Risk Management Policy

Policy Owner	EM, Service & Business Improvement	TRIM folder	*50/01/123*
Noted by	*ELT*	Noted date	*April 2017*
Adopted by	*Council*	Approval date	*June 2017*
		Next Review date	*June 2019*
		Review frequency	*2 years*

Risk Management Policy

April 2017

1. PURPOSE

1.1 The Council has significant legislative, financial, service delivery, asset management, and contractual responsibilities. It has a duty of care to councillors, employees, contractors, volunteers, the community, broader public and environment.

1.2 It is incumbent on Council to understand and manage the strategic, operational and project risks and opportunities it faces to enable it to make informed decisions and meet its responsibilities, council priorities and community expectations.

1.3 This policy sets out the key requirements, roles and responsibilities in relation to risk management at the City of Port Phillip. It is designed to embed an advanced risk management culture.

2. SCOPE

2.1 This policy applies to councillors, council staff, volunteers, contractors and service providers engaged to conduct authorised Council business.

3. GUIDING PRINCIPLES

3.1 Council has moral, financial and legal responsibility to effectively manage risk and opportunities in all areas of its operations.

3.2 Risk management is an essential element of corporate governance and will be integrated into enterprise planning, reporting, asset management and project management.

3.3 Council will take a risk-based approach to managing risks based on the severity of the risk and effectiveness of controls. Management of catastrophic and high risks will be prioritised.

3.4 Council will embed and resource the Three Lines of Defence Model (see definitions) including (1) operational managers (2) specialist risk roles and (3) audit.

4. POLICY

Risk Management Framework

4.1 The Council will maintain a Risk Management Framework detailing its approach to risk management and to provide a consistent methodology to assess, prioritise and manage risk.

4.2 The Risk Management Framework will be approved by the Executive Leadership Team (and noted by the Audit & Risk Committee and Council) and reviewed at least every two years.

4.3 The Framework will be aligned to the Australian/New Zealand ISO Standard on Risk Management (AS/NZS ISO 31000:2009).

Strategic Risk Management

4.4 Council will maintain a strategic risk register including the key risks in the external and internal operating environment that could materially impact the delivery of the Council Plan.

4.5 A summary of strategic risks, controls and improvement actions will at a minimum:

- be considered by the Council at the commencement of the annual planning process (usually December)
- be considered by the Audit and Risk Committee (ARCO) as part of development of the Internal Audit and Compliance Plan (usually May)
- be considered by the Executive Leadership Team (ELT) on a quarterly basis.

4.6 A separate risk appetite will be set for each individual strategic risk and tolerance levels agreed. Where possible these tolerance levels will be quantified.

4.7 Any material negative changes in strategic risks will be reported to the ELT, ARCO and Council as soon as practical.

4.8 The CEO will delegate management of strategic risks to a General Manager or Manager.

Operational Risk Management

4.9 Council will maintain an operational risk register including the key risks faced by each department in the internal operating environment.

4.10 Managers are accountable for the management of operational risks within their respective departments.

4.11 While risk management will be continuous, a full operational risk review will be conducted by divisional leadership teams at the start of the annual planning process each year.

4.12 A separate risk appetite will be set for each operational risk in the form of a target risk rating. In general, the following minimum treatment will apply for each risk rating:

Risk Rating	Minimum treatment	Description
Very high risk (Catastrophic)	Reject and avoid or mitigate	Immediate action required in consultation with ELT to either avoid the risk entirely or to reduce the risk to a low, medium or high rating
High risk	Accept and mitigate	These risks need to be mitigated with actions as required and managers need to be assigned these risks
Medium risk	Accept	Manage by specific monitoring or response procedures
Low risk	Accept	Manage by routine procedures

4.13 The status of catastrophic, high and any operational risks outside the target risk rating will be reviewed and reported monthly to divisional management and quarterly to ELT.

4.14 Any material negative change in operational risk will be reported to the ELT and where appropriate ARCO and Council as soon as practical.

4.15 Operational risks will be reviewed and where appropriate updated as part of internal and external audits or following a material event eg restructure, system change, injury.

Project risk management

4.16 Risk management will be integrated with the project management framework including key decision making and reporting processes.

4.17 The status of high priority projects will be reported at least quarterly to the Council and community.

Risk Management Awareness and Capability

4.18 Councillors, staff and where required volunteers and contractors will be appropriately briefed in relevant risk management principles, practices and processes.

4.19 Those staff with specialist risk and compliance roles will be supported to develop and maintain appropriate qualifications.

5. KEY ROLES & RESPONSIBILITIES

Council

5.1 Approve the Risk Management Policy and note the Risk Management Framework.

5.2 Be satisfied that strategic risks are identified, managed and controlled appropriately.

5.3 Appoint the Audit and Risk Committee.

Audit & Risk Committee

5.4 Oversee the Risk Management Framework and review the mechanisms in place to comply with the framework.

5.5 Monitor the systems and process via the council's risk profile and consider the risk profile when developing and implementing the Internal Audit and Compliance Program.

5.6 Consider the adequacy of actions taken to ensure that the risks have been dealt with in a timely manner to mitigate exposures to the Council.

5.7 Identify and refer specific projects or investigations deemed necessary to assess risk management through the Chief Executive Officer, the internal auditor and the Council.

5.8 Oversee any subsequent investigation, including the investigation of any suspected cases of fraud.

5.9 Review Project Portfolio and associated risks.

Internal Auditor

5.10 Considering strategic and operational risks in the development and implementation of the Internal Audit and Compliance Plan and recommending improvements.

5.11 Periodically auditing Council's Risk Management practices and providing recommendations on improvement to management and the Audit and Risk Committee.

Executive Leadership Team

5.12 The CEO, supported by the General Manager Organisational Performance, is accountable for ensuring appropriate risk management within Council.

5.13 Endorse the Risk Management Policy for approval by Council, approve the Risk Management Framework, and monitor implementation.

5.14 Provide executive leadership in the management of strategic, operational and project risk and generally champion risk management within Council.

5.15 Ensure that their respective divisional risk profile as entered by each department is reviewed, updated and approved quarterly (monthly for high> risks);

5.16 Report expeditiously to ARCO on any fraud and corruption incidents or material risk mitigation failures and actions taken.

Executive Manager Service and Business Improvement

5.17 Provide assurance in the development, implementation and review of the Risk Management Policy, Risk Management Framework, and general risk management practice within Council.

5.18 Quality assure enterprise risk management reporting to the ARCO, Council and the ELT.

5.19 Ensure the organisation has the appropriate culture, capability, processes and systems to deliver on this policy and the Risk Management Framework.

Risk & Assurance Coordinator

5.20 Lead the development, implementation and review of the Risk Management Policy, Risk Management Framework, and supporting processes and systems.

5.21 Develop, maintain and quality assure enterprise risk registers and monitor implementation of controls and agreed treatment actions.

5.22 Preparing various risk management reports to the Council, ARCO, ELT, and divisional leadership teams in accordance with this policy and the Risk Management Framework.

5.23 Provide risk management training, advice and support and conduct risk assessments as agreed with the ELT or Senior Management.

5.24 Liaise with the Internal Auditor and provide secretariat support to the Audit and Risk Committee.

5.25 Measure enterprise risk management maturity and report on the implementation of actions to achieve target maturity.

Managers

5.26 Ownership of risk management within their department or as delegated by the CEO in accordance with this policy and the Risk Management Framework.

5.27 Championing risk management within their department and appropriate risk management practice by staff, volunteers, contractors, and service providers.

Staff, contractors and service providers

5.28 Applying risk management practices in their area of work and ensuring that management are aware of risks associated with council's operations.

5.29 Recommending or providing suitable plans to manage risks; obtaining appropriate approval prior to action (where required); and reporting on risk management practices.

6. DEFINITIONS

Risk The effect of uncertainty of objectives. Risk is measured in terms of the likelihood of an event occurring and the consequence (impact)

Risk appetite The level of risk Council is prepared to accept, tolerate or be exposed to at any point in time. Once the risk appetite threshold has been breached, risk management controls and actions are required to bring the exposure level back within the accepted range

Risk management The coordinated activities (culture, processes, and systems) to identify, analyse, mitigate, monitor and report risks

Controls Measurable activities that are intended to modify the level of risk

Risk treatment strategy Additional activities should the level of risk remain unacceptable after controls are applied

Three lines of defence model (First line): Operational managers own and manage risk (Second line): various risk and compliance functions to help build &/or monitor first-line-of-defence controls. (Third line): Audit provides assurance on the effectiveness of controls.

Monitoring Continual checking or surveillance to determine the status and effectiveness of controls / treatments

7. LEGISLATION AND OTHER REFERENCES

- Local Government Act 1989
- Occupational Health & Safety Act 2004
- AS/NZS ISO 31000:2009 *Risk Management – Principles and Guidelines*
- City of Port Phillip Risk Management Framework 2017
- Fraud Control and Management Policy
- Legislative Compliance Framework
- Business Continuity Policy ** currently under development

14.3 APPENDIX 1: RISK LEVEL MATRIX *(extract from Risk Management Framework)*

		Rare	Unlikely	Possible	Likely	Almost Certain
		Event may occur in exceptional instances & needs unlikely factors to occur together. Risk unlikely to have occurred before.	Event unlikely to occur (1 in 5 year period). For risk to eventuate need single or couple of unlikely factors. Risk may have occurred before.	Event expected to possibly occur in a 3 year period. Risk is unlikely to be part of business process. For risk to eventuate likely to need multiple factors to occur.	Event expected to occur at least annually. Risk is possibly part of routine business process & can occur a number of times per annum.	Event expected to occur regularly per annum. This risk is part of daily business operations. If controls removed the risk would certainly eventuate on a daily to weekly basis.
Extreme	Likely to impact Council in such a way that it would take a significant amount of time to recover, if at all. Timeframes > 10 to 15 years, e.g. closure of whole business or significant part of it.	Medium	High	Catastrophic	Catastrophic	Catastrophic
Major	Would significantly challenge Council & take considerable amount of time to get over. It wold take between 3 - 10 years to recover from.	Medium	Medium	High	High	Catastrophic
Moderate	Would need involvement from ELT to resolve. May take between 1 month & 1 year to overcome & up to 3 years to recover from.	Low	Medium	Medium	High	High
Minor	Some impact which can be dealt with through some ELT involvement & in normal day-to-day operations. May need up to a few months to resolve & overcome.	Low	Low	Medium	Medium	High
Insignificant	No real impact to Council & would be deal with in the day-to-day operational process. Can be resolved in a few weeks.	Low	Low	Low	Low	Medium

Consequence

Likelihood

14.4 APPENDIX 2: RISK TREATMENT MATRIX *(extract from Risk Management Framework)*

The matrix is broken into four shaded areas reflecting the increasing level of risk.

The table below is used to determine how a risk should be treated once it has been identified and assigned Residual risk rating. The Residual risk rating is used to determine the level of action and focus required to further mitigate the risk and the level of involvement from each group of management required to develop strategies, including costs and resources and to identify new treatment plans to strengthen the existing control environment.

🟩	= Low Risk
🟨	= Medium Risk
🟧	= High Risk
🟥	= Catastrophic Risk

Risk Rating	Risk Acceptibility	Accountability	Actions Required	Risk Treatment Guidelines
Extreme	Unacceptable	CEO or Council	Urgent	• Risk is unacceptable. Likely to prevent achievement of objectives • Treatment plans / controls require CEO/Council input / sign-off • Risk owned by CEO • Controls (cost/implementation) may not be viable leading to cessation of activity/program • Very regular monitoring & reporting to ELT & governance committee
High	Unacceptable	Executive Leadership Team	Important	• Risk unacceptable. May prevent achievement of objectives. • Treatment plans / controls require detailed planning & decision making by Executive & implementation by project team • Risk owned by ELT level • Control owner assigned to ensure risk treatment implementation is effective • Requires regular monitoring and monthly reporting to ELT
Council will not accept >High level risks. Risk treatment strategies must be undertaken to modify the risk: (by reducing the consequence or likelihood / transferring the risk / eliminating the risk or retaining the risk by informed)				
Moderate	Tolerable under certain situations	Department or General Manager	Operational	• Management ownership & controls identified and generally managed within normal budget parameters • Risk is regularly monitored to ensure risk exposure is managed effectively • Investigate feasibility of risk treatment strategies for any Medium risks with controls identified as 'Fair' or 'Poor' • Risk may be shared / transferred i.e. insurers • Risk reported to ELT on 3 monthly basis as part of normal risk reporting cycle
Low	Acceptable	Department Manager or Coordinator	Capture in risk register	• Accept the risk as it is as it is within acceptable risk tolerances. • Ensure risk is captured • Risk should be managed via routine procedures & internally reporting