Risk Management Framework

Version 4, February 2023

City of Port Phillip

99a Carlisle Street
St Kilda VIC 3182

Phone: ASSIST 03 9209 6777
Email: portphillip.vic.gov.au/contact-us
Website: portphillip.vic.gov.au

Divercity

Receive the latest news from your City and Council portphillip.vic.gov.au/divercity

National Relay Service

If you are deaf or have a hearing or speech impairment, you can phone us through the National Relay Service (NRS):

TTY users, dial 133677, ask for 03 9209 6777

Voice Relay users, phone 1300 555 727,

then ask for 03 9209 6777.

relayservice.gov.au

Please consider the environment before printing.

Framework

Responsible Service / Department:

Risk Management and Assurance – Governance & Organisational Performance

Adoption authorised:

SRIA

Date of adoption:

12 December 2022

Date effective from:

12 December 2022

Document Set ID (ECM):

TBC

Subject (Index name in ECM):

TBC

Endorsed CEO or ELT member or department manager to make and approve document editorial amendments:

EM Governance & Organisational Performance

Desktop review date:

February 2025 – brief check in (unless organisation experiences significant change or exposure to risk has increased)

Full Review date:

Aligns with 4 year cyclical policy review

Version number:

#4 Four-year review, including alignment with updated Risk Management Policy and VGRMF.

Stakeholder review and engagement:

DTS, Finance, Safety & Wellbeing, Accessibility and EPMO

Relevant Legislation:

Nil

Associated Strategic Direction #5:

Well-Governed Port Phillip: A City that is a leading local government authority, where our community and our organisation are in a better place as a result of our collective efforts.

Associated instruments:

Risk Management Policy, Fraud and Corruption Awareness and Prevention Policy, Fraud Control Plan, Legislative Compliance Policy & Framework, Business Continuity Plan

Supersedes:

Version 3.1

Review history:

Name	Document Set ID (ECM)	Date	Description of Edits
J Snowden	3.1	01/07/2020	**Editorial amendments prior to a full review in December 2022**
J.Snowden / A.Lowe	4	6/12/2022	**Four year full review, including alignment with updated Risk Management Policy and VGRMF**

Contents

Framework 3
1. Introduction 7
2. Risk Management Objectives 7
3. Overview of Risk Management Framework 8
4. Risk Management Framework Elements 9
Three Lines Model 9
4.1 Ownership and Risk Culture (Tone from the Top): 10
4.2 Risk Training & Learning: 11
4.3 Risk Appetite: 12
4.4 Incidents, Issues, Breaches and Claims: 12
4.5 Control Effectiveness Testing: 12
4.6 Annual Attestation: 13
4.7 Risk Reporting: 14
4.8 Insurance as a risk management tool: 15
4.9 Key Risk Indicators / Key Performance Indicators: 17
4.10 Project Related Risks: 17
4.11 Link with Emergency Management: 18
4.12 Link with Health & Safety 18
4.13 Link with Fraud and Corruption Control: 19
4.14 Link with Business Continuity: 19
4.15 Link with Legislative & Regulatory Compliance: 19
4.16 Ongoing Review and Improvement: 20
4.17 Risk Maturity: 20
APPENDIX 1: Core Risk Management Process 21
APPENDIX 2: Roles and Responsibilities 31
5.1 Council 32
5.2 Audit and Risk Committee (ARCO) 32
5.3 Executive Leadership Team (ELT & SRIA) 32
5.4 Internal Audit 33
5.5 Executive Manager of Governance & Organisational Performance 33
5.6 Risk & Assurance Coordinator 33

5.7 Project Managers 33
5.8 Executive Manager, People, Culture and Safety (through Head of Safety and Wellbeing) ... 34
5.9 Managers 34
5.10 Risk Owners 34
5.11 Control Owner 34
5.12 Staff, Contractors, and Service Providers 35
APPENDIX 3: Glossary 36
APPENDIX 4: Sample Risk Register 37
APPENDIX 5: Risk Assessment and Analysis Template 38

1. Introduction

Risk management is defined as "*the coordinated activities to direct and control an organisation with regard to risk*".

City of Port Phillip's (Council's) Risk Management Framework ('framework') is aligned to the ISO standard on risk[1] and shall be applied to all activities of council. Risk needs to be considered and addressed by everyone, including governing bodies, executive staff and senior management, employees, partners and related stakeholders. Council is committed to promoting an organisational culture where risk management is embedded in all activities and business processes.

Council undertakes proactive risk management because:

a. It is good practice to understand the strategic and operational risks and opportunities facing council in order to make informed decisions and achieve organisational and strategic goals;
b. Council provides critical services and infrastructure to the residents and visitors of this municipality; and
c. Council has service agreements and contractual obligations with government and non-government agencies and organisations.

The framework is designed to provide the architecture for a common platform for all risk management activities undertaken by council, from individual functional, process or project based assessments to whole-of-organisation assessments, with the aim of enabling comparative analysis and prioritisation of those assessments either individually or cumulatively.

The framework will be reviewed regularly and formally approved every two years by the Executive Leadership Team (ELT) or the Strategic Risk & Internal Audit Group (SRIA) and will be noted by Council every four years aligned with Risk Management Policy review cycle. This document describes the tools, processes, structures, and behaviours for Council to meet the requirements of the Risk Management Policy.

[1] *Australian / New Zealand ISO Standard on Risk Management: AS/NZS ISO 31000-2018*

2. Risk Management Objectives

The primary objective of the framework is to support the achievement of Council's strategic objectives contained in the Council Plan and safeguard the council's resources, people, finance, property, knowledge and reputation.

Council will actively consider risks during strategic and tactical decision-making processes and will determine the level of residual risk they are willing to accept.

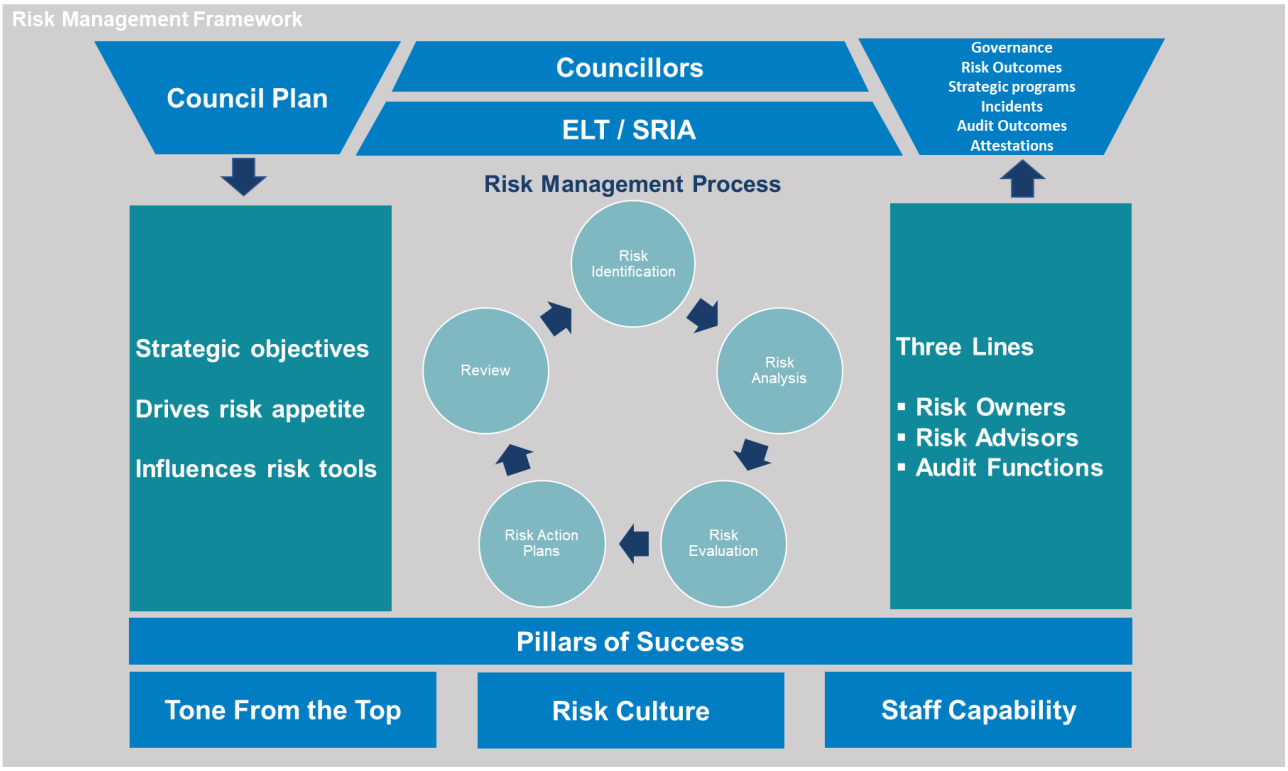
Council will take a risk-based approach to managing internal and external projects, operational and strategic risks: i.e. risks will be managed and monitored according to severity.

The Risk Management framework will support the ongoing development and embedding of a Child Safe Culture at COPP. Identifying and mitigating child safety-related risks is a core component of being a child safe organisation. Child safety risks come in many forms, including environmental, operational and cultural risks. The level and type of risk varies across the organisation and can change over time. Council will annually review child safety risks to continue to promote a culture of continuous improvement and to identify new / emerging risks and support ongoing, appropriate management of existing child safety risks.

Management will conduct full annual reviews of their Department risks (facilitated by the Risk & Assurance Team) with monthly monitoring of High > risks and annual monitoring of Medium and Low risks. Management will also conduct out-of-cycle reviews of operational, project or strategic risks if material changes occur, there is a breakdown of controls, or new risks emerge. For example: organisational change; major process or system change; failure of controls; a major incident; a serious compliance breach; serious complaint; or significant near miss.

3. Overview of Risk Management Framework

The diagram below provides an overview of how the Risk Management Framework operates in order to support Council's objectives.



The 4-yearly Council Plan sets strategic objectives and considers the risk-reward areas for consideration in delivering on objectives. The achievement of objectives and prudent management of risks is influenced by risk culture, with the day-to-day activities of staff, including staff development, playing a key role in success.

The Risk Management Framework provides tools, processes, and structures to drive risk culture uplift and the robust, effective management of both risks and issues consistently across Council.

The appetite for risk is enshrined in various layers of the Risk Management Framework. The risk acceptance matrix guides decision making on how to approach the treatment of risks and which levels of risk must be escalated to Executive and Council forums. This is complemented by the Waterline Tool, which encourages teams to think strategically about risk management.

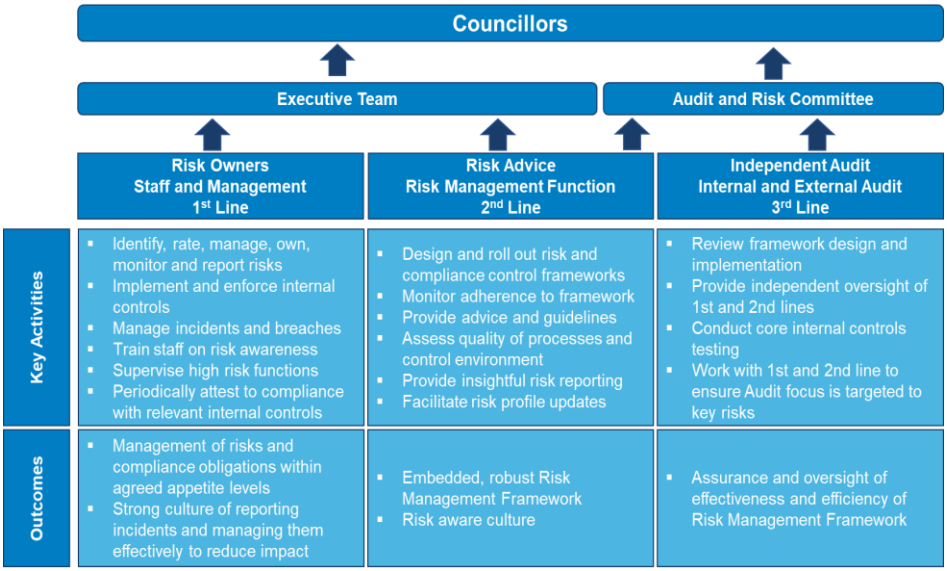
The core risk management process describes the life cycle of managing risks from identification through to treatment and review *(See APPENDIX 1 - Core Risk Management Process page 20)*

Governance closes the loop and ensures key decision makers are aware of and ultimately manage key risks to strategic objectives and the ongoing viability of Council.

4. Risk Management Framework Elements

Three Lines Model

Council uses the Three Lines Model to operationalise and reinforce the framework by allocating responsibilities for risk owners, risk advisers, and audit functions.



1st Line: Staff and Managers

Each Department manager is responsible for the ownership and management of risks in their area. They are also responsible for overseeing relevant internal controls and implementing corrective treatment actions to address control deficiencies. All staff perform day to day control activities that ensure effective ongoing management of risks and compliance with relevant laws and regulations. All staff are responsible for reporting incidents and breaches to their direct manager, who will ensure the appropriate response based on the incident type and severity.

2nd Line: Risk & Assurance and Compliance Functions

The Risk & Assurance Team and various compliance functions establish policies, frameworks, tools, and processes for the management, monitoring and reporting of risk. They also provide:

- Oversight of the adequacy of first line controls to ensure that risks are being managed effectively;
- Advice on continuous improvement;
- Application of policies and frameworks; and
- Reporting to Executive and Audit & Risk Committee forums.

In some areas, specialist compliance roles have also been established to assist in promoting and monitoring compliance e.g. Finance, Business Technology and Governance. These roles fulfil both 1st and 2nd line roles.

3rd Line: Internal Audit

Internal Audit (IA) provides independent assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the 1st and 2nd lines achieve risk management and control objectives. IA provides Council and senior management with comprehensive assurance based on the highest level of independence and objectivity. There are a range of external assurance bodies that also provide additional defence in the conduct of Council's activities.

The Internal Audit function also plays an integral role by providing independent oversight of the design, implementation, and ongoing operation of the RMF at Council. The Internal Audit and Compliance Plan is formed via collaboration with risk owners and the Risk & Assurance Team to focus audit resources on areas of highest risk.

4.1 Ownership and Risk Culture (Tone from the Top):

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.

The Chief Executive Officer has the ultimate responsibility and accountability for ensuring that risk is managed appropriately across the Council. However, to achieve the best outcomes from risk management, it is imperative for Council to have a good risk culture. A number of key elements of the Risk Management Framework and leadership behaviours contribute to the ongoing uplift in organisational risk culture, including:

- The Executive Leadership Team promotes, demonstrates, and regularly communicates to staff the importance of risk management;
- Applying the waterline principle to support a positive risk culture in the organisation. The waterline principle provides a simple methodology to enable officers at all levels to understand what level of risk the organisation will tolerate and where to escalate potential risks quickly for management at the appropriate level;
- Defining a desired risk culture and identifying any gaps between the current risk culture and desired risk culture then defining council's approach to close any identified gaps over time;
- Investing the appropriate time and resources into training and awareness for all staff (including incident management through business continuity);
- Providing specialised training for managers and nominated risk and control owners and staff with specified risk management roles;
- Establishing and maintaining internal controls that are designed to reinforce desired risk-aware behaviours across the organisation.

4.2 Risk Training & Learning:

To ensure the ongoing successful implementation of risk management throughout the organisation, appropriate training in risk management will be provided to relevant staff and all managers. 101 risk management training will generally be delivered as part of the annual departmental operational risk review process and will involve all relevant staff selected by the manager to participate. The accountable manager will however be afforded more in depth training specifically around the risk management process, application of risk management tools, and risk reporting.

In addition, the Risk & Assurance Team will coordinate with People, Culture & Safety Department to work towards ensuring:

- Induction training includes a module &/or other on Risk Management and Fraud awareness;
- Relevant staff receive regular Risk Management awareness and Fraud awareness update training focussed on those staff directly involved in financial and/or cash transactions);
- Any updates and changes to the Risk Management Policy, Framework, Fraud related policies and procedures etc. are communicated to all employees.

4.3 Risk Appetite:

Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that Council is willing to accept in pursuit of its objectives. Once the risk appetite threshold has been assessed as breached, risk management controls and actions are required to bring the exposure level back within the accepted range. This process is known as risk treatment and is fully described in *risk treatment page 23* Council will re-assess agreed risk appetite levels periodically.

Residual Risk Evaluation page 22, includes a table describing the requisite actions (treat or accept) for the various risk ratings that are attached to a documented risk. There may however be some room to move outside requisite actions. For example,

- Risks that might be outside Council's control (i.e. political change);
- Where Council might want to take on additional risk to pursue a strategic objective or expectation of above average returns.

Where higher-rated risks are accepted, outcomes will be actively monitored against relevant performance indicators on a monthly basis by the Strategic Risk & Internal Audit Group (SRIA).

4.4 Incidents, Issues, Breaches and Claims:

At times risks will materialise in the form of incidents, issues, or breaches. The process below ensures issues or incidents are recorded and managed as efficiently as possible. Some incidents have existing protocols that must be followed. For example, child safe issues, or material privacy breaches. In such circumstances, the relevant protocols take precedent and must be strictly followed.

1. An incident, issue, or breach is reported by an employee in the first instance to their line manager;
2. The line manager assesses if there is a need to escalate further. The waterline diagram in *Appendix 2 page 24* provides guidance on how to treat and report incidents, issues, or breaches. For matters "above the waterline", manage locally. For matters "on the waterline", the line manager advises his/her ELT member, who will consider advising the SRIA for active response and for matters "below the waterline", the line manager needs to quickly escalate to ELT and ensure SRIA actively manages the response.
3. Incidents sometimes result in third party injury, loss or damage and accordingly need to be appropriately managed and settled. The Risk & Assurance team manages all such claims made against Council with assistance from an independent claims management service provider, insurance brokers and insurers.

4.5 Control Effectiveness Testing:

Control effectiveness testing involves regular reviews of key (material) risk controls to ensure they are designed and operating effectively to minimise the risks they are intended to mitigate. Controls testing and validation is important in ensuring Departments are reviewing their risks, developing and maintaining effective methods to minimise these where possible. An annual program of

Control Effectiveness Testing will be established by Risk & Assurance in conjunction with Internal Audit taking into account the audit schedule and core compliance testing.

The establishment of an effective controls framework includes:

- Establishing key controls that can provide reasonable assurance that material errors will 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, observing / inspecting that the control is working.

4.6 Annual Attestation:

Council's leadership network has a key role in implementing and overseeing internal controls that impact Council's financial performance and reporting.

As part of the process underpinning the certification of Council's financial statements at the end of each financial year, the leadership network (General Managers and Level 3 Managers) are required to provide certifications to the Chief Financial Officer (CFO) by completing the Manager Certification checklist (attestation). Council's Audit and Risk Committee Charter also requires attestation from management to the effectiveness of key internal controls.

Completion of the certification checklist enables the Chief Executive Officer and CFO to certify that Port Phillip City Council has a sound system of risk management and internal controls to ensure that Council's financial information and annual financial statements are true and fair, in all material respects.

This checklist is distributed a number of weeks in advance of the return deadline to enable potential weaknesses to be identified and appropriate remedial actions to be undertaken.

The checklist questions directly related to the risk framework include:

- Notification of any fraud or suspected fraud;
- All known actual or possible litigation and claims with potential financial impact have been disclosed to the Chief Financial Officer and the Insurance Officer;

- The departmental operational risk register has been reviewed and updated in the last 12 months;
- 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; and
- Any audit recommendations and matters for action arising from internal audit reports were actioned and closed off during the year or actions and timetables are in place to ensure implementation.

4.7 Risk Reporting:

Risk reporting is a fundamental pillar in effective governance of risk outcomes across Council. Reports are provided to various forums to help each forum discharge its duties within the RMF. The Risk and Assurance Team is responsible for overall coordination of elements to provide timely and robust reporting of:

Key incidents, risks, and assurance activities

The implementation, performance, and status of the RMF

The table below indicates the responsibilities and frequencies for each report.

Report Name	Author	Recipient	Frequency
Strategic Risk Assessment	Executive Manager, Governance & Organisational Performance / Risk & Assurance Coordinator	Council	Annually
		ARCO	Annually
		SRIA	Quarterly
Attestation of Control Effectiveness	Risk & Control owners	ELT / SRIA ARCO	Annually
Below Waterline and Watch List Report	Risk owners (facilitated by Risk & Assurance Team)	ARCO	Quarterly
		SRIA	Monthly
High Risk Treatment Actions on Track	Responsible risk action owners (facilitated by Risk & Assurance Team)	ARCO	Quarterly
		SRIA	Monthly
Portfolio risks and issues Report	Project Managers (facilitated by EPMO & Risk & Assurance Team)	ARCO	Quarterly
		SRIA	Monthly
		EGG	Monthly
Divisional Risk Register Status Report	Risk & Assurance Team	SRIA Divisional leadership meetings	Deep Dive bi-monthly or as required

Outstanding Audit actions	GMs, Managers, Responsible Officers (facilitated by Risk & Assurance Team)	SRIA ARCO	Monthly Quarterly
Risk Update Report	Risk & Assurance Team	SRIA ARCO	Monthly Quarterly
Compliance Update Report	Risk & Assurance Team & Governance	SRIA ARCO	Monthly Quarterly
Internal Audit Reports	Internal Audit Team	SRIA ARCO	Monthly (or out of meeting cycle if required) Quarterly (or out of meeting cycle if required)

4.8 Insurance as a risk management tool:

Council must make best use of its available resources and assets to manage risk and minimise loss. Insurance is another tool to manage risk and can 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 organisation can bear.

Insured risk still requires preventative and mitigating treatments where appropriate to reduce the probability of occurrence or severity of the outcome of an adverse event.

If the risk is not insurable due to lack of insurance capacity, withdrawal from the market or simply no existing cover, Council's risk management processes will establish alternative response to address the risk i.e. captive / self-insurance or the broad use of indemnity provisions.

Insurance Cover

In order to provide the best cover possible for Council, the Risk & Assurance team:

- Determine the most appropriate insurance products and levels of cover for the organisation's present and future risk exposures, including undertaking insurance gap analysis, in consultation with insurance brokers and key stakeholders;
- Establish Council's insurance portfolio and purchase the appropriate policies;
- Maintain appropriate deductibles (self-insurance) 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;
- Work towards minimising exposure to insurable risk.

4.9 Key Risk Indicators / Key Performance Indicators:

A key risk indicator (KRI) is a metric for measuring the likelihood that the combined probability of an event and its consequence will exceed the organisation's risk appetite and have a profoundly negative impact on an organisation's ability to achieve its strategic goals and objectives.

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.

- For example, a council might monitor and measure the likelihood of losing key staff and the risks to their employer of chioce brand as a KRI.

Key Performance Indicators (KPIs), in simple terms, provide a way to measure how well companies, business units, projects or individuals are performing in relation to their strategic goals and objectives.

- In terms of the above KRI, a council might measure staff engagement or staff satisfaction as an important KPI and control against the KRI of the likelihood of losing key staff.

Monitoring and measurement of KRIs and 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.

These indicators will be consdered as part of council's risk maturity process and will be determined through consulltation and negotiation with the ELT and the Leadership Network. Once established they will be inserted into the reporting processes and updated in the RMF.

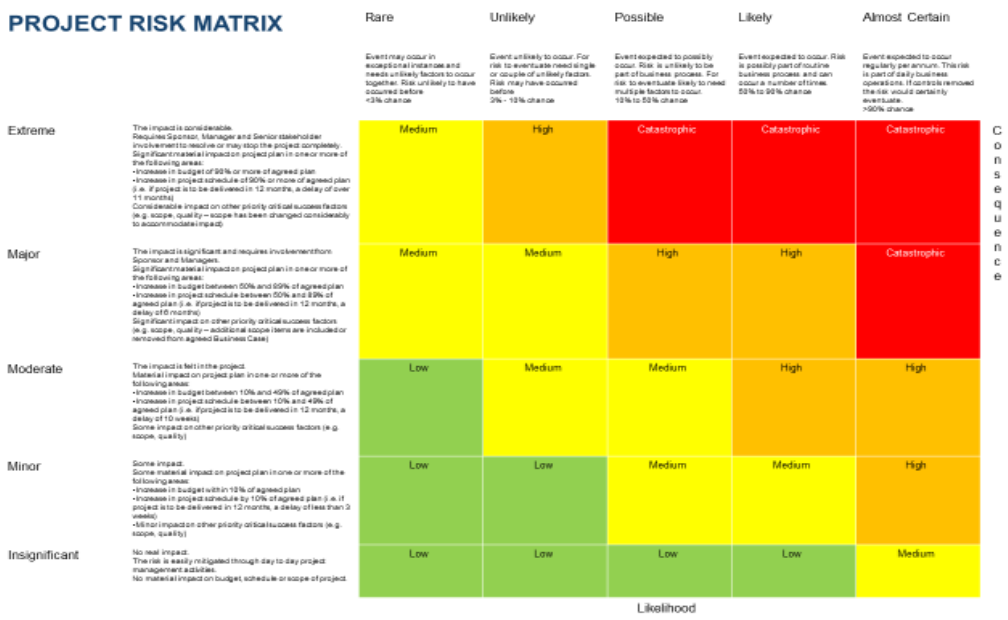
4.10 Project Related Risks:

To help ensure Council actively manages risks associated with key change programs and projects, Project Managers, Owners and Sponsors are jointly responsible for implementing an appropriate governance structure and risk control measures to manage:

- Risks to do with program / project management and delivery. Eg. quality, financial, timeliness;
- Risks of implementing change to Council operations; and
- Risks of non-realisation of project benefits.

Each formal project set up and managed within Council has a Project Control Group (PCG). The PCG is responsible for managing project risks and issues to ensure the delivery of the project and realisation of project benefits. Any risks deemed to be High or Catastrophic should be assessed by the PCG for escalation to the Executive Governance Group (EGG for projects) and ELT.

Project managers will use the below project risk matrix and other tools described in this RMF to aid with uniformity of risk management tools and processes across Council, and to allow for program-wide risk and issues reporting. These tools are applied and reported in a project's Project Management Plan.



During handover to “business as usual” when a project team is disbanding, a key deliverable before project closure is a set of risks to be managed within normal Council risk management structures. These risks should be assessed using normal (non-project) risk tools by the Manager responsible for the ongoing management of the building / activity or program.

4.11 Link with 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 in the CoPP municipality is undertaken by the Coordinator Emergency Management & Community Safety. Details of relevant process are found in the Municipal Emergency Management Plan (MEMP) located on the Intranet under Emergency Management.

4.12 Link with Health & Safety:

Recognising that there is an intrinsic link between Occupational Health & Safety and risk management, each Departmental Operational Risk Register acknowledges the importance of the OH&S Hazard registers as a tool to identify and reduce hazards that if eventuate may casue injury or illness to our staff. Hazard Registers are a strong control in mitigating workplace hazards and keeping our people safe. Organisational requirements and templates for the establishment and on going management of hazard registers is found here Hazard Identification & Risk Assessment Procedure.

4.13 Link with Fraud and Corruption Control:

Similar to Risk Management Standard compliance, organisational fraud and corruption programs that are compliant with Australian Standard AS 8001 Fraud and Corruption Control would be considered best practice. In order to be compliant, organisations have to do certain things as stipulated in the Standard.

In its 2021 update, the Standard includes guidance relating to preventing, detecting, and responding to external attack particular cyber-born attack and introduces the concept of 'pressure testing' for internal control systems. As Fraud and Corruption is a specific organisational wide risk and as such requires its own Fraud and Corruption awareness and prevention Policy and Fraud Control Plan both of which are managed by the Risk & Assurance Team. The Policy can be located on the Intranet under Risk Management.

4.14 Link with Business Continuity:

The applicable Standard for Business Continuity is - Managing disruption-related risk is AS/NZS 5050: (Int) 2020. This Standard provides guidance on the unique nature of disruption-related risk and different approaches required for its management. Guidance in this Standard is used in conjunction with Council's existing risk management arrangements. All Managers have a Business Continuity Sub Plan for their department captured in the ECM Document Management system. For a copy of the organisation Business Continuity Plan, please contact the Risk & Assurance Team.

4.15 Link with Legislative & Regulatory Compliance:

Council's Internal Auditor has undertaken a Compliance Framework Audit with the objective to support Council in assessing the current state and maturity of how compliance is managed at Council and to develop a roadmap for implementing a good practice compliance framework against the principles of AS ISO 19600:2015 *Compliance Management Systems.*

As a Council that provides a broad range of services to the community, there is a substantial volume of legislative and regulatory obligations which are required to be complied with, in addition to internal compliance requirements. Having the appropriate policies, processes and systems in place is fundamental for ensuring that council can prioritise and manage compliance obligations in a systematic, planned, and timely manner.

We all play a role in managing our Compliance obligations. Whilst the Compliance Framework is being developed, please direct any enquiries to the Risk & Assurance team.

4.16 Ongoing Review and Improvement:

Council is committed to periodic review and measurement of the RMF elements to ensure that risk management is effective and continues to support organisational performance and is clearly aligned to strategic objectives. Examples of review and measurement activity include:

- Evaluation of the effectiveness and alignment of this Risk Management Framework with relevant standards and guidelines (e.g. Victorian Government Risk Management Framework);
- Assessment through surveys of staff awareness in relation to their risk management responsibilities;
- Review of evolving training and development needs of managers and staff in relation to their risk management responsibilities;
- Review of the completeness and currency of strategic, operational and relevant project risk registers;
- Consideration of additional framework elements as required.

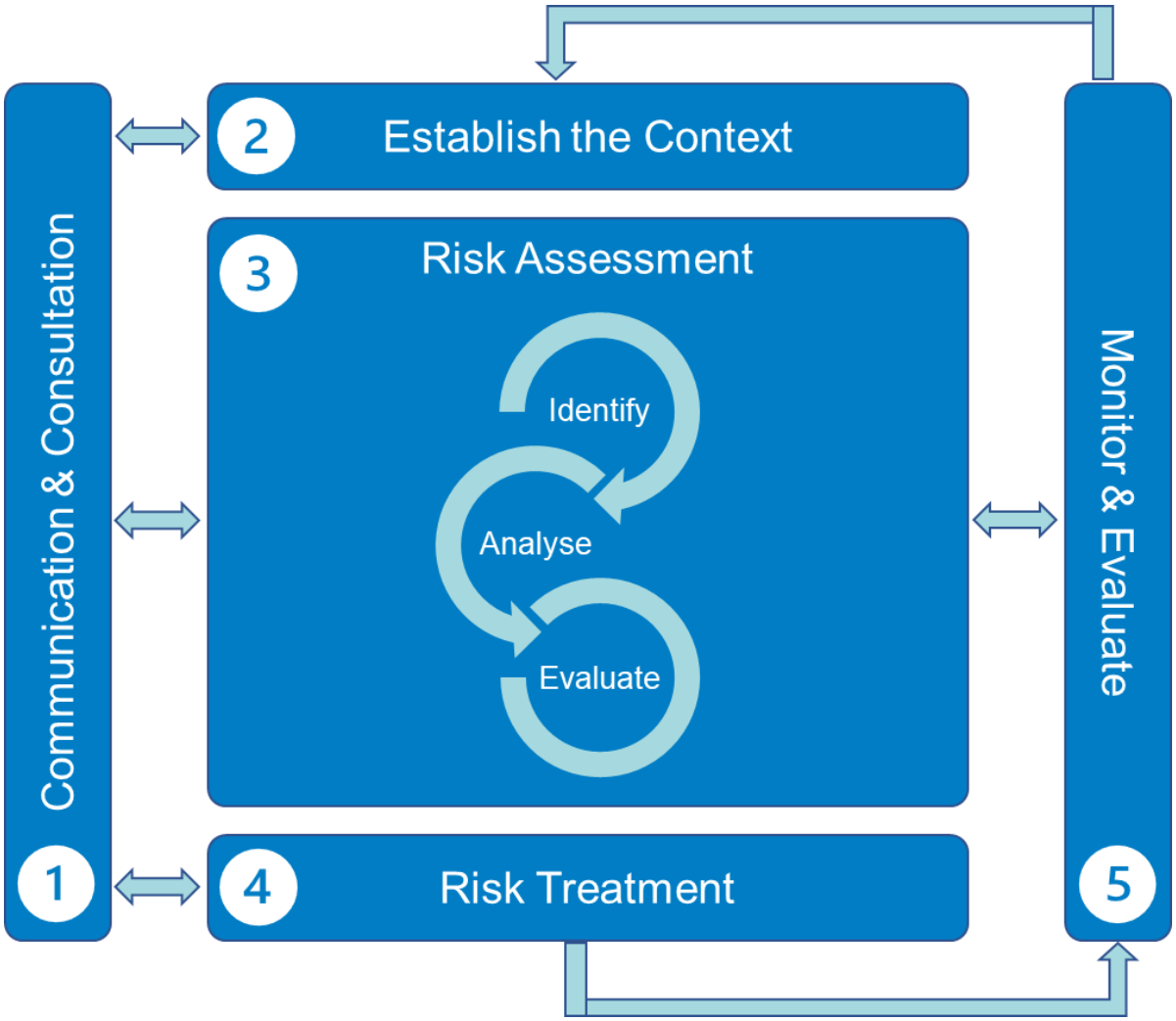
The results of reviews will inform decisions relating to how the RMF can be improved to support the management of risk and an improved risk management culture across Council.

4.17 Risk Maturity:

Risk maturity describes risk capability and the level of sophistication that council 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 councils strategic objectives. As council environments and services change, risk management evolves to ensure that it continues to support achieving the strategic objectives. Council will continue to develop and implement strategies to improve its risk maturity (or maintain it at the desired level) to ensure it promotes effective risk management.

APPENDIX 1: Core Risk Management Process

The risk management process is the “how to” element of the framework. The process used to manage risks at Council is modelled on ISO31000:2018.



1

Communication and Consultation

Communication and consultation with internal and external stakeholders are important elements of the risk management process to ensure appropriate buy-in, incorporate diverse opinions and requirements, and to ensure consistency.

Typical elements of this facet of risk management include awareness training for staff; specialised training for key risk owners, senior management, and Councillors; hearing the voice of the community where applicable; transparency of the decision-making process; consistent application of tools and processes; and the transparent, effective reporting of outcomes across stakeholder groups.

2

Establish the Context

Establishing the context for managing risks and embedding structures, tools, and processes is integral for successfully incorporating disciplines and proactive risk management activities into operations and the achievement of strategic objectives. This Risk Management Framework outlines how measures will be implemented into Council, considering pertinent external and internal drivers.

External Context
Key external considerations that have contributed to this Risk Management Framework and which will be considered as Council implements and executes risk measures include: • Legal and regulatory obligations • Community issues and sentiment • External opportunities and threats • Health and safety developments, including State Government directives, where appropriate • Media sentiment • Key third party relationships. Establishing the external context is important to ensure that our community and external partners and their objectives are considered when developing risk management criteria and that externally generated threats and opportunities are actively monitored.
Internal Context
Key internal considerations that have contributed to this Risk Management Framework and which will be considered as Council implements and executes risk measures include: • Strategic Council Plan, budget and drivers • Goals and objectives and the strategies that are in place to achieve them • Culture and morale • Occupational Health and Safety, where an identified cross over is established • Governance and structure • Capabilities in terms of resources such as people and systems • Council's internal strengths, weaknesses, opportunities and threats (SWOT)

3 4 5

Risk Assessment / Risk Treatment / Monitor & Evaluate

a. Risk Identification

The first step in the iterative risk assessment process is to identify and document risks to Council's objectives, reputation, operations, staff, or stakeholders. This may be done through varied channels, including strategic planning, formal risk assessment forums, or day to day detection by staff members.

Documentation of identified risks occurs through the development of a description of the risk and entry into the Council Risk Register (Microsoft Excel Spreadsheet, see (Appendix 5 page 31) for an example). The risk description should contain a description of the risk event and the thing that may cause that event to occur. The following structure should be used:

"there is a risk of <event> due to <cause>"

For example: there is a risk of privacy breach due to inadequate controls on usage of storage devices in Council PCs. This form of wording helps articulate what might happen, along with the areas where Council can treat the risk. This risk could be more generally articulated as "…risk of data leakage…", however depends on the remit of the team / person documenting the risk.

Strategic risks are formally developed annually in conjunction with the ELT and Councillors, using Council's strategic objectives and plan as a starting point.

Operational risks are identified in conjunction with Department managers on an annual basis as a minimum, at meetings with Risk and Assurance staff, which run parallel with the organisation's annual business planning cycle. Output from all risk assessments can, in turn, be used as input to the business planning process.

b. Risk Analysis

This step involves the following:

1. Allocating an *inherent* risk impact should the risk eventuate, along with an associated inherent risk likelihood. **Inherent risk ratings do not take into account any mitigating controls**.
2. Documenting and assessing the *effectiveness of any controls* in place to mitigate the risk.
3. Allocating *residual* impact and likelihood ratings, taking into account the controls in place and their effectiveness.

Using the three step approach above provides Council with an understanding of the relative importance of controls in place, which informs the design of business processes and assurance activities (including audit).

Identification of impact and likelihood is not scientific: outcomes should be performed based on context, perception, and historical data. Of key importance is that the impact and likelihood ratings are addressing the same underlying risk theme. A privacy breach can have *major* impacts in regulatory, reputational, and possibly financial areas. The likelihood of a privacy breach happening might be *almost certain*. For example, privacy protocols not followed during a customer call. Yet if the identified risk being described is about a significant, material privacy breach which exposes sensitive data, the likelihood for such an event is *unlikely* or *rare*. The Risk and Assurance team can advise on this process.

The tools below are to be used for assigning impact and likelihood ratings (both inherent and residual). Consider the impact category (column) in the impact table below that is the area where the highest impacts would be felt if the risk eventuated. Firstly, assign inherent risk rating.

Impact Table Including Waterline Criteria

	SERVICE DELIVERY / BUSINESS CONTINUITY	NATURAL ENVIRONMENT/ SUSTAINABILITY	REPUTATION	FINANCE	LEGAL/ REGULATORY	INFRASTRUCTURE/ASSETS	CORPORATE INFORMATION SYSTEMS	COMMUNITY SAFETY & RESILIENCE	HEALTH & SAFETY	ORGANISATION CAPACITY & CAPABILITY
INSIGNIFICANT	Inability to deliver non-essential services within specification for a period of less than 3 days.	Single occurrence which causes environmental harm with no ongoing affect.	Complaint by one or a number of disassociated members of the general community	Negative financial impact, increased costs, lost revenue or direct loss of Less than $30k)	Civil litigation or breach of contract which does not result in legal remedy. Or Statutory breach which results in issue of a PIN notice.	Localised damage to a single general asset which can be remedied within a short time frame.	Minor disruption to non-critical information systems < 24 hours or security compromise of low risk unclassified or official data	Displacement of single groups or households for a period less than one week Inconsequential short - term reduction in community wellbeing, no effect on social networks	Incident or hazard only, no injury or illness	Localised employee dissatisfaction resulting in a staff satisfaction rating drop of less than 5%. Increase in turnover of personnel or absenteeism of less than 5%.
MINOR	Inability to deliver non-essential services within specification for a period of greater than 3 days but less than 1 week.	Repeated occurrences which cause environmental harm with no ongoing affect.	Complaint by a group from the community which is escalated into the public arena Or Minor adverse local media attention	Negative financial impact, increased costs, lost revenue or direct loss of Greater than $30k but less than $300k)	Civil litigation or breach of contract which could result in non-material legal remedy. Or Statutory breach which results in non-material fine. Or Imposition of prohibition notice.	Localised damage to a single general asset which can be remedied over a long-time frame. Or Widespread damage to a single general asset which can be remedied over a short time frame.	Minor disruption to non-critical information systems < 48 hours or security compromise of official sensitive data	Displacement of multiple groups or households for a period less than two months Localised disruption to community wellbeing and social networks over a small area and for a period of weeks	First aid treatment only, no further intervention required	Localised employee dissatisfaction resulting in staff satisfaction rating drop of greater than 5%. Increase in turnover of personnel or absenteeism of greater than 5%
MODERATE	Inability to deliver essential services within specification for a period of less than 3 days. Inability to deliver non-essential services within specification for a period of greater than 1 week.	Single or repeated occurrence which cause ongoing environmental harm which is able to be remediated in less than 2 years.	Serious attention / concern from the public, state media or stakeholders which will be overcome within 3 months.	Negative financial impact, increased costs, lost revenue or direct loss of greater than $300k but less than $1M	Civil litigation or breach of contract which could result in material legal remedy. Or Statutory breach which results in a material fine Or Suspension of a non-material licence permit etc.	Localised damage to a single “priority” asset which can be remedied over a short time frame. Or Widespread damage to a number of general assets which can be remedied over a short time frame.	Moderate disruption to information systems including some critical systems < 24 hours or security compromise / unauthorised access of official sensitive / legal privilege data	Displacement of persons across a small area for a period less than two months Wide-ranging disruption to community wellbeing and social networks over a large area for a period of several months	injury/illness requiring medical treatment and/or lost time of less than 1 week	Localised lack or loss of staff capability to deliver Council Plan objectives for a period of greater than three months Increase in turnover of personnel or absenteeism of greater than 10%
MAJOR	Inability to deliver critical services within specification for a period of less than 3 days Inability to deliver essential services within specification for a period of greater than 3 days but less than 1 week	Single or repeated occurrences which cause ongoing environmental harm which is able to be remediated in greater than 2 years but less than 5 years.	Significant attention / concern from the public, National media or stakeholders which will take longer than 3 months to overcome.	Negative financial impact, increased costs, lost revenue or direct loss of greater than $1M but less than $10M.	Civil litigation or breach of contract which could result in actions taken in the supreme court or federal court. Or Statutory breach which results in a significant fine / Suspension of a material licence, permit, etc.	Localised damage to a single “priority” asset which can be remedied over a long-time frame. Or Widespread damage to a number of general assets which can be remedied over a long-time frame.	Unavailability of critical systems > 24 hours or unauthorised removal, loss or manipulation of critical / sensitive / legislative secrecy / personal privacy data	Displacement of majority of persons within a suburb for any period Extensive disruption to community wellbeing and social networks over the majority of the municipality for a period of at least 12 months	injury or illness resulting in lost time, potential for permanent restriction and or impairment, multiple people involved in incident	Widespread lack or loss of staff capability to deliver Council Plan objectives for a period of greater than three months Widespread employee dissatisfaction resulting in staff satisfaction rating drop of greater than 5% Increase in turnover of personnel or absenteeism of greater than 15%
EXTREME	Inability to deliver critical services within specifications for a period of greater than 3 days. Inability to deliver essential services within specification for a period of greater than 1 week.	Single or repeated occurrences which cause ongoing environmental harm which cannot be remediated in under 5 years.	Ministerial intervention appointment of commissioners.	Negative financial impact, increased costs, lost revenue or direct loss of greater than $10M	Civil litigation or breach of contract which could result in action taken in the full court. Or Statutory breach which may result in imprisonment.	Wide spread damage to a number of “priority” assets which can be remedied over long time frame. Total and permanent destruction of one of more “priority” assets.	Extensive and total loss of critical systems, data and functions across the whole organisation for an extended period	Displacement of majority of persons within municipality for any period All-encompassing disruption to community wellbeing and social networks over the entire municipality for several years	Permanent impairment, fatality. Large volume of people impacted staff and/or Public	Widespread lack or loss of staff capability to deliver Council Plan objectives for a period of greater than six months Widespread employee dissatisfaction resulting in staff satisfaction rating drop of greater than 10%. Increase in turnover of personnel or absenteeism of greater than 25%.

The likelihood of a risk occurring is measured by the probability or frequency of its occurrence. How likely is the risk to eventuate? Or how frequently will the risk eventuate?

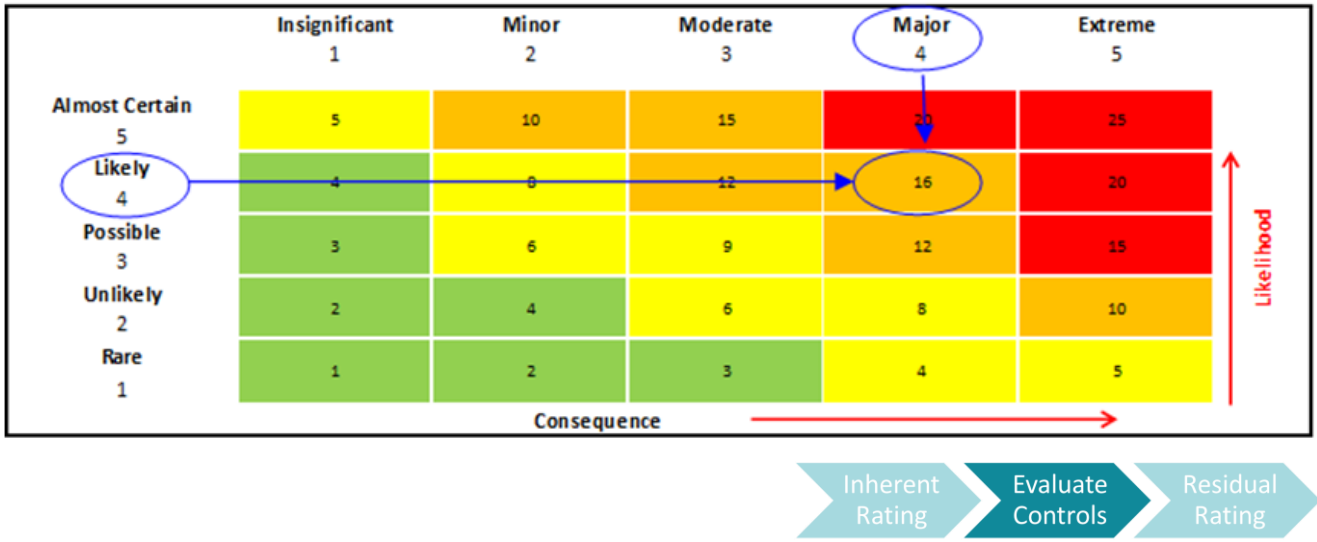
Description	Likelihood of Occurrence	Probability
Almost Certain	Incidents will occur frequently each year	Multiple times per year
Likely	Incidents will almost certainly occur each year	1 per year
Possible	Incidents will possibly occur every 2 to 3 years	1 in 2-3 years
Unlikely	Incidents are unlikely; every 3 to 5 years	1 in 3-5 years
Rare	Incidents possible in exceptional circumstances; 5+ years	1 in 5+ years

How to plot a risk on the risk matrix to determine the risk rating inherent / residual.
For each of the risks listed from the Risk Identification process, the inherent / Residual Likelihood of occurrence and potential consequences can be plotted by multiplying the numbers associated to each criteria of Likelihood and consequences.

For example, the inherent risk of a Fraud occurring in the Payroll process, **in the absence of effective controls**, could be assessed as follows:

The Likelihood is considered as 'Likely' (=4) (= 4) with the consequence assessed as being 'Major' (= 4).

The resulting level of inherent risk will be shown at the intersection of the two dimensions on the Risk Level Matrix below. This provides an Inherent Risk Rating of 16 = which is High.



Once the inherent risk rating is assigned, controls can be listed in the risk register. Most risks will have multiple controls in place. Controls may reduce the risk rating in a number of ways. For example, preventing a risk from occurring, reducing the likelihood, reducing the impact, or detecting when a risk is more likely to happen so it can be prepared for or promptly actioned.

1. Document in the risk register the controls in place that help manage the risk.

Once controls are listed, assess their *collective* effectiveness using the ratings shown below.

Control Rating	Description
Excellent	Controls are well designed, documented, embedded, and address the root cause Controls are effective and reliable at all times Nothing more to be done except review and monitor the existing controls Likely to be automated and regularly performed
Good	Most controls are designed correctly and embedded, documented and effective Some work needs to be done to improve operating effectiveness Consideration be given to implementing further controls for risks outside of appetite
Fair	There are some controls, but they do not address the risk effectively and require substantial improvement Some controls are not correctly designed and they do not operate effectively May be manually performed and/or infrequent
Poor	Significant control gaps exist Controls do not treat root causes, do not operate effectively or are not documented Manual and infrequently performed

When controls have been assessed and rated, the residual risk rating (the amount of risk left over taking controls into account) can be determined. Where controls are in place and operating effectively, the residual risk rating will be always be lower than the inherent risk rating.

As per the inherent risk rating process, assign impact and likelihood levels, but take into account the effect the controls have to reduce either the impact, likelihood, or both. Map the ratings against the risk matrix to assign an overall residual risk rating. This will reveal the current exposure Council is facing for the risk at hand.

c. Residual Risk Evaluation

Evaluation involves assessing the risk for acceptance or treatment, and allocating the required governance around chosen treatments. These decisions are based on the residual risk rating. The Risk Treatment Matrix below provides responses for each residual risk rating level. 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 required from each management group.

Residual Rating	Escalation	Acceptability	Accountability	Risk Treatment Guidelines
Catastrophic	• Immediate attention of ELT member and CEO • Active management by SRIA and Audit and Risk Committee (ARCO)	Unacceptable	CEO or Council	Risk to be urgently mitigated to acceptable levels, avoided or eliminated.
High	• Notification to ELT member • Governance by SRIA and ARCO	Unacceptable	Executive Leadership Team	Risk to be mitigated to acceptable levels.
Medium	• Annual reporting to ARCO	Assess for acceptability	Department or General Manager	General Manager to determine whether a risk treatment is required. Risk to be managed through normal risk monitoring and review activities.
Low	• N/A Retire from register if requested	Acceptable	Department Manager or Coordinator	Possibly no action required. Any activities will probably be managed through business-as-usual processes.

d. Treating the Risk

Risk mitigation/treatment involves identifying the most appropriate actions to reduce the residual risk rating to an acceptable level. Actions may be one-off or can be the introduction of new internal controls which operate into the future to mitigate a risk.

Typical treatment options include the establishment and operation of controls designed to mitigate, discourage, identify and/or limit the impact and likelihood of a risk from occurring. The Risk & Assurance Team can advise on the most appropriate treatments for given risks.

When determining the most appropriate treatment, the risk owner should consider:

- Will the treatment modify the level of risk to acceptable levels?
- How do costs balance out against benefits?
- How compatible is the treatment with overall business objectives?
- Does it comply with legislation or internal policy requirements?
- Does it introduce new or secondary or unintended risks?

Often more than one treatment response may be necessary to address an identified risk. A description of key actions, including owner and due date for each item must be entered in the risk register and reviewed routinely.

e. Ongoing Review of Material Risks

Risk assessments, the measurement of effectiveness of controls, and the progress against action plans, are ongoing, iterative processes at Council. Each iteration provides an opportunity to reasses ratings, control effectiveness, and the achievement of documented actions. During the review of risk, care should be taken to consider any changes which may impact outcomes. For example:

- Have there been changes in internal and external environments or drivers?
- Have our strategic objectives changes?
- Are there new regulatory requirements or standards to consider?
- Have incidents occurred that change our risk outlook or acceptance levels?

Internal audit will provide particular attention to those controls, mitigation activities or other responses identified through the risk assessment as having significant priority. In addition, the Risk Assessment Process, including the Framework, will be monitored, evaluated and reviewed by the Internal Auditor.

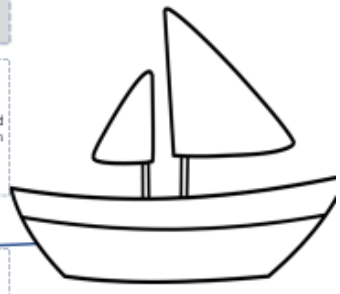
Risks are to be monitored and reviewed by the responsible manager/officer on an ongoing basis and reported to committees when required. The effectiveness of risk responses will be continuously monitored by the responsible manager/officer and reviewed six monthly.

Organisational Waterline – A tool for positive risk management

The organisation has adopted the waterline principle to encourage teams to think more strategically about how we manage risk. The principle uses a 'sinking ship' to articulate our how we manage risks and respond to issues. Below is a tool to help assess the impact of risks or issues and determine an appropriate course of action.

- **Above the waterline, manage locally.** If these risks eventuate, they will rock the ship but everything will most likely stay intact. These risks can be managed at a local level.
- **On the waterline, monitor closely.** These risks have the potential to sink the ship if they escalate, so they should be closely monitored and referred to SRIA for consideration. They will be monitored until controls bring it above the waterline.
- **Below the waterline, refer to SRIA.** If these risks eventuate, they are likely to sink the boat! These risks should be referred to SRIA as soon as practicable. Please contact Organisational Performance for more information on making a referral to SRIA.

	SERVICE DELIVERY / BUSINESS CONTINUITY	NATURAL ENVIRONMENT / SUSTAINABILITY	REPUTATION	FINANCE	LEGAL / REGULATORY	INFRASTRUCTURE / ASSETS	CORPORATE INFORMATION SYSTEMS	COMMUNITY SAFETY AND RESILIENCE	HEALTH AND SAFETY	ORGANISATION CAPACITY AND CAPABILITY
ABOVE THE WATERLINE *Manage locally.*	Inability to deliver non-essential services for less than 1 week.	Environmental harm with no ongoing affect.	Minor negative attention from local media or the community.	Increased costs, lost revenue or direct loss less than $100k.	A possible non-material fine or prohibition notice.	Damage to a general asset which can be remedied easily.	Loss of low-moderate risk data or systems for less than 7 days.	Localised displacement of persons for less than 1 week or short-term reduction in wellbeing.	Incapacitation for less than 7 days.	Localised employee dissatisfaction, increased turnover or absenteeism up 10%.
ON THE WATERLINE *Monitor closely.*	Inability to deliver an essential service for any time or non-essential services for more than 1 week.	Environmental harm that can be remedied within 2 years.	Persistent negative attention from stakeholders, the public or state media	Increased costs, lost revenue or direct loss about $300k.	A possible material legal remedy or fine, or a loss of non-material licence permit.	Localised damage to a priority asset or several general assets which can be remedied in a short time frame.	Loss of moderate risk data or systems for more than 7 days.	Displacement of persons for less than 2 months or localised disruption to wellbeing and networks.	Incapacitation for more than 7 days.	Loss of staff capacity to deliver the Council Plan, widespread employee dissatisfaction, increased turnover or absenteeism up 10%.
Factors that sink risks below the waterline.	• Whether essential or critical services are impacted. • Length of time unable to deliver services.	• Length of time to remedy harm	• The severity, reach, frequency and recovery time of the attention received.	• If the financial loss is greater than $300k	• Possible action in the supreme or federal court or a significant fine or suspension.	• The length of time to remedy the damage to any assets.	• If unauthorised access to data is detected or high risk data is lost.	• Length of time and number of people displaced. • The size of the area disrupted.	• The long term impacts and recovery timeframe of the injury or disease.	• The significance of capability loss. • Quantum of employee satisfaction change, turnover or absenteeism
BELOW THE WATERLINE *Refer to SRIA.*	Inability to deliver critical services for any period of time.	Environmental harm that cannot be remedied within 5 years.	Significant negative attention which will take longer than 3 months to overcome, or Ministerial intervention.	Increased costs, lost revenue or direct loss greater than $1m.	Possible action in the full court or imprisonment.	Widespread damages or permanent destruction to any number of 'priority' assets.	Loss of high risk data or unauthorised access to data.	Displacement of many people in a suburb or municipality or significant disruption to the municipality.	Likelihood of total or permanent disability or fatality.	Loss of capability for more than 6 months, a satisfaction drop of 10% or a turnover or absenteeism up 25%.



NEED HELP?

For advice on referring a risk to SRIA (Strategic Risk & Internal Audit Group) or the information on this sheet contact Risk and Assurance.

This tool reflects our organisational waterline as at July 2017.

APPENDIX 2: Roles and Responsibilities

The Responsible, Accountable, Consulted, Informed (RACI) table illustrates risk management accountabilities across the varied risk roles at Council.

It is therefore everyone's responsibility within the Council to manage risk; the accountability for managing any specific risk sits with the person most appropriate to manage that risk. This is reflected in position descriptions (with varying degrees of responsibility at the various levels) and the performance management process.

Notwithstanding our "whole of organisation" approach to risk management responsibility, our RMF has specific elements which require defined alignment of roles and responsibilities. The responsibilities for each of the roles identified are as follows:

Responsible (R) - Accountable (A) - Consulted (C) - Informed (I)											
Activity	**Staff (includes volunteers / contractors)**	**Coordinator / Team Leader**	**Manager**	**Risk & Assurance**	**Risk Owner**	**Control Owner**	**ELT / SRIA**	**CEO**	**ARCo**	**Council**	**Audit**
Risk Culture	I	I	C	C	R	R	R	A	I	A	
Risk Appetite setting	I	I	C	C	R	R	R	A	A	A	
Risk Policy & Risk Framework	I	I	I	R	C	C	A	A	I	A	
Risk tools / matrices	I	I	I	R	C	C	I	I	A	I	
Communication	I	I	R	R	R	R	C	A	I	I	
Training / Awareness	I	I	I	R	C	C	A	A	I	I	
Hazard identification	R	R	R	R	R	R	R	R	R	R	
Risk Assessment / Evaluation	I	C	C	R	C	C	A	A	I	I	
Out of cycle risk assessment	C	C	R	C	R	C	A	A	I	I	
Risk treatment strategies / action plans	I	C	C	C	C	A	A	A	I	I	
Monitoring	I	R	A	C	A	A	A	A	A	I	I
Reporting	I	C	R	R			A	I	I	I	I
Assurance	I	I	C	R	C	C	A	A	C	I	R
Attestation	I	R	C	C	A	A	I	I	I	I	
BCP / Emergency Management	I	R	R	R	R	R	R	A	C	I	
Post incident reviews	C	C	C	R	C	C	A	I	I	I	
Responsible (R)	those who do the work to achieve the task				Accountable (A)		approval or final approving authority				
Consulted (C)	those whose opionions are sought (SME)				Informed (I)		Those who are kept up-to-date on progress				

5.1 Council

- Approve the Risk Management Policy and note the Risk Management Framework.
- Be satisfied that strategic risks are identified, managed, and controlled appropriately.
- Appoint the Audit & Risk Committee

5.2 Audit and Risk Committee (ARCO)

- Oversee the implementation, operation, and effectiveness of the Risk Management Framework and review the mechanisms in place to comply with the framework.
- 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.
- 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.
- Identify and refer specific projects or investigations deemed necessary to assess risk management through the Chief Executive Officer, the internal auditor and the Council.
- Oversee any subsequent investigation, including the investigation of any suspected cases of fraud.
- Review Project Portfolio and associated risks.

5.3 Executive Leadership Team (ELT & SRIA)

- The CEO is accountable for ensuring appropriate risk management within Council.
- Endorse the Risk Management Policy for approval by Council, approve the Risk Management Framework, and monitor implementation.
- Provide executive leadership in the management of strategic, operational and project risk and generally champion risk management within Council.
- Ensure that their respective divisional risk profile as entered by each Department is reviewed, updated at least annually (monthly for high> risks);
- Report expeditiously to ARCO on any fraud and corruption incidents or material risk mitigation failures and actions taken.
- Provide oversight and active management of major risks, issues, opportunities, and Council's assurance environment. Play a lead role in promoting and embedding a positive risk, innovation and opportunity culture across the organisation in accordance with the waterline principle.

5.4 Internal Audit

- Consider strategic and operational risks in the development and implementation of the Internal Audit and Compliance Plan and recommend improvements.
- Provide independent oversight of the design, implementation, and ongoing operation of the RMF at Council.

5.5 Executive Manager of Governance & Organisational Performance

- Provide assurance in the development, implementation and review of the Risk Management Policy, Risk Management Framework, and general risk management practice within Council.
- Quality assure enterprise risk management reporting to the ARCO, Council and the ELT.
- Ensure the organisation has the appropriate culture, capability, processes and systems to deliver on this policy and the Risk Management Framework.

5.6 Risk & Assurance Coordinator

- Lead and manage the development, implementation and review of the Risk Management Policy, Risk Management Framework, and supporting processes and systems.
- Develop, maintain and quality assure enterprise risk registers and monitor implementation of controls and agreed treatment actions.
- Prepare various risk management reports to the Council, ARCO, SRIA, ELT, and divisional leadership teams in accordance with this framework and the Risk Management Policy.
- Provide risk management training, advice and support and conduct risk assessments as agreed with the ELT or Senior Management.
- Liaise with the Internal Auditor and provide secretariat support to the ARCO.
- Measure enterprise risk management maturity and report on the implementation of actions to achieve target maturity.

5.7 Project Managers

- Ensure that this framework is applied to the projects under their overview; and
- Where the project is considered to materially influence the achievement of Council's Corporate Objectives, ensure that the project risk assessment is facilitated by the Risk and Assurance Team.

5.8 Executive Manager, People, Culture and Safety (through Head of Safety and Wellbeing)

- Develop & facilitate implementation of a Safety Management System throughout the City
- Ensure that the Safety Management System is based on risk management standards and is consistent with this framework.
- Assist Risk & Assurance Team in relation to safety related 3rd party risk assessments.

5.9 Managers

- Ownership of risk management within their Department or as delegated by the CEO in accordance with this policy and the Risk Management Framework.
- Championing risk management within their Department and appropriate risk management practice by staff, volunteers, contractors, and service providers.

5.10 Risk Owners

- Responsibility that risk remains within defined tolerances;
- Triggers out-of-cycle review of the risks if material change occurs (e.g. restructure, new IT systems or processes being implemented, risk eventuates);
- Ensure personal compliance with risk management policies and procedures in performance of duties/activities;
- Ensure controls mitigating risks are designed and operating effectively to reduce the risk exposure to a level which is acceptable to the Council; and
- Responsible for annual attestation of risks with Manager and possibly control owner if different to risk owner.

5.11 Control Owner

- Is in charge of ensuring that controls (which may be outside responsibility of risk owners e.g. IT controls) are identified and documented;
- Responsible for annual attestation that controls are effective with risk owners;
- Understands the importance of the effective operation of the control and potential impact of failure on all areas that rely upon it; and
- Provide appropriate communication when their controls fail or do not operate as expected.

5.12 Staff, Contractors, and Service Providers

- Report incidents promptly to direct manager upon detection.
- Apply risk management practices in their area of work and ensure that management are aware of risks associated with council's operations.
- Recommend or provide suitable plans to manage risks; obtaining appropriate approval prior to action (where required); and report on risk management practices.

APPENDIX 3: Glossary

Terminology	Explanation
Risk	The effect of uncertainty on objectives. It is measured in terms of a combination of the likelihood of an event and its impact.
Risk Appetite	The level of risk that the Council is prepared to accept, tolerate, or be exposed to at any point in time.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk Analysis	A systematic use of available information to determine which risk events may occur, the likelihood of their occurrence, and the magnitude of their impacts.
Likelihood	The probability or expected frequency of an event happening.
Impact	The outcome of an event expressed either in financial terms or qualitatively, being a loss, injury, disadvantage or gain (impact).
Inherent Risk	The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls)
Control	Controls or mitigating actions in place to prevent, detect, minimise the impact of an identified risk.
Residual Risk	The risk level remaining after taking account the effectiveness of current controls or mitigating actions in place.
Risk Treatment / Action Plan	The additional controls / mitigation action required to ensure that the risk appetite level is achieved.
Risk Profile	The residual risk impact and likelihoods and control effectiveness ratings can be reflected on a one page Heat Map with supporting opinion and insight on risks, controls and actions – the Risk Profile.
Waterline Principle	The waterline principle establishes a clear perspective on tolerance based on an event's perceived impact to Council or its stakeholders. The waterline principle is visually presented as a blue tint (waterline) overlayed against the Impact Matrix. The waterline principle encourages active contemplation of risk elements in decision making across Council.

APPENDIX 4: Sample Risk Register

EXAMPLE RISK REGISTER

Dept.	Manager	Dept Risk Number	Risk Description	Cause	Consequences	Inherent Impact rating	Inherent Likelihood rating	Inherent risk rating	Existing Controls	Control Owner	Control rating	Residual Likelihood	Residual Impact	Residual risk rating	Target	Actions	Who	When
		Number of the risk in seqence	Concise description of the risk for example: Unable to attract, retain and develop experienced and professional staff; Department staff are injured at work; Department experiences a fraud or corruption event	There are generally a number of causes that will contribute to the occurrence of a risk Poor working conditions Lack of advancement opportunities Poor manually handling practices Lack of separation of duties No annual leave plans	What are the consequences after a risk occurs High staff turnover Disengaged staff Productivity loss Lost time injury Workcover claim Financial loss Employment termination Reputational loss	Moderate	Possible	**Medium**	All controls that currently mitigate the risk Flexible working conditions Staff development programs Safety Management System Manual handeling training Separation of duties Mandatory annual leave plans for all staff	Who owns or is resposible for the control	Fair	Unlikely	Moderate	**Medium**	Low	Any addition actions that have been approved to mitigate the risk Implement a working from home policy Develop a master class program Introduce an electronic health & safety management reporting system Establish a staff rotation process Develop a spot checks procedure for all high risk activities		

APPENDIX 5: Risk Assessment and Analysis Template

Title	**Describe the thing you are assessing for risks - Example (Beach Access matting - St Kilda foreshore) or (Dog off leash Elwood Reserve joint use facility with school)**							
Scope								
Reason for risk assessment	Legal requirements (changes to legislation etc)	Records of incidents, illness & disease	Evaluation of available information including Aust Standards, guidance material etc.	Potential for emergency situations	Review of tasks/activities/ programs	Indication that control measures may be inadequate	Requested by HSR or other area	Other
Location ***(if applicable)***								
Assessment Team								
Assessment Date/Review date								

Risk identified	**Likelihood**	**Consequence**	**Initial Risk Rating**	**Current Controls to Manage Risk**	**Revised Likelihood**	**Revised Consequence**	**Residual Risk Rating**	**Further Planned Risk Treatment Action**	**Action Anticipated Completion Date & Responsible officer**	**Future / target risk rating**	**Notes / Long-term Actions**
Example *What can happen, leading to what event or consequence?* Use wording to describe risk such as: *Failure to….* *Loss of…..* *Inability to…..* *Lack of…..* *Insufficient…* *Inadequate…* *Ineffective…..* *Uncontrolled..*	Analyse the Risk without any controls		Refer to RMF	What is Council now doing to manage this risk or maximise opportunities?	Analyse the risk with current controls in place			Is further treatment needed? What plans or actions are there to reduce the risk further?	Who is responsible to carry out the action? By what date?	What is the estimate of the risk once any further controls are put in place?	Add any information which may explain how you reached this decision or any other explanatory notes.
EXAMPLE 1 Beach access mats shift / move after installation	likely	Mod	HIGH	MOU with Life Saving Clubs (LSC) for reporting change of conditions to Council Fore-warning of extreme weather conditions (BOM) Contractors & Council staff inspection obligations Contractors "on call" to re-install mats to original location	Poss	Mod	MEDIUM	Establish a schedule of inspections to ensure mats are in correct location and pined down properly	Who is responsible to carry out the action? By what date?	Target Risk Rating	


CITY OF
PORT PHILLIP