City of STONNINGTON

Risk Management Policy

VERSION 12.0

1.0 - Introduction

- Enterprise Risk & Opportunity Management Framework (ER&OMF)
  - > Risk Appetite statement
  - > Risk tolerance range
- Risk Management Policy
- Audit & Risk Committee Charter
- Risk Register – Pulse
- Risk Procedure

2.0 - Purpose

To integrate and optimise risk management systems to deliver performance improvement and value to Council. To provide clarity to all stakeholders on their roles and responsibilities within the risk management system. To meet Council's statutory and contractual obligations in the management of strategic, operational and corporate risks.

3.0 - Scope

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

4.0 - Policy

Risk Management Framework

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

4.2 The Risk & Opportunity 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 31000:2018) and Victorian Government Risk Management Framework (VGRMF).

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 tasks will at a minimum be:

- reviewed by the Council at the commencement of the annual planning process (usually December)
- reviewed by the Audit and Risk Committee (ARC) as part of development of the Internal Audit and Compliance Plan (usually May)
- reviewed by the Executive Team (ET) 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 significant changes to strategic risks will be reported to the ET, ARC and Council as soon as practical. Significant changes include new and emerging risk and risk rating changes from high to catastrophic.

4.8 The CEO will delegate management of strategic risks to a Director or Chief.

Corporate Risk Management

4.9 Council will maintain a corporate risk register including the key risks which are across most or all departments and business units in Council. This includes human resources, IT, information security.

4.10 Directors, Chiefs or Managers are accountable for the management of corporate risks in consultation with the relevant departments.

4.11 While risk management will be continuous, a full corporate risk review will be conducted by directorates at the start of the annual planning process each year.

4.12 The risk rating table/matrix which forms part of the ER&OMF is to be referenced when rating Corporate risks. 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 (Major)	Accept and mitigate	Directors, Chief and Managers who are assigned ownership of the risk in Pulse need to ensure that controls are in place to mitigate these risks. The assigned owner is accountable for these controls and their effectiveness.
Medium Risk	Accept	Manage by specific monitoring or responce 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 ET.

4.14 Any significant changes to corporate risks will be reported to the ET, ARC and Council as soon as practical. Significant changes include new and emerging risk and risk rating changes from high to catastrophic.

4.15 Corporate 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.

Operational Risk Management

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

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

4.18 While risk management will be continuous, a full operational risk review will be conducted by directorate at the start of the annual planning process each year.

4.19 The risk rating table/matrix which forms part of the ER&OMF is to be referenced when rating operational risks. In general, the minimum treatment will apply for each risk rating as set out in the table above in risk rating table in 4.12:

4.20 The status of catastrophic, high and any operational risks outside the target risk rating will be reviewed and reported monthly to Director or Chief and quarterly to ET.

4.21 Any significant changes to operational risks will be reported to the ET, ARC and Council as soon as practical. Significant changes include new and emerging risk and risk rating changes from high to catastrophic

4.22 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

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

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

Risk Management Awareness and Capability

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

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

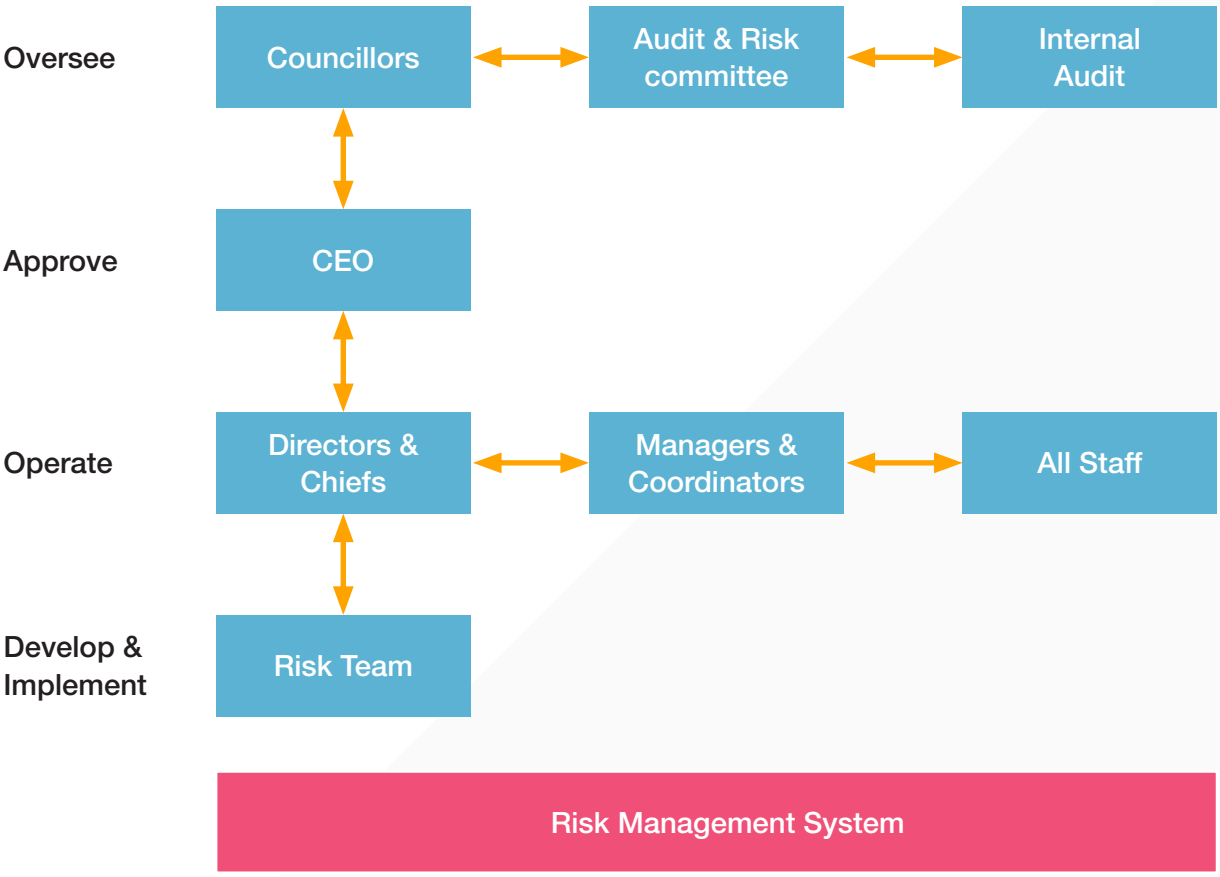
5.0 - Roles & Responsibilities

The roles and responsibilities for risk management at Council are specified in this policy, committee charters and individual success profiles.

	Roles & Responsibilities
Councillors	> Note the Risk Management Policy the Risk and Opportunity Management Framework. > Be satisfied that strategic risks are identified, managed and controlled appropriately. > Oversee the Audit and Risk Committee.
Chief Executive Officer	> Overall accountability for risk management. > Setting and role modelling the tone, culture and expectations for risk management and governance activities. > Ensuring resources for risk management activities as set out in the ER&OMF are adequate for Council purposes. > Setting appropriate delegations for the risk management functions. > The key point of contact between management and Councillors on risk management matters.
Audit & Risk Committee	> Independent oversight of Council's governance, risk management and control activities. > Advisory oversight of the internal audit function. > Oversee the Enterprise Risk and Opportunity Management Framework and review the mechanisms in place to comply with the framework.
Internal Audit	> Risk assurance to the CEO and Audit & Risk Committee through execution of the internal audit plan.
Directors and Chiefs	> Accountable for ownership and management of risks in their respective areas of responsibility, in accordance with the ER&OMF. > Role modelling the tone, culture and expectations for risk management and governance activities. > Working with the Risk team to identify, manage and report on strategic risks and significant insurance matters as set out in the ER&OMF within their directorate, including shared risks with other directorates and external stakeholders. > Accountable for the risk management performance of employee in their directorate.

	Roles & Responsibilities
Managers	> Managing risks in their respective departments, in accordance with the ER&OMF. > Working with the Risk team to identify, manage and report on risks and insurance matters within their respective departments, including shared risks with other departments and external stakeholders. > Responsible for the risk management training and performance of employees in their respective departments.
Coordinators	> Managing risks in their respective business units, in accordance with the ER&OMF. > Working with the Risk team to identify, manage and report on risks and insurance matters within their respective business units. > The effective operation of risk controls. > Timely escalation of risk and control matters through management. > Co-ordinating the risk management training and performance of employees in their respective business units.
Risk Team	> Leading the risk management function. > Developing and implementing a risk management framework that is fit for purpose. > Providing risk reporting to the Executive Team, Audit & Risk Committee and Councillors including new and emerging risks. > Supporting the organisation to manage its risks through: - Facilitation of risk profiling activities; - Provision of risk management training, advice and guidance to employees; and - Co-ordination of insurable risk treatments
All staff, contractors, volunteers and service providers	> Applying sound risk management practices in accordance with Council policies, frameworks and the ER&OMF. > Timely escalation of risk and control matters through management.

Enterprise Risk & Opportunity Management Roles & Responsibilities



6.0 - Definitions

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

Risk appetite
The amount and type of risk we are willing to accept to achieve objectives. It describes our attitude towards risk taking across the whole of the City of Stonnington.

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 Council believes that thinking about and managing risk is part of their job.

Risk management
Coordinated activities to direct and control the City of Stonnington with regards to risk.

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

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

3 Lines model

(First line): Directors, Chiefs and/or Managers own and manage risk
(Second line) various risk and compliance functions to help build &/or monitor first line 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

7.0 - Review

This document is to be reviewed by the Risk Coordinator annually from date of adoption by Council, with each review to be approved via a CEO Notice Paper.

Document Control			
Author:	Risk Coordinator	**QA:**	Chief People Officer
Owner:	Risk Coordinator	**Next Review:**	July 2022

Reviews and Updates			
Date	**Details**	**Version**	**Reviewer**
23 Sep 2014	Annual administrative review of document and insertion of Internal Audit recommendations regarding Risk Tolerance and the roles of the Audit Committee and EMT	1	Risk Coordinator
17 Nov 2015	Annual administrative review	2	Risk Coordinator
7 Feb 2017	Annual administrative Review	3	Risk Coordinator
20 Dec 2017	Annual administrative Review	4	A/Manager Risk Management & Contracts Compliance
5 June 2018	Review of wording following completion of 2017 Risk Register Review, changes to Risk Management Strategy and ISO31000:2018	5	Manager Risk, Safety & Assurance
6 July 2019	Policy disaggregation and up-date from risk management procedures	6	Coordinator Risk & Integrity
30 March 2021	Policy updated inline with organisation restructure	7	Risk Coordinator
July 2021	Clarity on Roles and Responsibilities	8	Risk Coordinator

8.0 - Supporting Reference Documents

1. Council Plan 2017–2021
2. Enterprise Risk & Opportunity Management Framework (ER&OMF)
3. Audit & Risk Committee Charter
4. Australian/International Risk Standard – AS/NZ ISO 31000:2018, *Risk Management – Guidelines*
5. Victorian Government Risk Management Framework (VGRMF)
6. Risk Register;
7. Risk Management Procedures;
8. Fraud & Corruption Control Policy; and
9. Codes of Conduct.

City of
STONNINGTON

CONTACT US

Telephone 8290 1333 (all hours)

Email council@stonnington.vic.gov.au

Post PO Box 58, Malvern, Victoria 3144