Victorian Government Risk Management Framework

August 2020

(to take effect from 1 July 2021)

VICTORIA State Government | Treasury and Finance

The Secretary
Department of Treasury and Finance
1 Treasury Place
Melbourne Victoria 3002
Australia
Telephone: +61 3 9651 5111
Facsimile: +61 3 7005 9165
dtf.vic.gov.au

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

ISBN 978-1-925551-62-4 **(**pdf/online/MS word)
Published June 2020 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 PDF format at dtf.vic.gov.au

Contents

Foreword

I am delighted to present to you the 2020 update to the Victorian Government Risk Management Framework.

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.

When I was Chair of the Public Accounts and Estimates Committee, , we examined the Government's risk management framework against the Victorian Auditor General's October 2013 report. The Committee made a number of recommendations, and I am pleased to see the updated Framework is consistent with the recommendations in both reports.

The 2020 edition of the Victorian Risk Management Framework provides greater clarity as to the roles of managers and audit committees when it comes to risk management functions. Departments and agencies are now asked to consider and define their risk appetite within their risk management frameworks, and to demonstrate a positive risk culture based on the guidelines.

The Framework now includes clear directions on the management and responsibility of shared risks, including the requirement for greater inter-departmental collaboration and coordination, and sets out roles within Government for coordinating risk responses to shared and state significant risk, including the role of the SSR IDC and the Victorian Secretaries Board.

Finally, the Framework includes new guidance on the use of data and analytics to encourage the greater use of data, including the use of key risk indicators to support improved decision making.

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 continues to move 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 shared and state significant risks as well. This needs to be the hallmark of joined-up service delivery.

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 congratulate Victorian public sector agencies on building their risk management capabilities since the last revision of the Victorian Government Risk Framework and encourage them to continue their risk management journey.

The Hon. Danny Pearson MP Assistant Treasurer

1. Introduction

Effective risk management protects and creates value for the Victorian Public Service by enabling informed decision making, setting and achieving objectives and improving performance. 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 the management of both financial and non-financial risks 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 3.7.1 – 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 shared and state significant risk. It outlines the role and responsibilities of an agency's responsible body. The VGRMF adopts the ISO 31000:2018 Risk Management – Guidelines which provides an internationally accepted basis for best practice risk management.

The VGRMF is mandated by the Standing Direction of the Minister for Finance's (*Ministerial Standing Direction) 3.7.1 – 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 3.7.1 – 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

2.2.1 All agencies

All agencies must fully comply with the requirements of *Ministerial Standing Direction 3.7.1* and are responsible for appropriately identifying, assessing and managing all risks to which they are exposed. Agencies should establish and maintain effective corporate 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. Senior management at each agency own and lead engagement with their risk management framework.

Agencies should define their risk appetite considering their strategic objectives, risk profile, risk / reward trade off and risk management budget allocation. Agencies are to identify the specific behaviours expected within the agency which are required to reinforce a positive risk culture.

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.

2.2.2 Agency audit committee

Under *Ministerial Standing Direction 3.2 – Oversight and assurance*, 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 include:

- considering the agency's risk profile and insurance arrangements;
- reviewing and assessing the effectiveness of the agency's risk management framework;
- reviewing, monitoring and verifying compliance with *Ministerial Standing Direction 3.7.1*;
- reporting to the responsible body on the level of compliance attained; and
- reviewing and providing oversight of the agency's risk appetite and risk culture to ensure it is consistent with the expectations of the agency's responsible body.

2.2.3 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 3.7.1* through the annual attestation process and provides additional guidance on the DTF website at www.dtf.vic.gov.au.

2.2.4 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 and risk maturity assessments.

2.3 Other entities with roles and responsibilities in public sector management

2.3.1 Victorian Secretaries Board

The Victorian Secretaries Board (VSB) 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. The VSB receives periodical reporting on state significant risks.

2.3.2 State Significant Risk Interdepartmental Committee

The purpose of the State Significant Risk Interdepartmental Committee ('Risk IDC') is to support the identification of key shared and state significant risks and the development, operation and effectiveness of the whole-of-government risk management frameworks related to those risks.

The Risk IDC plays a vital role in the management of state significant risks and receives periodic reporting from all agencies to support the monitoring and reporting of state significant risks. DTF serves as the Risk IDC's Secretariat.

2.3.3 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.

2.3.4 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.

A separate State Crisis and Resilience Council (see Appendix 2) has also been established to support the state prepare and respond to emergency management risks.

3. Mandatory requirements

3.1 Mandatory requirements

Ministerial Standing Direction 3.7.1 – 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 3.7.1* 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

1. Risk management requirements

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

- the agency has a risk management framework in place consistent with AS *ISO 31000:2018 Risk Management – Guidelines*;
- the risk management framework is reviewed annually to ensure it remains current and is enhanced, as required;
- a positive risk culture in the agency is able to be demonstrated;
- the agency defines its risk appetite;
- it is clear who is responsible for managing each risk;
- 'shared risks are identified and managed through communication, collaboration and/or coordination by the impacted agencies;
- the agency contributes to the identification and management of state significant risks, as appropriate;
- strategic and business planning and decision-making processes embed risk management and demonstrate consideration of the agency's material risks;
- adequate resources are assigned to risk management; and
- the agency risk profile and risk appetite must be reviewed at least annually.

2. Insurance requirements

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

- Determine the most appropriate insurance products and levels of cover for the organisation's present and future risk exposures, in consultation with VMIA.
- Arrange all its insurance with VMIA, unless exempted by the responsible Minister or where VMIA cannot offer insurance for a specific risk.
- Maintain appropriate deductibles for each insurance product that reflects the organisation's risk appetite and capability for retaining financial risk;
- Provide adequate claims management capability, resources, structures and processes for the management for retained financial risks;
- Ensure claims management practices for retained financial risks are in place and that the agency maintains relevant claims data, and have this information available to VMIA on request;
- Work towards minimising exposure to insurable risk.

3.2 Attestation requirements

Under *Ministerial Standing Direction 5.1.4 – Financial management compliance attestation,* departments and agencies must provide an annual attestation of compliance with applicable requirements of the *Financial Management Act 1994*, the Standing Directions (incorporating this framework) and the Instructions and disclose all material compliance deficiencies.

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.

3.3 Guidance to support mandatory 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 concepts to support agencies address the mandatory requirements. Each agency's evaluation of the suitability and implementation of these guidelines will vary, depending of their size, resourcing and risk exposures.

3.3.1 Shared and State significant risks

To achieve the best outcomes for Victoria, agencies need to work collaboratively to identify and contribute to the management of both shared and state significant risks. Identifying and managing these risks is important to provide confidence to Government and the community that these risks are being managed and there is a clear line of sight over them. Both concepts are defined in Appendix 1.

Shared risks

Agencies must contribute to the management of shared risks. To clearly demonstrate this requirement, an agency will need to:

- **collaborate** to identify and assess risks
- **coordinate** in the management of risks
- **communicate** to support in early identification and effective management of these risks

A key component of effective shared risk management is cross-agency communication. Communication channels between agencies will promote information sharing and in respect to shared risk management, will assist in the identification of risks and controls over which an agency does not have line of sight. Example communication channels could include periodic interagency meetings, shared systems or emails and formal agreements. Regular communication with other agencies will promote more effective shared risk management.

Assigning accountability / ownership for a shared risk will require agencies to assess, communicate and collaborate to determine the appropriate lead agency. Agencies need to assign lead agencies as follows:

- Impacted agencies collaborating to agree on the lead agency responsible for the shared risk.
- In the very rare instance, where the agencies are unable to come to an agreement on the lead agency for a state significant risk, the Risk IDC will determine the lead agency.

Under the mandatory requirements (see bullet points 6 and 7 under 3.1.1) the agency's responsible body must be satisfied that shared risks are addressed and the agency contributes to the management of shared risks across government, as appropriate. For shared risks, an agency's approach includes:

- 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 or escalation to the Risk IDC;
- implementing appropriate measures to manage the risks;
- appropriate monitoring and reporting; and
- performing annual reviews or if there is a significant change in risk.

State significant risks

State significant risks are risks where the potential consequences or impacts of the risk on the community, the Government and the private sector are material at the State-wide level. 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. Each state significant risk has a risk lead appointed by the Risk IDC.

The agency's risk management framework should clearly demonstrate how the agency addresses state significant risks relevant to its operations.

If a 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.

Under the mandatory requirements the agency's 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 to the Risk IDC and VSB.

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. Insurance may be used to transfer or manage the risk of financial loss. The use of insurance needs to be considered in the context 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 can bear

VMIA can provide advice to Agencies on insurable risk transfer opportunities.

The level of insurance required should be based on:

- the agency's risk profile and risk appetite,
- past claims experience,
- the availability and cost of insurance.

Insured risk needs preventative and mitigating treatments where appropriate 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.

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

An agency electing to self-manage claims should ensure it is appropriately resourced to manage claims effectively. Agencies are required to provide below deductible claims data to VMIA for self-managed claims greater than $10 000, related to third party liability and employment liability claims (excluding WorkCover claims).

Claims information must be provided to VMIA on request, in a VMIA prescribed format to ensure reliability and accuracy of data.

3.3.3 Risk Culture

Risk culture refers to the system of beliefs, values and behaviours throughout an organisation that shapes the collective approach to managing risk and making decisions. A positive risk culture is one where staff at every level appropriately manage risk as an intrinsic part of their day-to-day work.

To encourage a positive risk culture, agencies should consider how the following key principles of effective risk culture work in practice:

- Tone from the top;
- Accountability;
- Strategy;
- Communication;
- Awareness and recognition of positive risk culture;
- Escalation of bad news;
- Supporting tools, templates and mechanisms; and
- Continuous improvement.

Leaders should understand and value risk culture as a driver of good risk outcomes and the Accountable Officer for each agency is responsible for setting, owning, instilling and overseeing an appropriate risk culture.

The management process for a prioritised focus on risk culture includes:

a) understanding the agency's current risk culture and defining the desired risk culture;

b) identifying any gaps between the agency's current risk culture and desired risk culture; and

c) defining the agency's approach to evolve the agency's risk culture to close gaps over time.

3.3.4 Risk Appetite

Risk appetite is the type and amount of risk that an agency is prepared to accept in pursuit of its strategic objectives and business plan. There is no one best way to articulate an agency's risk appetite and the approach taken must be tailored to the needs of each agency.

Defining the material risks of the agency and the level of risk acceptable to the agency, enables the allocation of scarce risk management resources to those areas of low or minimal appetite and less effort to be expended in moderate or high appetite areas. Where an agency sits on that spectrum depends on the nature of the risk and the level of effort and investment it is willing to dedicate to the mitigation or management of that risk.

It is important that the risk reward trade-off be considered when defining the agency's risk tolerance levels. The Executive Team should identify the strategic objectives of the agency where a level of increased risk taking would be accepted in pursuit of these objectives.

3.4 Guidance to support good practice risk management

3.4.1 Risk Evaluation

Risk Evaluation is completed to support decisions including whether to accept the risk (particularly if it falls within the agency's risk appetite) or whether to mitigate the risk through further treatment and prioritise those treatments

Factors to use in evaluating a risk include:

- comparing the level of the risk against the agency's view of the level of acceptable risk;
- determining the level of the risk so low that treatment is not appropriate;
- assessing if the opportunities outweigh the threats to such a degree that the risk is justified;
- considering if the cost of further treatment is excessive compared to the benefit and
- checking to ensure there is an available treatment.

The risk evaluation should be conducted by the risk owner. The risk evaluation may lead to a decision that either:

- accepts the risk
  - further treatment may be applied but will be a lower priority; or
  - if no further treatment, ongoing monitoring of the risk and controls is required to ensure the risk remains acceptable.
- does not accept the risk
  - further treatment will be required to bring the risk within the agency's risk appetite;
  - the risk owner may be required to undertake further analysis to better understand the risk; or
  - the agency may need to reconsider objectives.

3.4.2 Key Risk Indicators

Key Risk Indicators (KRIs) provide insight into the possibility of future adverse likelihood of risks and can identify potential events that may cause harm. KRIs are typically leading or predictive and used to signal changes in the likelihood of a risk event. They aid management taking action in advance of risks materialising.

As the State's access to data to measure its reform and service activities improve, both KRIs and risk KPIs become more accessible tools to effectively manage risk. Data analytics uses information to form a view as to whether that risk severity is increasing or decreasing.

Monitoring and measurement of KRIs and risk KPIs are powerful ways of keeping track of efforts and alerting management to important changes (both positive and negative) in the risk management initiatives through a data driven approach.

Agencies can utilise KRIs as an early warning of increasing risk, which can be achieved through:

- data driven risk assessments – use of data analytics to aid in the identification of risk, fraud, error or misuse or the early identification of a control breakdown or verification of control effectiveness.
- working with other agencies to agree KPIs and KRIs; and
- establishing data analytics networks to:
    - share success stories and provide a process for agencies to identify data sources across VPS; and
    - compile and maintain a risk register detailing the data sources utilised for risk management across the VPS.

3.4.3 Risk Maturity

Risk maturity describes risk capability and the level of sophistication an agency operates at in terms of its risk processes and procedures. Risk maturity is not a static concept and should be tailored to reflect how risk can best support delivery of the agency's strategic objectives. As agencies and their environments change, risk management evolves 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) to ensure it supports effective risk management.

3.4.4 Control Effectiveness Testing

Control effectiveness testing involves regular reviews of an agency's controls to ensure they are designed and operating effectively to minimise the risks they are intended to mitigate. This technique is best suited for use in agencies with stable control environments, mature risk management frameworks and resources able to perform the work involved.

Controls testing and validation is important in ensuring the agency is reviewing its risks and developing effective methods to minimise these where possible. It is beneficial for agencies to develop their controls framework to more effectively mitigate risk. The establishment of an effective controls framework includes:

- Defining a controls library. A controls library contains common controls testing examples, including what is considered to be a key control. A key control can provide reasonable assurance that material errors may be detected and prevented in a timely manner. This could include policies and procedures, embedded authorisations and approval process, training and clear descriptions or segregation of duties.
- Identifying control ownership. Control owners should be identified and designate roles and responsibilities defined. It may also be beneficial to focus on accountability and consequences of a failure to control and mitigate the risk as part of the risk owner's performance reviews.
- Control testing and validation. Controls should be regularly reviewed to ensure they are designed and operating effectively to minimise the risks they are intended to mitigate. Control testing and validation could include:
    - Control self-assessments by control owners
    - Consideration of breaches, internal audit findings and / or any process issues identified during the year as part of the annual review of the risk profile
    - Regular review and testing of key controls by either re-performing the control, observing / inspecting that the control is working.

3.4.5 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 3.7.1.

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

4. AS ISO 31000:2018 Risk Management – 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 *ISO 31000:2018 Risk Management – Guidelines*.

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.

Shared risks are risks shared by two or more agencies that require coordinated management by more than one agency. The responsibility for managing a shared risk is shared by all the relevant agencies and will benefit from a coordinated response where one agency takes a lead role.

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. While all state significant risks are shared between agencies, not all shared risks are state significant risks.

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 state significant risks identified.

Risk management concepts

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.

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).

Term	Description
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories and be applied at different levels.
Risk culture	Risk culture refers to the system of beliefs, values and behaviours throughout an organisation that shapes the collective approach to managing risk and making decisions. 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 appetite	The types and amounts of risk that an agency is willing to accept in the pursuit of its strategic and business objectives.
Risk management	Coordinated activities to direct and control an organisation with regard to risk
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Risk source	Element which alone or in combination has potential to give risk to risk.
Event	Occurrence or change of a particular set of circumstances. An event can have one or more occurrences and can have several causes and several consequences.
Consequence	Outcome of an event. A consequence can be certain or uncertain and can have positive or negative or direct or indirect effects on objectives.
Likelihood	Chance of something happening. In risk management, 'likelihood' is used to refer to the change of something happening, whether defined, measure or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.
Control	Measure that maintains and / or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and / or actions which maintain and / or modify risk.
Residual risk	The risk remaining after risk treatment; also known as retained risk. Can include unidentified risk.
Risk analysis	Process to understand the nature of the risk and to determine the level of risk.
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.

Term	Description
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 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 maturity	The benchmarking of an agency's risk management framework relative to leading practice
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.
Key risk indicator	A metric used to measure the likelihood of a risk event or the effectiveness of controls that prevent a risk event. They provide an early signal of increasing risk exposures.
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.
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.

Appendix 2 – Emergency management

Emergency management contributes to community safety through the reduction of the impact of emergency related events that can cause death, injury, loss of property and community disruption. The planning for, and the management of, emergencies is a shared responsibility with communities, government, agencies and business.

The potential consequences of emergencies can be sudden, visible and highly damaging. Victoria has in place a governance structure that assists in managing emergency risks through a shared vision of *safer and more resilient communities*.

Victoria operates a multi-agency framework for emergency management that enables capacity to adapt to new or changed circumstances, within a broader emergency management system.

Victoria's emergency management governance structure

The **State Crisis and Resilience Council (SCRC)**, is established under the *Emergency Management Act 2013* (the EM Act) to act as the peak crisis and emergency management advisory body in Victoria. The SCRC provides advice to the Minister for Police and Emergency Services (the Minister) in relation to whole of government policy and strategy for emergency management in Victoria and its implementation.

Section 12 of the EM Act requires the SCRC to develop a rolling three-year Strategic Action Plan (SAP) to be submitted to the Minister for approval. The SAP outlines a number of state-wide strategic priorities and actions to support Victoria achieve its vision of *safer and more resilient communities.* Emergency Management Victoria (EMV) facilitates an annual review of the SAP in liaison with emergency management agencies and departments.

Work programs are developed through the SAP which include elements aimed at enhancing each agency's operational capacity and capability and its capacity to operate together with other agencies for emergency response. EMV is responsible for coordinating the development of whole of government emergency management policy, implementing emergency management reform initiatives given to it by the Minister, and to support the performance of the Emergency Management Commissioner's functions. EMV must have regard to decisions made by the SCRC and must collaborate and consult with the emergency management sector.

The **Emergency Management Commissioner** supported by EMV has a range of powers and roles in relation to the coordinating response to and recovery from emergencies. The EMC leads the coordination of emergency preparedness, response and recovery across Victoria's emergency management sector in conjunction with communities, government, agencies and business. The EMC is also responsible for consequence management for a major emergency; the objective being to minimise the adverse consequences caused by an emergency on communities. Consequence assessments help to understand how medium to long term consequences may affect the delivery of recovery effects, rehabilitation and revitalisation.

The current governance arrangements for the management of emergencies within Victoria are enshrined in the EM Act and are described in the State Emergency Response Plan and the State Emergency Relief and Recovery Plan.

The *Emergency Management Legislation Amendment Act 2018* (EMLA Act) sets out underlying principles and requirements for the content of emergency management plans at State, regional and municipal levels. This includes the development of the State Emergency Management Plan (SEMP) and associated Ministerial guidelines, which will replace the State Emergency Response Plan and the State Emergency Relief and Recovery Plan.

The **Inspector General of Emergency Management** provides assurance to the Government and the community about emergency management arrangements and to foster continuous improvement.

Key references

Emergency Management Reform – White Paper

https://www.emv.vic.gov.au/publications/victorian-emergency-management-reform-white-paper-dec-2012

Australian Institute for Disaster Resilience – Handbook Collection

https://aidr.org.au/programs/handbook-collection/

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

VICTORIA
State Government

Treasury
and Finance