Falls Creek Resort Management Risk Management Framework

September 2019
BP 1.5(a)

Department of Treasury and Finance

Falls Creek Alpine Resort Management Board

1 Slalom Street | Falls Creek | VICTORIA | AUSTRALIA | 3699

Telephone: +61 3 5758 1200
www.fallscreek.com.au

Contents

1. Introduction

Effective risk management protects and creates value for the Falls Creek Alpine Resort Management Board (FCARMB) by enabling informed decision making, setting and achieving objectives and improving performance. Management of risk is an integral part of the culture of (FCARMB, 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.

FCARMB will 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 FCARMB moves to a more sophisticated approach to the development and delivery of services.

The Assistant Treasurer 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, but are not limited to:

- *Financial Management Act 1994* (FMA);
- Standing Direction 2018 Under the *Financial Management Act 1994* 3.7.1– Risk Management Framework and Processes;
- Victorian Government Risk Management Framework (VGRMF)
- 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

FCARMB will make every effort, where appropriate, to apply the VGRMF as it describes the minimum risk management requirements needed to be met in order to demonstrate that the organisation is managing risk effectively, including shared and state significant risk.

The suggested framework in this document outlines the role and responsibilities of FCARMB's responsible body, the Board (refer to Appendix 2 – Definitions).

To comply, FCARMB intends to utilise the VGRMF and thereby adopt the *Australian Standard AS ISO 31000:2018 Risk Management –Guidelines* for the provision of an internationally accepted basis for best practice risk management.

The VGRMF is mandated by the Standing Direction 2018 Under the *Financial Management Act 1994* 3.7.1 – Risk Management Framework and Processes.

FCARMB thereby adopts both the VGRMF and AS ISO 31000:2018 as the guiding principles applied to its Risk Management framework.

1.2 Coverage

Under Standing Direction 3.7.1 – Risk Management Framework and Processes, the VGRMF applies to FCARMB as covered by the *Financial Management Act 1994*.

Appendix 2 – Emergency Management within the VGRMF documentation is not replicated in this Risk Management Framework document, as emergency management matter is adequately covered in other FCARMB documentation (eg. Municipal Emergency Management Plan and other FCARMB disaster recovery and emergency management plans).

2. Roles and responsibilities

2.1 Entities with specific roles and responsibilities under the VGRMF

2.1.1 Falls Creek Alpine Resort Management Board (FCARMB)

FCARMB must fully comply with the requirements of Standing Direction 3.7.1 and is responsible for appropriately identifying, assessing and managing all risks to which the entity is exposed. FCARMB will establish and maintain effective risk governance that includes an appropriate internal management structure and oversight arrangements for managing risk. FCARMB is accountable for the organisation's risk management obligations. Senior management own and lead engagement with FCARMB's risk management framework.

FCARMB will define its risk appetite considering the organisation's strategic objectives, risk profile, risk / reward trade off and risk management budget allocation, and identify the specific behaviours expected within the organisation which are required to reinforce a sound risk culture.

Under section 13A 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, FCARMB must report appropriately up to the Secretary of the Department of Environment, Land, Water and Planning (DELWP) who is expected to advise the portfolio Minister on any significant risks relating to the relevant public entities.

2.1.2 Finance, Risk and Audit Committee (FRAC)

Under Standing Direction 3.2 – Oversight and Assurance, FCARMB 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 FCARMB.

In relation to risk management, the FCARMB audit committee may:

- consider FCARMB's risk profile and insurance arrangements;
- review and assess the effectiveness of the FCARMB's risk management framework;
- review, monitor and verify compliance with Standing Direction 3.7.1;
- report to the responsible body (FCARMB's Board) on the level of compliance attained; and
- review and provide oversight of the organisation's risk appetite and risk culture to ensure it is consistent with the expectations of FCARMB's responsible body.

2.1.3 Department of Treasury and Finance (DTF)

DTF advises the Victorian State 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 Standing Direction 3.7.1 through the annual Financial Management Compliance attestation process and provides additional guidance on the DTF website at www.dtf.vic.gov.au.

2.1.4 Victorian Managed Insurance Authority (VMIA)

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 FCARMB 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.

2.1.5 Other public sector entities with risk roles and responsibilities

Particularly for shared and state significant risks and whole-of-government risk management frameworks, FCARMB may also liaise with the Victorian Secretaries Board (VSB), the State Significant Risk Interdepartmental Committee (Risk IDC), the Department of Premier and Cabinet (DPC), the Victorian Public Sector Commission (VPSC) and other agencies as required.

3. Mandatory requirements

3.1 Mandatory requirements

Standing Direction 3.7.1 – Risk Management Framework and Processes directs that the responsible body (the Board) must ensure that the organisation complies with the mandatory requirements set out in the VGRMF. The responsibility for FCARMB's risk management performance rests primarily with the responsible body.

Mandatory requirements of the VGRMF

3.1.1 Risk management requirements

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

- The organisation 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*; and
  - *a positive risk culture in FCARMB is able to be demonstrated*.
- the risk management framework defines FCARMB's risk appetite;
- it is clear who is responsible for managing each risk;
- shared risks are identified and managed through communication, collaboration and / or co-ordination by the impacted organisations and stakeholders;
- FCARMB contributes to the management of state significant risks, as appropriate;
- risk management is embedded in FCARMB's strategic planning and decision making processes and demonstrates consideration of the organisation's material risks;
- adequate resources are assigned to risk management; and
- the risk profile and risk appetite of FCARMB is reviewed at least annually.

3.1.2 Insurance requirements

Where FCARMB is required to insure with VMIA (as defined by the VMIA Act) it 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 relevant 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 of retained financial risks;
- ensure claims management practices for retained financial risks are in place and that FCARMB maintains relevant claims data and has this information available to VMIA on request;
- work towards minimising exposure to insurable risk in line with s23 of the VMIA Act.

3.2 Attestation requirements

Under Standing Direction 5.1.4 – Financial Management Compliance Attestation, FCARMB must provide an annual attestation of compliance with applicable requirements of the FMA, the

Standing Directions (incorporating this framework) and the Instructions - including those relating to risk management - and disclose all material compliance deficiencies.

FCARMB 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.

Mandatory requirements for attestation under Standing Direction 5.1.4

3.2.1 For the risk management and insurance requirements, FCARMB must:

- conduct an annual review of its compliance with risk management and insurance requirements (in addition to compliance with all Standing Directions requirements);
- attest in FCARMB's annual report that it has complied with all Standing Directions - including Standing Direction 3.7.1: Risk management framework and processes - or, if it is partially in compliance, identify areas of non-compliance and remedial actions taken in the attestation; and
- ensure FRAC reviews and monitors compliance with Standing Directions 5.1.4 and 3.7.1, and advises the responsible body on the level of compliance attained.

3.2.2 Guidance material in support of attestation requirements

For the purposes of FCARMB attestation, and to ensure compliance with Standing Direction 5.1.4, FCARMB will use the recommended format, prescribed below:

Sample Attestation
Statutory Authority and other relevant agency I, (Name, on behalf of the Responsible Body, certify that the (name of agency) has complied with the applicable Standing Directions made under the *Financial Management Act 1994* and Instructions.

FCARMB may amend the wording of the attestation having regard to its risk profile, risk management maturity and operating context. In the event that FCARMB has only partially complied with the Standing Directions, the attestation must include an explanation of remedial actions to address areas of partial compliance.

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 on concepts to support FCARMB address the mandatory requirements.

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.

3.3.1.1 Shared risks

Agencies must contribute to the management of shared risks. To clearly demonstrate this requirement, FCARMB 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 FCARMB does not have line of sight. Communication channels could include periodical interagency meetings, shared systems or emails, formal agreements, etc. 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.
- There may be instances where the agencies are unable to come to an agreement on the lead agency and in such a scenario, assigning the lead agency will be determined by the Risk IDC.

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

- identifying current and emerging risks and other agencies/bodies 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 at a minimum.

3.3.1.2 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.

If a state significant risk is brought to FCAMRB's attention, the organisation will 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, FCARMB must be satisfied that it has contributed 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

FCARMB must make best use of its 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 FCARMB on insurable risk transfer opportunities. DELWP is accountable for providing oversight on FCARMB's insurance and risk arrangements.

The level of insurance required should be based on FCARMB's risk profile and tolerance, past claims experience, and 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, then FCARMB's risk management framework should set out an alternative response to address the risk.

Where FCARMB elects to self-manage claims, the organisation must ensure that it is appropriately resourced to manage those claims effectively. Where applicable, FCARMB is 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 every person in the agency believes that thinking about and managing risk is part of their job.

To encourage a positive risk culture, FCARMB should understand 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 FCARMB's Accountable Officer is responsible for setting, owning, instilling and overseeing an appropriate risk culture.

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

- understanding FCAMRB's current risk culture and defining the desired risk culture;
- identifying any gaps between the agency's current risk culture and desired risk culture; and
- defining FCAMRB's approach to evolve its risk culture to close gaps over time.

3.3.4 Risk Appetite

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

Defining FCARMB's material risks of and the level of risk acceptable 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 FCARMB 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 FCARMB's risk tolerance levels. The Executive team should identify the strategic objectives of FCARMB where a level of increased risk taking would be accepted in pursuit of these objectives.

3.4 Guidance to support better 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 organisation'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 FCARMB'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 FCARMB's risk appetite;
  - the risk owner may be required to undertake further analysis to better understand the risk; or
  - FCARMB may need to reconsider objectives.

3.4.2 Key Risk Indicators

Key Risk Indicators (KRIs) provide insight into the future 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.

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.

The organisation 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 etc;
- 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 the 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 maturity that FCARMB operates at in terms of its risk processes and procedures. Risk maturity is not a static concept and should be tailored to reflect the FCARMB's strategic objectives. As the organisation and its environments change, risk management evolves to ensure that it continues to support the achievement of objectives. FCARMB should consider developing and implementing strategies to improve its risk maturity (or maintain it at the desired level) alongside all other aspects of the organisation.

FCARMB undertakes a self-assessment of its risk maturity using the VMIA's on-line Risk Maturity Assessment (RMA) service. This tool enables FCARMB to benchmark against similar organisations and across all VGRMF agencies, as well as the development and monitoring of action plans to improve the organisation's risk maturity.

3.4.4 Control Effectiveness Testing

Control effectiveness testing involves regular reviews of FCARMB'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 where the organisation has a stable control environment, a mature risk management framework and resources able to perform the work involved.

Controls testing and validation is important in ensuring that the organisation is reviewing its risks and developing effective methods to minimise these where possible. FCARMB will develop its controls framework to more effectively mitigate risk. The establishment of a strong controls framework includes:

- Defining a controls library, which may be appropriate for an entity with low to medium risk maturity as it 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 designated 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; and
  - Regular review and testing of key controls by either re-performing the control or observing / inspecting that the control is working.

3.4.5 Additional guidance and risk management support

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. Where FCARMB policy is reviewed, or deemed deficient, upon annual review or Ministerial directive, FCARMB will refer to the VMIA website for contrast and to access VMIA Risk Management Guidelines outlining sound practice in implementing an effective risk management framework and complying with Standing 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.

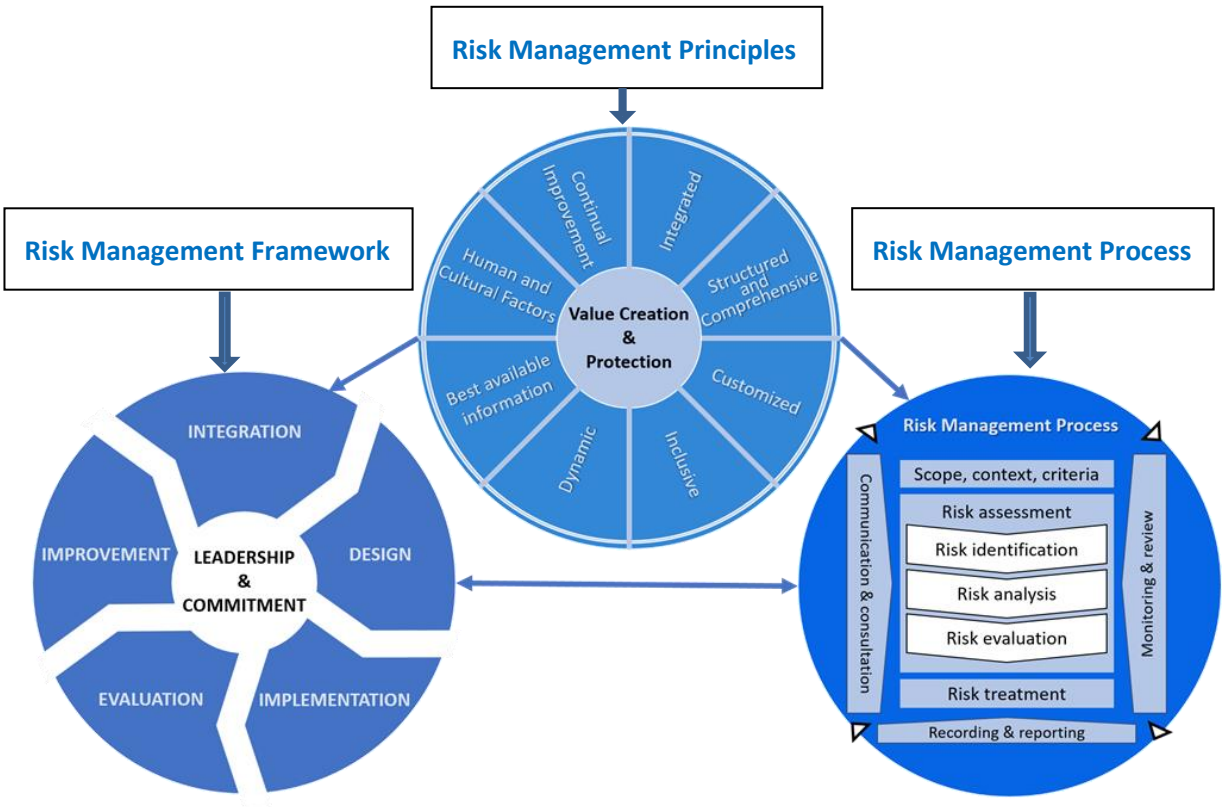
The VMIA website is at www.vmia.vic.gov.au.

4. AS ISO 31000:2018 Risk Management - Guidelines

FCARMB recognises that the approach to managing risk needs to be appropriate and tailored to its activity, size, complexity and risk profile. However, in order to conform to the prescribed approach to risk management, FCARMB undertakes to ensure that it is consistent with the revised risk management standard AS ISO 31000:2018 Risk Management - Guidelines.

FCARMB undertakes that, where applicable and based on assessed and appropriate evaluation of its risk tolerances, the following risk management principles, framework and processes will be adopted from AS ISO 31000:2018 Risk Management - Guidelines.

The below diagram shows the interconnectivity of the 3 main risk management elements of principles, framework and process within the revised standard AS ISO 31000:2018 Risk Management – Guidelines.



AS ISO 31000:2018 Risk Management – Guidelines

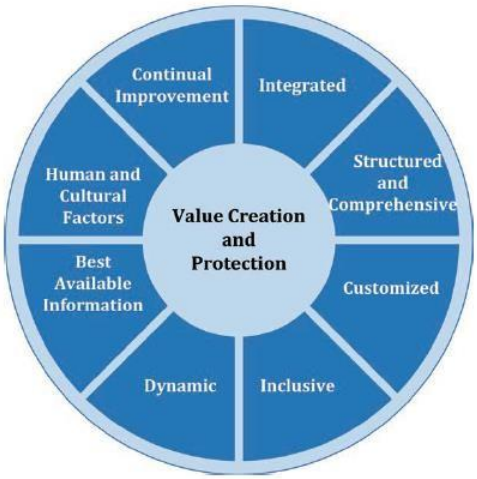
4.1 Principles of risk management

The purpose of risk management is the creation and protection of value.

The revised standard states that the 8 principles of effective and efficient risk management are:

- Integrated - risk management is an integral part of all organisational activities;
- Structured and comprehensive - approach to risk management contributes to consistent and comparable results;
- Customised – risk management framework and processes are customised and proportionate to the agency;

- Inclusive - appropriate and timely involvement of stakeholders will drive improved awareness and informed risk management;
- is an integral part of the agency's processes;
- Dynamic - risks can emerge, change or disappear and risk management anticipates, detects and responds to these changes;
- Best available information – inputs to risk management are based on historical and current information, as well as future expectations;
- Human and cultural factors influence all aspects of risk management; and
- Continuously improved through learning and experience.



AS ISO 31000:2018 Risk Management – Guidelines, Figure 2, p4

4.2 Risk management framework

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

Leadership and commitment –to ensure the ongoing effectiveness of risk management in their organisation, top management and oversight bodies should ensure that risk management is integrated into all organisational activities. This commitment should be reinforced through communication of the value of risk management and its impact within the organisation.

Integration – Risk should be managed in every part of the organisation's structure. The integration of risk management should be a dynamic and iterative process, customised to the organisation's needs and culture and be included as part of the purpose, governance, leadership and commitment, strategy, objectives and operations.

Design – to ensure the risk management framework takes into account all the needs of the organisation, the design of the framework should consider the following: an understanding of the organisation and its context, an articulation of the risk management commitment, assigning of roles, responsibilities and accountabilities, allocation of resources and establishment of communication and consultation.

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

Evaluation – FCARMB should periodically evaluate the effectiveness of the risk management framework against its purpose, implementation plans, indicators and expected behaviours to ensure it is suitable in supporting the achievement of the organisation's objectives.

Improvement– The organisation should continuously look to adapt and improve their risk management framework. To ensure the effectiveness of the framework, relevant gap and improvement opportunities should be identified and implemented

AS ISO 31000:2018 Risk Management – Guidelines, Figure 2, p11

4.3 Risk management process

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

- ***Communication and consultation*** take 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.
- ***Scope, context and criteria*** means understanding FCARMB'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 assessment*** involves the identification of risks that could prevent an organisation from achieving its objectives, the analysis of the nature of the risk and its potential consequences and the evaluation of what action is required. This assessment may take into account risks with sources not under control of the organisation and may affect one or more objectives of the organisation.
- ***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.
- ***Monitoring and review*** provides assurance over the quality and effectiveness of the risk management framework and should take place in all stages of the process.
- ***Recording and reporting*** ensures that all outcomes from the risk management process are documented and reported to provide information for decision making and improvement of risk management activities.

5. Risk Rating Criteria and Guidelines

Illustrative Likelihood Rating Scale

Likelihood Rating	Descriptor	Definition	Indicative Frequency
5	Almost certain	The consequence is expected to occur on an annual basis	Every year or more frequently
4	Likely	The event has occurred several times or more throughout history of the organisation	Every three years
3	Possible	The event might occur once in the organisation	Every ten years
2	Unlikely	The event does occur from time to time	Every thirty years
1	Very Unlikely	Hear of something like that occurring elsewhere	Every hundred years

Risk Description

Risk Level	Description
Very High	Requires ongoing executive lever oversight. The level of risk warrants that all possible mitigation measures be analysed in order to bring about a reduction in exposure.
High	Action plans and resources required. The level of risk is likely to endanger capability and should be reduced through mitigation strategies where possible.
Medium	This level of risk should not automatically be accepted for risk mitigation but rather a cost-benefit analysis is required to determine if treatment is necessary.
Low	Treatment when resources are available. The risk should be managed via existing controls and normal operating procedures.

Consequence Matrix

Likelihood						
	5	Medium (5)	High (10)	Very High (15)	Very High (20)	Very High (25)
	4	Low (4)	High (8)	High (12)	Very High (16)	Very High (20)
	3	Low (3)	Medium (6)	Medium (9)	High (12)	Very High (15)
	2	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
	1	Low (1)	Low (2)	Low (3)	Medium (4)	High (5)
		1	2	3	4	5
		Consequence				

Control Effectiveness Rating

Control Rating	Descriptor	Definition
3	High	Control operating effectively, no deficiencies noted
2	Medium	Some deficiencies in the control have been identified however there are compensating controls to cover identified faults
1	Low	Significant control deficiencies have been identified

Authorisations and Document Parameters

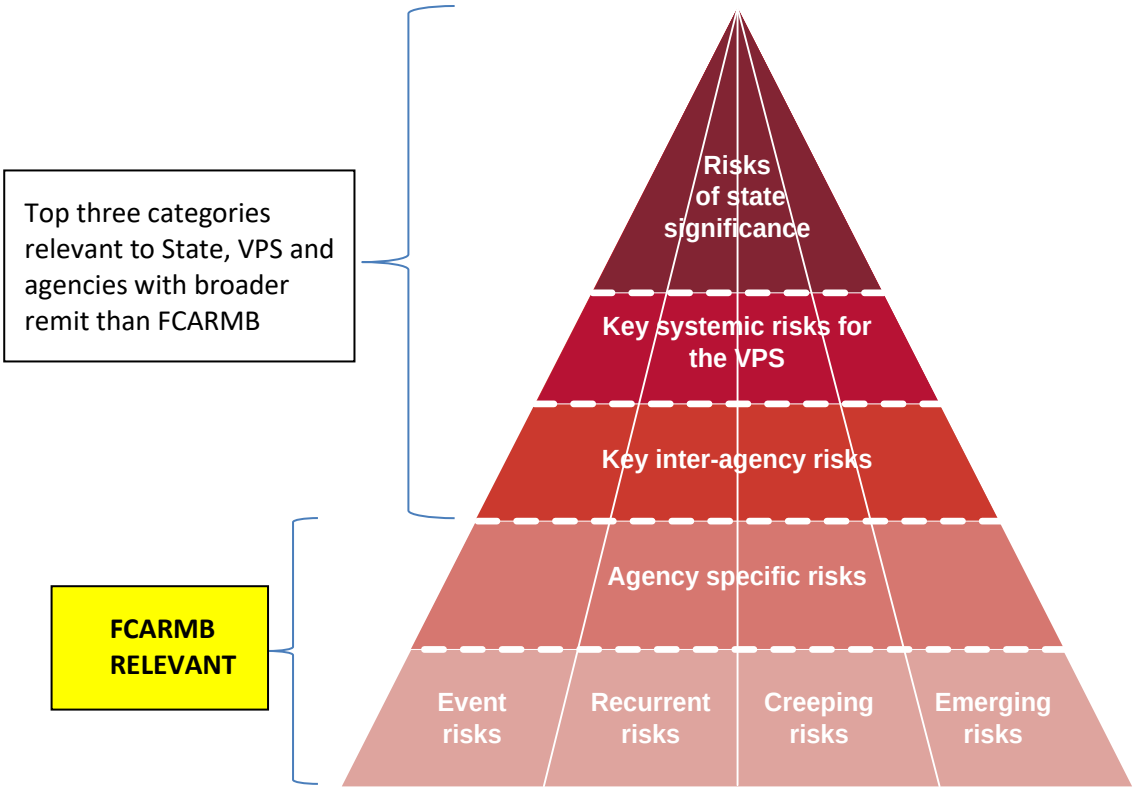
Document Title:	BP 1.5(a) Risk Management Framework		
Document Subject:	Framework for FCARMB's risk management based on VGRMF and Risk Management Standard ISO31000:2018 requirements.		
Author:	CEO - Stuart Smythe	**Owner (Title):**	CEO
Contributors:	DCS – Craig Thompson	**Authorised By:**	FCARM Board
Filepath:	T:\14. Policies & Work Practices\14.02 Board Policies\14.02.01 Approved\BP 1.5(a) Risk Management Framework (2019).docx		
First Adopted:	27 March 2017	**Status:**	Approved
Last Amended:	21 October 2019	**Next Review:**	21 October 2020
Last Amendment approved by:	FCARM Board	**To be approved by:**	FCARM Board
Revision No:	4	**Replaces:**	**3**
Amendment summary	Version 4 (Aug 2019) – Comprehensive revision following update of ISO Risk Management standard, the VGRMF and changes to Standing Directions naming and attestation requirements.		

Appendix 1 – Introduction to risk management

FCARMB has referred 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.

The FCARMB categorisation of risk and approach to risk management (where applicable) 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.

FCARMB specific risks are risks that can be managed entirely within its operations and can generally be well understood and effectively managed with straight forward risk management processes.

Shared risks (inter alia Alpine Resorts) are risks shared by two or more agencies that require co-ordinated management by more than one agency. The responsibility for managing a shared risk is shared by all the relevant agencies and will benefit (ARCC) from a co-ordinated 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 statewide 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 FCARMB 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 **risk profile** for FCARMB 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.

A positive **risk culture** is one where every person in FCARMB believes that thinking about and managing risk is part of their job.

Risk management needs to be incorporated into the **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.

FCARMB maintains 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

In respect of FCARMB risk policy and procedures, the following provides a broad definition / overview of terms applied (Note: these are not definitions or standards). More detailed explanations and guidance is included in VMIA guidance materials. See also ISO Guides 73:2009 which provides the basic vocabulary and understanding of risk management concepts.

Term	Description
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.
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.
Key risk indicator	A metric used to measure the likelihood of a risk event. They provide an early signal of increasing risk exposures.
Likelihood	Chance of something happening. In risk management, 'likelihood' is used to refer to the change of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.
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 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 can be applied at different levels.
Risk analysis	Process to understand the nature of the risk and to determine the level of risk.
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 attitude	The organisation's approach to assess and pursue, retain, take or turn away from risk.
Risk 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.
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 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 organisation believes that thinking about and managing risk is part of their job.
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	Co-ordinated activities to direct and control an organisation with regard to risk.
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 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 maturity	The benchmarking of an organisation'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 register	Record of information about identified risks.
Risk source	Element which alone or in combination has potential to give rise to risk.
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 / acceptance	The organisation's readiness to bear / accept the risk after risk treatment in order to achieve objectives. Risk tolerances / acceptances 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.
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Appendix 2 – Definitions

Agency	Any department or public body as defined in the *Financial Management Act1994.*
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.* For FCARMB, the Accountable Officer is the CEO.
ARCC	Alpine Resorts Co-ordinating Council, as defined under Part 3 of the *Alpine Resorts (Management) Act 1997*.
Audit Committee	The Standing Directions 2018 Under the *Financial Management Act 1994* 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 (Board) which has been formulated to deal with issues of a specific nature.
Responsible Body	For FCARMB, the Board is the Responsible Body, being the body with ultimate decision-making authority.