Risk Management Policy

Purpose	This policy sets out the key requirements, roles, and responsibilities in relation to risk management at the City of Port Phillip.
Policy outcome	A mature risk management program and corresponding healthy risk culture is essential for: • Positioning Council to fulfil the objectives as outlined in the Council Plan • Protecting people from injury and preserving life • Ensuring best use of Council resources through integration with operations, enterprise planning, reporting, asset management, and project management • Understanding risk-reward trade-off when assessing opportunities • Ensuring the long-term sustainability of the organisation • Prioritising the treatment of catastrophic and high risks • Driving appropriate corporate governance
Responsible area	Governance and Organisational Performance
Version	Version 3.0
Date adopted by Council	6 September 2023
Planned review date	2 years from date endorsed by Council
Expiry date	6 September 2027

Definitions

Term	Definition
Controls	Measurable activities that are intended to modify the level of risk.
Risk	The effect of uncertainty on objectives.
Risk management	The coordinated activities (culture, processes, and systems) to direct and control an organisation with regard to risk.
Risk Management Framework	Companion document to the Risk Management Policy which details the tools, structures, and processes to be implemented across Council in order to meet the requirements of the Policy.
Risk tolerance	The level of risk Council is prepared to accept, tolerate or be exposed to at any point in time.
Risk treatment strategy	Documented actions to reduce a level of risk to within tolerances.
Three lines model	A key governance tool for establishing and maintaining sound risk management disciplines and controls throughout the organisation. (First line) Risk owners. Operational managers and their staff. (Second line) Risk advisers. Various risk and compliance functions to advise, help build, and monitor first line controls. (Third line) Audit. An independent function that evaluates and assures the effectiveness of controls.

Scope and responsibilities

This policy applies to Councillors, staff, volunteers, contractors, and service providers engaged to conduct Council business. The policy contributes directly to the achievement of all strategic objectives outlined in the Council Plan.

Role	Responsibility
Council	Approve the Risk Management Policy and note the Risk Management Framework (RMF). Appoint the Audit & Risk Committee. Be satisfied that the RMF is embedded and effective, and that risks are identified, managed, and controlled appropriately. Provide adequate budgetary provision for risk management strategies to be implemented.
Audit & Risk Committee	Oversee the implementation, operation, and effectiveness of the RMF. Consider the adequacy of actions taken to reduce exposure of key risks to acceptable risk levels. Commission and oversee specific projects or investigations aimed at assessing risk management, including suspected cases of fraud. Consider the risk profile when developing and implementing the Internal Audit and Compliance Program. Review Project Portfolio and associated risks.
Internal Auditor	Consider the risk profile when developing and implementing the Internal Audit and Compliance Program. Audit Council's risk management practices against Policy and RMF requirements, including assessment of effectiveness of internal controls. Report audit outcomes to Audit & Risk Committee.
Executive Leadership Team / SRIA	Endorse the Risk Management Policy. Approve the Risk Management Framework. Actively manage key strategic and operational risks across the organisation – ensuring appropriate resources for risk management actions are made available. Drive and champion the proactive and appropriate management of risk across the organisation.
Risk & Assurance Coordinator	Lead and manage implementation of RMF. Provide staff with continued access to adequate training in risk management, provision of risk advice, undertaking risk assessments, and other support. Champion and quality assure risk management across the organisation. Drive second line assurance of controls and agreed treatment actions. Manage risk reporting to Council, ARCO, SRIA and others as required.
Managers / Leadership Network	Drive and champion the proactive and appropriate management of risk within the department. Complete and submit the annual Departmental risk attestation. Encouragement and reinforcement of positive risk management behaviours and risk culture.
Staff, contractors, and service providers	Understand key obligations around risk, compliance, and incident management when engaging in workplace activities. Speak up when an incident occurs, or something seems out of place.

Policy statement and objectives

1. Council will maintain a Risk Management Framework (RMF) to articulate the tools, structures, and processes in place to best meet the objectives of the Risk Management Policy.
2. Council will use the Three (3) Lines Model to operationalise the RMF components, allocating responsibilities to (1) risk owners, (2) risk advisers, and (3) audit functions.
3. Council will align the RMF to the Australian / New Zealand ISO Standard on Risk Management (AS/NZS ISO 31000:2018).
4. Council will maintain active risk registers to manage key strategic, operational and project risks. Responsibility for management and governance of each risk area is as follows:

Risk Area	Ownership	Governance / Visibility	Considerations
Strategic	Strategic Risk and Internal Audit Group	Council (Annually) ARCO (Annually) SRIA/ELT (quarterly)	To be reviewed as required by Council / SRIA / ARCO quarterly and as part of the Business Planning process.
Operational	Department Managers	Council (annually) ARCO (quarterly) SRIA/ELT (monthly + deep-dive bi-monthly)	Catastrophic and High risks to be reported to SRIA/ELT monthly. Divisional / Department deep dive bi-monthly or as agreed by SRIA/ELT.
Project	Project Managers	Council (quarterly) Community (quarterly)	Project Manager to customise RMF tools to project. Typical risk consequences would be specified in terms of impacts on time, budget, or benefits / quality.

5. Managers will complete an annual risk management attestation – to confirm that:
    a. The departmental operational risk register has been reviewed and updated in the last 12 months;
    b. Any material emerging risks have been escalated to an officer level where appropriate action can be taken or formally reported to the Strategic Risk & Internal Audit Group (SRIA) for consideration.
6. A summary of all key risks, controls, and treatment actions will at a minimum:
    a. Be considered by the Council at the commencement of the annual planning process
    b. Be considered by the Audit and Risk Committee at each Committee meeting
    c. Be used as input to the annual development of the Internal Audit and Compliance Plan
    d. Be considered monthly by the Executive Leadership Team/SRIA.
7. Residual risk levels will be assessed for treatment based on the risk treatment table outlined in the RMF. Typically, any risks with Catastrophic or High risk levels will require ELT/SRIA management and prompt treatment.

Imbedded 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, Council will consider how the following key principles of effective risk culture work in practice:

- Tone from the top;
- Accountability;
- 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 and business outcomes and that they are ultimately responsible for setting, owning, imbedding and overseeing the desired risk culture. Imbedding the desired risk culture would include:

1. understanding the Councils current risk culture and defining the desired risk culture;
2. identifying any gaps between Council's current risk culture and desired risk culture; and
3. defining Council's approach to evolve its risk culture to close gaps over time.

Related legislations and documents

Local Government Act 2020

Occupational Health & Safety Act 2004 & Regulations 2017

Safety & Wellbeing (CoPP Safety Management System SMS including Hazard Registers)

Victorian Government Risk Management Framework (VGRMF)

AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines

Risk Management Framework

Fraud & Corruption Awareness & Prevention Policy

Legislative Compliance Framework

Business Continuity Framework