Commissioner of Police, the Emergency Management Commissioner (EMC), the CEO of Emergency Management Victoria (EMV), a representative of the Municipal Association of Victoria and the Inspector-General for Emergency Management as an observer.

The SCRC has committees focusing on:

- risk and resilience;
- capability and response; and
- relief and recovery.

In the event of an emergency, the SCRC convenes to ensure whole of government attention is paid to the broad social, economic, built and natural environmental implications.

2.2.3 Department of Premier and Cabinet

The Department of Premier and Cabinet (DPC) plays a pivotal role in management of state significant risk through coordination of the Cabinet process and support of the Premier on government wide issues, as well as in the Premier’s portfolio of ministerial responsibilities.

2.2.4 Victorian Public Sector Commission

The Victorian Public Sector Commission promotes high standards of governance, accountability and performance in the Victorian public sector. The Commission produces guidance materials to support effective public sector governance. This includes guidance on the role of public entity boards in ensuring appropriate risk management policies and practices.

3. Mandatory requirements

3.1 Mandatory requirements

Ministerial Standing Direction 4.5.5 – Risk Management Framework and Processes directs that the responsible body must ensure the agency complies with the mandatory requirements set out in the VGRMF.

To comply with *Ministerial Standing Direction 4.5.5* agencies need to meet the following mandatory requirements. The responsibility for the agency's risk management performance rests primarily with the responsible body.

Mandatory requirements of the Victorian Government Risk Management Framework

3.1.1 Risk management requirements

The **responsible body** must be satisfied that:

- the agency has a risk management framework in place consistent with *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines*;
- the risk management framework:
  - *is reviewed annually to ensure it remains current and is enhanced, as required*; and
  - *supports the development of a positive risk culture within the agency*.
- the risk management processes are effective in managing risks to a satisfactory level;
- it is clear who is responsible for managing each risk;
- inter-agency risks are addressed and the agency contributes to the management of shared risks across government, as appropriate*****;
- the agency contributes to the identification and management of state significant risks, as appropriate*****;
- risk management is incorporated in the agency's corporate and business planning processes;
- adequate resources are assigned to risk management; and
- the agency risk profile has been reviewed within the past 12 months.

3.1.2 Insurance requirements

The Responsible Body of an agency required to insure with VMIA (as defined by the VMIA Act) must:

- *arrange all its insurance with VMIA unless exempted by the responsible Minister or where VMIA cannot offer insurance for a specific risk;*
- *as part of its annual insurance renewal process:*
  - determine the appropriate level of insurance in consultation with VMIA;
  - maintain a register of all insurance and indemnities and make this available to VMIA on request; and
  - provide information on claims management capability, resources, structures and processes for any self-insured retained losses to VMIA, including the basis for valuation of self-insured retained losses.
- in relation to managing below deductible claims:
  - maintain adequate claims management capability and processes where the agency has opted to manage below deductible claims; and
  - provide required below deductible claims data for self-managed claims to VMIA.

* Agencies do not need to attest to the mandatory requirements marked with an asterisk for the 2014-15 year. In 2015-16 agencies will need to attest to the full set of requirements.

3.2 Attestation requirements

Under *Ministerial Standing Direction 4.5.5 – Risk Management Framework and Processes* departments and agencies must provide an annual attestation of compliance.

The Responsible Body is responsible for the accuracy and completeness of attestation and should utilise audit committees or other internal governance bodies, where available, to support the view expressed.

Transition arrangements:

Agencies do not need to attest to the mandatory requirements marked with an asterisk for the 2014-15 year. In 2015-16 agencies will need to attest to the full set of requirements.

Mandatory requirements for attestation under *Ministerial Standing Direction 4.5.5*

3.2.1 For the risk management and insurance requirements the agency must:

- conduct an annual review of its compliance with both requirements;
- attest in the agency's annual report that it has complied with *Ministerial Standing Direction 4.5.5* or, if it is partially in compliance, identify areas of non-compliance and remedial actions taken in the attestation; and
- ensure the Audit Committee reviews and monitors compliance with *Ministerial Standing Direction 4.5.5*, and makes a recommendation to the Responsible Body on the level of compliance attained.

3.3 Guidance material in support of the risk management and insurance requirements

The guidance materials below are not mandatory requirements. They serve to provide examples or guidance to the Responsible Bodies on ways to address the mandatory requirements.

3.3.1 Inter-agency and state significant risks

An agency's responsibilities for managing risk extend beyond the effective management of agency specific risks. Arrangements for addressing inter-agency and state significant risks must be part of an agency's risk management framework. Collaboration will be necessary for shared risks to be managed effectively.

An agency should have an appreciation of the wider risk environment and where risks extend beyond its direct control, cooperate to identify and prioritise risks, develop clear accountabilities for their management and commit to collective solutions and outcomes. Unlike agency specific risks, inter-agency and state significant risks cannot be addressed in isolation by agencies.

Under the mandatory requirements the responsible body must be satisfied that inter-agency risks are addressed and the agency contributes to the management of shared risks across government, as appropriate. For inter-agency risk, an agency's approach should include:

- identifying current and emerging risks and other agencies likely to be affected by those risks;
- analysing and evaluating identified risks in consultation with other affected agencies;
- agreeing on a lead agency and relative responsibilities of affected agencies;
- implementing appropriate measures to manage the risks; and
- appropriate monitoring and reporting.

Under the mandatory requirements the responsible body must be satisfied that the agency contributes to the identification and management of state significant risks, as appropriate. For state significant risk, an agency's approach should include:

- identifying current and emerging risks that are of state significance, including those that require a coordinated whole of state response;
- bringing identified state significant risks to the attention of decision makers in a position to assess, prioritise and oversight the management of the identified risk;
- contributing to the management of the risk, as appropriate; and
- appropriate monitoring and reporting.

Agencies need to understand and consider the broader business of government and how risks that affect more than one agency can arise. Agencies are likely to have informal processes at agency and inter-agency level and may also have internal executive forums and committees in place that consider agency, inter-agency and state significant risk. The agency's risk management framework should clearly demonstrate how the agency addresses inter-agency and state significant risks.

If an inter-agency or state significant risk is brought to the attention of an agency, the agency is expected to work collaboratively with the identifying agency in analysing and evaluating the risk and to contribute, as appropriate, to the management of the risk.

3.3.2 Insurance as a risk management tool

Agencies should make best use of their available resources and assets to manage risk and minimise loss to the community and consolidated revenue. Insurance may be used to transfer or manage the risk of financial loss. However, risk may not be transferred in every instance and it may not always be cost beneficial to do so.

The use of insurance needs to be considered in light of:

- the nature of the risk;
- the availability of alternative risk management and risk mitigation strategies;
- the financial consequences of choosing not to insure; and
- the level of loss the agency is able to manage and fund (generally the risk of loss beyond this point would be insured).

The VMIA can provide advice on insurance. Departments or participating bodies must arrange all their insurance with the VMIA unless:

- exempted by the Minister for part or all risks; or
- VMIA has formally declined or cannot offer insurance for a specific risk.

Agencies must ensure they have the appropriate insurances in place for their specific risk profile and portfolio departments are accountable for providing oversight of their agencies.

The level of insurance required should be based on the agency's risk profile and tolerance, past claims experience, the availability and cost of insurance. Agencies are responsible for managing and funding any self-insured and under-deductible losses.

The **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 all 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 and 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; and
- ensure required below deductible claims data is provided to VMIA.

Even if a risk is insured, preventative and mitigating measures should be considered to reduce the probability of occurrence or severity of the outcome of an adverse event, and to provide a cost-benefit analysis of potential actions.

The VMIA has the capacity and expertise to help manage below deductible claims on behalf of the agency. The default position is for agencies to use the VMIA to manage below deductible claims. An agency electing to self-manage claims should ensure it is appropriately resourced to manage claims effectively.

If the risk is not insurable, the agency's risk management framework should set out an alternative response to address the risk.

Agencies are required to provide below deductible claims data to the VMIA for self-managed claims greater than $10 000, related to third party liability and employment liability claims (excluding WorkCover claims). Claims data should be provided to the VMIA annually as part of the insurance attestation process. The VMIA may also request details of other self-managed claims, and agencies must provide these upon request and in a VMIA prescribed format to ensure reliability and accuracy of data.

Further guidance, tools and templates are available on the VMIA website at www.vmia.vic.gov.au.

3.3.3 Additional guidance and risk management support

The VMIA provides advice to the Victorian public sector and delivers risk management assistance, guidance and training to build risk management capability and maturity across the State. Agencies can refer to the VMIA website to access VMIA Risk Management Guidelines outlining sound practice in implementing an effective risk management framework and complying with *Ministerial Direction 4.5.5*.

The VMIA website provides other references and information, including:

- upcoming learning and development programs and risk events;
- risk management information and updates;
- risk management tools and templates;
- publications;
- insurance policies; and
- links to other relevant websites.

The VMIA website is at www.vmia.vic.gov.au.

3.3.4 Guidance material in support of attestation requirements

The following examples of attestations have been provided to assist agencies that are fully compliant with *Ministerial Standing Direction 4.5.5*.

Sample Attestation

Department
I, (Name – Responsible Body) certify that the (name of department) has complied with the *Ministerial Standing Direction 4.5.5 – Risk Management Framework and Processes*. The (Name of Department) Audit Committee has verified this.

Statutory Authority and other relevant agency
I, (Name – Responsible Body) certify that the (name of agency) has complied with the *Ministerial Standing Direction 4.5.5 – Risk Management Framework and Processes*. The (Name of agency) Audit Committee verifies this (if an audit committee is available to verify).

Departments and agencies may amend the wording of the attestation having regard to their risk profile, risk management maturity and operating context. Where an agency has only partially complied with the Direction, the attestation must include an explanation of remedial actions to address areas of partial compliance.

4. AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines

Each agency is unique and the approach to managing risk needs to be appropriate and tailored to the activity, size, complexity and risk profile of the agency. An agency's approach to risk management must be consistent with the *AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines*.

The following risk management principles, framework and processes have been adopted from *AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines*.

4.1 Principles of risk management

The 11 **principles of risk management** state that risk management:

- creates and protects value;
- is an integral part of the agency's processes;
- is part of decision making processes;
- explicitly addresses uncertainty;
- is systematic, structured and timely;
- is based on the best available information;
- is tailored to the agency;
- takes human and cultural factors into account;
- is transparent and inclusive;
- is dynamic, iterative and responsive to change; and
- facilitates continual improvement of the agency[1].

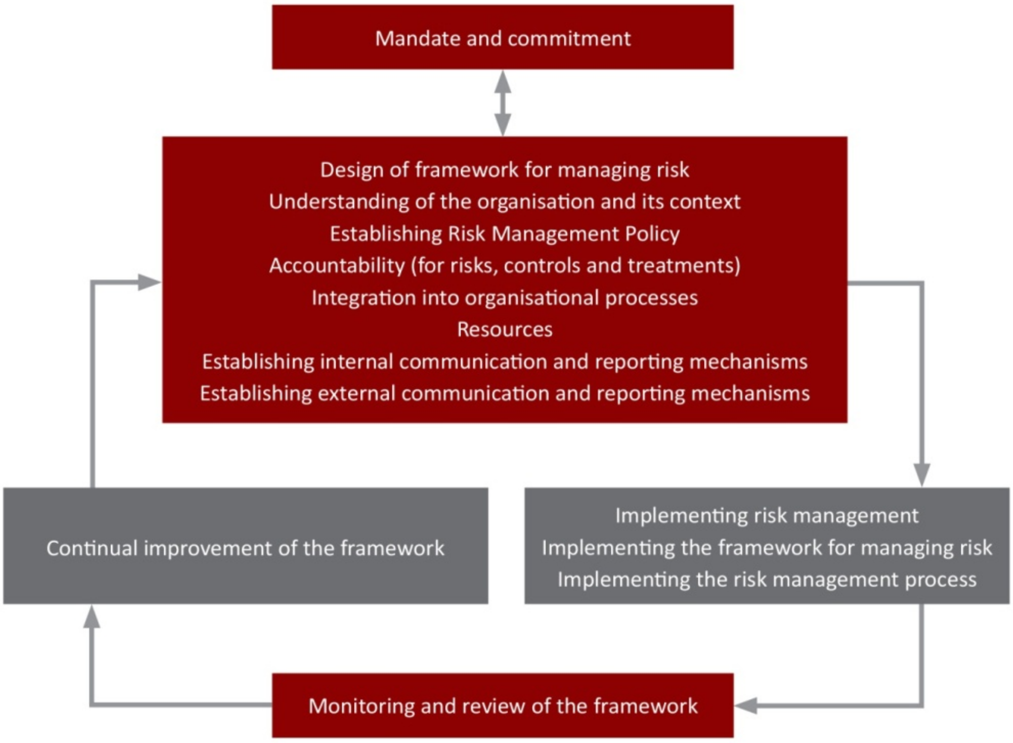
Agencies wanting to enhance their performance in managing risk can also apply the following approaches:

- continual improvement in risk management and organisational performance;
- full accountability for risks, controls and risk treatments;
- application of risk management in all decision making, whatever the level of importance and significance;
- continual communication and consultation with stakeholders; and
- full integration of risk management in the agency's governance structure[2].

[1] Standards Australia, 'Australian/New Zealand Risk Management Standard: AS/NZS ISO 31000: 2009', pp7, 8, clause 3.

[2] Standards Australia, 'Australian/New Zealand Risk Management Standard: AS/NZS ISO 31000: 2009', pp22, 23, Annex A.

4.2 Risk management framework


Mandate and commitment
Design of framework for managing risk
Understanding of the organisation and its context
Establishing Risk Management Policy
Accountability (for risks, controls and treatments)
Integration into organisational processes
Resources
Establishing internal communication and reporting mechanisms
Establishing external communication and reporting mechanisms
Continual improvement of the framework
Implementing risk management
Implementing the framework for managing risk
Implementing the risk management process
Monitoring and review of the framework

Standards Australia, 'Australian/New Zealand Risk Management Standard: AS/NZS ISO 31000: 2009', Figure 2, p9.

The key elements of the risk management framework are as follows:

Mandate and commitment – Agencies require a strong and sustained commitment by management to ensure the ongoing effectiveness of risk management in their organisation. This commitment should support the development of a positive risk culture within the agency.

Design of framework for managing risk – Agencies require a systematic approach in designing a risk management framework that is relevant, effective, efficient and adequate. The framework should include: appropriate risk management strategies, including working with other agencies to manage risk; a risk management policy and plan; effective governance, communication and reporting arrangements; resource requirements; and risk management accountabilities.

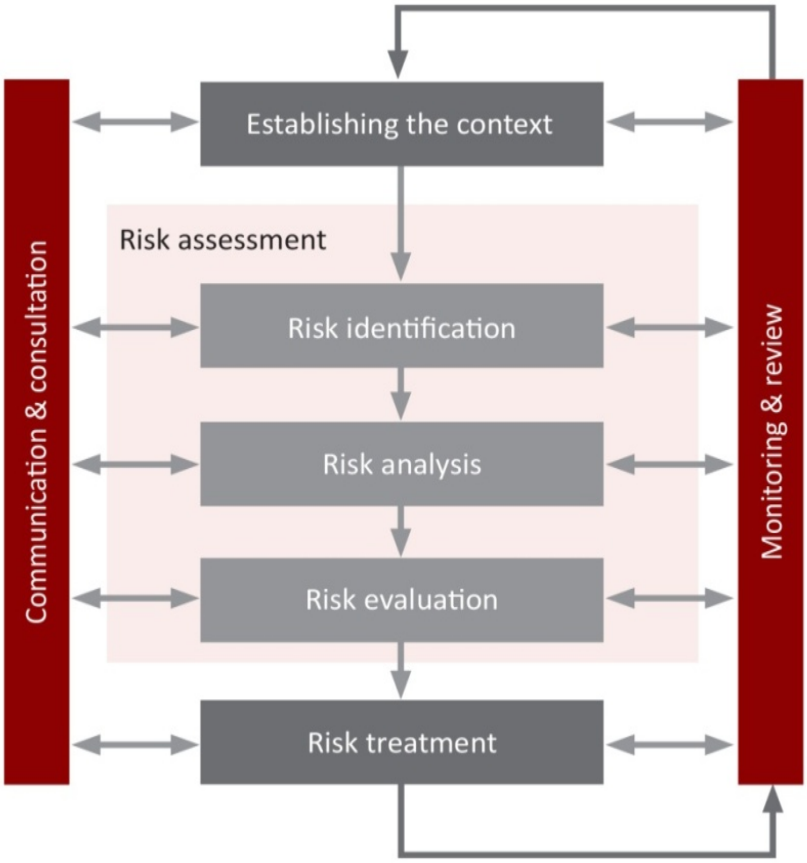
Implementing risk management – The risk management process is applied through a risk management plan at all relevant levels and functions of the department or agency as part of its practices and processes. Investment in resources and capabilities should enable an organisation to effectively and efficiently apply its risk management activities.

Monitoring and review of the framework – Agencies should continually ensure that risk management is effective and supports organisational performance. Under the mandatory requirements the risk management framework is to be reviewed annually and enhanced as required.

Continual improvement of the framework – Based on the results of monitoring, reviews, and any independent assurance of risk management controls and practices, decisions can be made on how the risk management framework, policy and plan can be improved[3].

[3] Standards Australia, 'Australian/New Zealand Risk Management Standard: AS/NZS ISO 31000: 2009', pp. 8-13, clause 4.

4.3 Risk management process



Standards Australia, 'Australian/New Zealand Risk Management Standard: AS/NZS ISO 31000: 2009', Figure 3, page 14.

The key elements of a risk management process are as follows:

- *Establish the context* means understanding the agency's objectives, defining internal and external factors that could be a source of uncertainty, helping identify risk and setting the scope and risk criteria for the remaining risk management process.
- *Risk identification* determines what, where, when, why and how risks could arise, and the effect this would have on the agency's ability to achieve its objectives. A range of government and industry resources may be employed to assist in the identification of risks. Risks may also be investigated through workshops that engage relevant stakeholders drawn from the public, private or community sectors.
- *Risk analysis* determines the risk level against the risk criteria by understanding how quickly a risk can occur, the sources and cause of a risk, the consequences and likelihood of those consequences. Analysis takes into account the effectiveness of existing controls. Risk evaluation compares the level of risk against the risk criteria and considers the need for treatment. The approach to risk evaluation should follow a typical risk assessment process of applying a consequence and likelihood matrix. Assessing the risks in relation to each other supports prioritisation and highlights differences. Mitigation strategies can be taken into account to derive the residual risk.

- *Risk treatment* involves assessing and selecting one or more options for modifying risks by changing the consequences or likelihood and implementing selected options through a treatment plan.
- *Communication and consultation* takes place throughout the risk management process with all identified stakeholders to ensure those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made.
- *Monitoring and review* confirms that risk and the effectiveness of control and risk treatments are monitored and reported to ensure that changing context and priorities are managed and emerging risks identified[4].

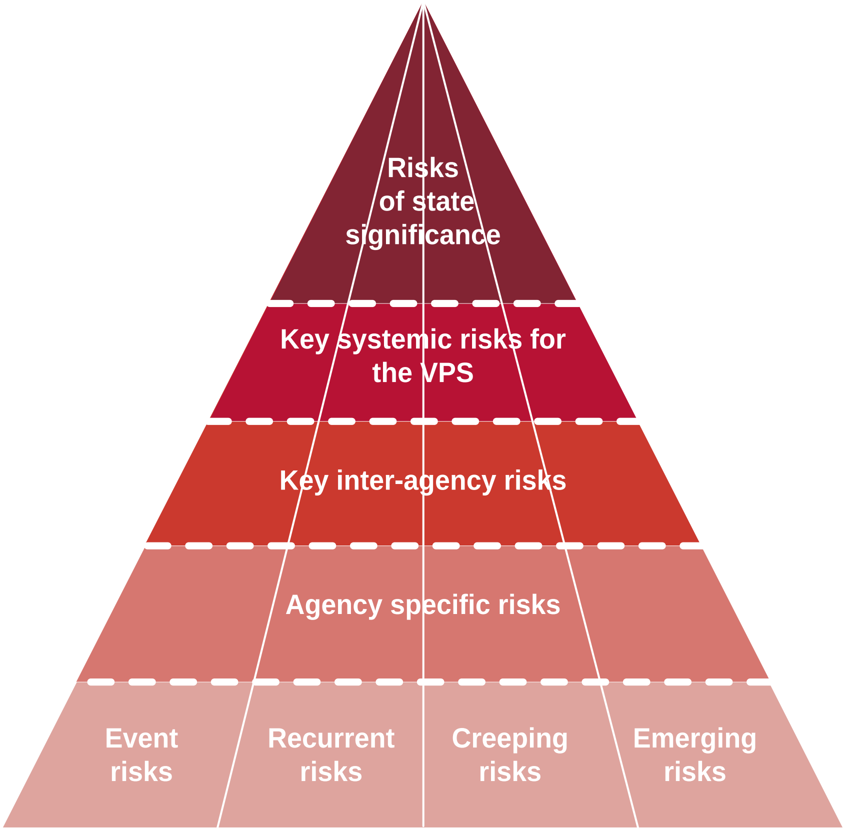
[4] Standards Australia, 'Australian/New Zealand Risk Management Standard: AS/NZS ISO 31000: 2009', pp13 – 21, clause 5.

Appendix 1 – Introduction to risk management

Agencies can refer to the VMIA website www.vmia.vic.gov.au for **advice and support on managing risk**, including implementing an effective risk management framework and the effective use of insurance as a risk management tool.

A brief introduction to risk management and concepts is provided below.

Categories of risks



Risks can involve short and long-term impacts and may have event-based, recurrent, creeping (becomes more serious over time) or emerging features. With an emerging risk we are still developing an understanding of the opportunities or threats, but due to their potential impacts, the risk is monitored and further investigated.

Agency specific risks are risks that can be managed entirely within a single agency's operations and can generally be well understood and effectively managed with straight forward risk management processes.

Inter-agency risks are 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 an inter-agency risk is shared by all the relevant agencies and will benefit from a coordinated response where one agency takes a lead role.

Systemic risks are risks that have implications for all parts of government operations, requiring a high level of management and coordination between agencies. As with inter-agency and state significant risks agencies are responsible for contributing to the identification and management of systemic risks, as appropriate.

State significant risks are 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. A state significant risk can be the extension of an existing agency risk which, beyond a certain threshold, becomes severe enough to have state wide implications or it could be the aggregation of many agency specific risks. An agency's responsibility is to ensure that a state significant risk is considered by decision makers at the appropriate level of government. Agencies are also responsible for contributing to management of the risks identified.

Risk management concepts

The responsibility for managing risk within an agency must be clear, and include:

- who is responsible for determining the agency's risk appetite and how it is communicated or documented, as appropriate;
- how the responsibility for implementing the agency's risk management framework is allocated; and
- roles and responsibilities for managing individual risks.

Risk appetite supports risk evaluation and defines the amount and type of risk that an agency is willing to accept in pursuing its objectives. Risk appetite may be expressed in various ways to ensure that it is understood and consistently applied by the organisation.

The agency's **risk profile** is a description of any set of risks. The set of risks can contain those that relate to the whole organisation or part of the organisation.

It is important to take human and cultural factors into account in an agency's approach to risk management. A positive **risk culture** is one where every person in the agency believes that thinking about and managing risk is part of their job.

Risk management needs to be incorporated in the agency's **corporate and business planning process**. An effective risk management approach strengthens corporate and business planning by:

- enabling better decision making;
- building organisational confidence in new opportunities through a considered risk approach;
- supporting improved performance outcomes; and
- establishing clear accountabilities.

Agencies need to maintain adequate **resources** and capability to ensure that the risk management function operates effectively. This includes:

- the necessary people, skills, experience and competence;
- adequate funding;
- processes, methods and tools for managing risk;
- information and systems;
- staff training and education; and
- risk tools and techniques.

Risk maturity describes risk capability and the level of maturity an agency operates at in terms of its risk processes and procedures. Risk maturity is not a static concept. As agencies and their environments change, risk management also needs to evolve to ensure that it continues to support agencies achieving their objectives. Agencies should consider developing and implementing strategies to improve their risk maturity (or maintain it at the desired level) alongside all other aspects of their organisation.

Agencies may choose to undertake a self-assessment of their risk maturity using an internally developed methodology or an established model such as that defined in *AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines* or the VMIA risk management assessment methodology.

Other risk terms

The following provides an overview of other risk terms; more detailed explanations and guidance is included in VMIA guidance materials. (Note: these are not definitions or standards). See also *ISO Guides73:2009* which provides the basic vocabulary and understanding of risk management concepts.

Residual risk	The risk remaining after risk treatment; also known as retained risk. Can include unidentified risk.
Risk	The effect of uncertainty on objectives. An effect may be positive or negative. Objectives may be related to aspects such as financial, health and safety or environmental and may apply at strategic, operational project or process related levels.
Risk analysis	Process to understand the nature of the risk and to determine the level of risk.
Risk attitude	The organisation's approach to assess and pursue, retain, take or turn away from risk.
Risk control	Measures taken to modify the risk or reduce an undesired consequence.
Risk criteria	Terms of reference against which the significance of risk is evaluated. Based on organisational objectives and internal and external contexts. Risk criteria can be derived from standards, laws, policies and other requirements.
Risk evaluation	The process of assessing risk analysis results to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists the decision about risk treatment and needs to consider the risk appetite and risk tolerance of the organisation.
Risk event	An occurrence or change of a particular set of circumstances. May have one or more occurrences and can have several causes. An event can consist of something not happening and may also be referred to as an 'incident'.
Risk identification	The process of finding, recognising and describing risks. Involves the identification of risk sources, events and potential consequences. Can involve historical data, theoretical analysis, informed and expert opinions and stakeholder needs.
Risk management	The combination of organisational systems, processes and culture which facilitate the identification, assessment, evaluation and treatment of risk to achieve an appropriate balance between realising opportunities while minimising losses in the pursuit of strategic objectives.
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk profile	A description of any set of risks. The set of risks can contain those that relate to the whole organisation or part of the organisation.
Risk management process	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.
Risk register	Record of information about identified risks.
Risk strategy	A risk management strategy (may be referred to as the risk plan or risk policy) that outlines and describes the key elements of the risk management framework. It specifies the approach, the management components and resources to be applied to the management of risk.
Risk tolerance	The organisation'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.
Risk treatment	Process to modify risk, may include deciding to take, retain, avoid, remove, change or share the risk. Risk treatments that deal with negative consequence may also be referred to as risk mitigation.

Appendix 2 – Emergency management

Emergency risks are risks that, if realised, would result in emergencies. The potential consequences of emergencies can be sudden, visible and highly damaging. Managing these risks requires coordinated inter-agency activity, which is a function of Victoria's emergency management arrangements.

Victoria's emergency management governance structure

The **State Crisis and Resilience Council (SCRC)**, the peak crisis and emergency management advisory body in Victoria, is required to have a three-year rolling strategic action plan in relation to the fire services, Department of Environment, Land, Water and Planning, Victoria State Emergency Services and the Emergency Services Telecommunications Authority, which the agencies must implement. The plan must include elements enhancing each agency's operational capacity and capability, and its capacity to operate together with the other agencies for emergency response.

Emergency Management Victoria (EMV) is responsible for coordination of the development of whole of government emergency management policy, to implement emergency management reform initiatives given to it by the Minister for Police and Emergency Services, and to support the performance of the Emergency Management Commissioner's (EMC) functions. EMV must have regard to decisions made by the SCRC and must collaborate and consult with the emergency management sector.

The EMC, a member of EMV, has a range of powers and roles in relation to the response to and recovery from emergencies. In addition, the EMC is responsible for consequence management for a major emergency. Consequence management means the coordination of organisations responsible for managing or regulating services or infrastructure. The objective is to minimise the adverse consequences to users of services or infrastructure caused by an interruption while recognising that safety needs are paramount.

The Inspector-General of Emergency Management (IGEM) stands outside EMV. The IGEM's role is to provide assurance to the Government and community about emergency management arrangements and to foster continuous improvement.

The publication of *Emergency Risks in Victoria in 2014* presents the first-ever ranking of emergency risks in Victoria, in order to share the State's understanding of emergency risk priorities with the private and non-profit public sectors and academia. This also recognises that governments do not carry sole responsibility for managing such risks. It also sets out what is being done about those risks and sources of further information. The emergency risks include bushfire, earthquake, flood, heatwave, hazardous materials emergency, storm, transport infrastructure emergency and marine pollution. A copy of the report is available via www.justice.vic.gov.au.

Key references

Emergency Management Reform – White Paper

www.depi.vic.gov.au/water/Floods-and-floodplains/government-flood-initiatives/emergency-management-reform

Australian Emergency Management Institute – National Strategy for Disaster Resilience

www.em.gov.au/Publications/Program%20publications/Pages/NationalStrategyforDisasterResilience.aspx

Emergency Management Manual Victoria (contains the state emergency response and recovery plans)

www.emv.vic.gov.au/policies/emmv/

Security related risks

Terrorism

www.nationalsecurity.gov.au

Cyber attacks

www.cert.gov.au

www.asd.gov.au

www.staysmartonline.gov.au

www.cybersmart.gov.au

Appendix 3 – Definitions

Agency	Any department or public body as defined in the *Financial Management Act 1994.*
Accountable Officer	In relation to a department or public body, means the accountable officer for that department or public body as determined under section 42 of the *Financial Management Act 1994.*
Audit Committee	The Standing Directions of the Minister for Finance require that an audit committee be appointed to oversee and advise the department or agency on matters of accountability and internal control. This committee is a subset of the Responsible Body (or Board) which has been formulated to deal with issues of a specific nature.
Responsible Body	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.

dtf.vic.gov.au

State Government Victoria

Department of Treasury & Finance