Risk Management Framework

Date of approval
April 2017

Responsible Manager/s
Executive Manager Service Business and Improvement

TABLE OF CONTENTS

Appendices

1. INTRODUCTION

The City of Port Philip (Council) provides a diverse range of services to 110,000 residents in one of Victoria's most densely populated municipalities. Council is required to plan for and manage growth and change, deliver on its objectives within the context of significant population, climate and urban change as well as increased legislative and regulatory compliance obligations and financial accountability.

It is incumbent on Council to understand the internal and external risks that may impact the delivery of its organisational goals and have processes in place to identify, mitigate, manage and monitor those risks to ensure the best outcome for Council, staff and the community.

The Australian/New Zealand ISO Standard on Risk Management [1] describes ***risk*** as "*the effect of uncertainty on objectives*". Risk is the probability of an internal or external situation (an incident) having the potential to impact upon Council; preventing Council from successfully achieving its objectives, delivering its services or capitalising on its opportunities. Risks are an everyday occurrence that could potentially impact on Council's ability to meet its obligations to stakeholders and the community. Council recognises that while some risks cannot be fully eliminated they can be identified, controlled and managed to an acceptable level.

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

Council's Risk Management Framework ('Framework') is aligned to the ISO Standard 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:

4. It is good practice to understand the strategic and operational risks and opportunities facing Council in order to make informed decisions and meet organisational and strategic goals;
5. Council provides critical services and infrastructure to the residents and visitors of this municipality; and
6. 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

[1] Australian / New Zealand ISO Standard on Risk Management: AS/NZS ISO 31000-2009

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 approved every two years by the Executive Management team and noted by Council. This document should be read in conjunction with Council's Risk Management Policy.

2. RISK MANAGEMENT PRINCIPLES

All levels of the Council shall commit to incorporating the following principles from the ISO Standard. Risk management will:

- Create and protect value;
- Be an integral part of Council's organisational processes;
- Be part of the decision-making process;
- Explicitly address uncertainty by providing a framework in which risk can be assessed;
- Be systematic, structured and timely;
- Be based on the best available information;
- Be tailored to Council's internal and external environments;
- Take into account Council's human and cultural factors;
- Be a transparent and inclusive process;
- Be dynamic, iterative and responsive to changes; and
- Continually improve.

3. RISK MANAGEMENT OBJECTIVES

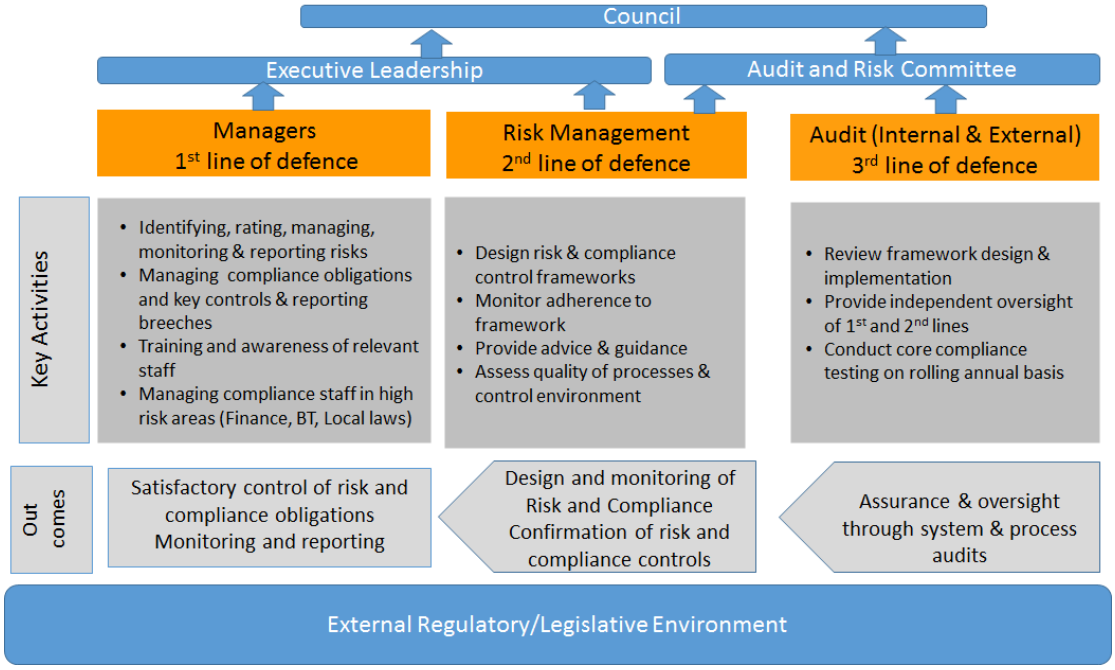
The primary objective of the Framework is to support the achievement of Council's strategic objectives contained in the Council Plan and safeguard the council's resources, people, finance, property, knowledge and reputation through:

- Provision of a structured and consistent approach to identifying, rating, mitigating, managing and monitoring risks;
- Assisting decision makers to make good management decisions within an environment of tolerable strategic and business risk limits, including identifying and leveraging opportunities. The Risk Profile should be used to challenge and inform strategic decisions;
- An environment where staff understand and assume responsibility for managing the risks for which they are responsible and the controls to mitigate those risks;
- Provision of relevant, timely information across clear reporting structures; and
- Independent assurance and audit activities to provide feedback to management that quality processes and controls are in place and are effective.

For the Framework to be effective it must be integrated into Council's strategic and business planning cycles.

4. THREE LINES OF DEFENCE MODEL

The Three Lines of Defence model provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties.



4.1 Ist Line of Defence – Departmental managers

Each Department is responsible for the ownership and management of their risks. They are also responsible for implementing corrective actions to address process deficiencies. Each Department naturally serves as the 1st line as controls are designed into systems and processes under their guidance. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes and unexpected events.

In some areas, specialist compliance roles have also been established to assist in promoting and monitoring compliance e.g. Finance and Business Technology.

4.2 2nd line of defence: risk management and compliance functions

The risk management and compliance functions ensure that the Framework is fully embedded, operational and monitor the 1st line controls to ensure that risks are being effectively managed. It is a risk management function that facilitates and monitors the implementation of effective risk management practices by management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organisation. Each of these functions has some degree of independence from the first line of defence.

4.3 3rd line of defence: 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.

5. ORGANISATIONAL RISK CULTURE

The Chief Executive Officer has the ultimate responsibility and accountability for ensuring that risk is managed across the Council supported by the General Manager, Organisational Performance.

The Chief Executive Officer and the Executive Leadership Team (ELT) provides governance leadership, agrees the strategic direction and risk appetite, promoting the culture and 'tone from the top', to ensure the best outcome for Council, staff and the community.

Council will actively consider risks during strategic and tactical decision-making processes as will all levels of management and will determine the level of residual risk/appetite they are willing to accept, at least annually. 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.

Management will conduct full six monthly reviews of their Department risks (facilitated by the Risk & Assurance Team) with monthly monitoring of High > risks and quarterly 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 organisation change, major process or system change, failure of controls, a major incident, a compliance breach, serious complaint or significant near miss.

Council will invest the appropriate time and resources into training and awareness for all staff but in particular for managers and nominated risk and control owners and staff with specified risk and emergency management roles.

6. RISK MANAGEMENT GUIDELINES

The Council has finite resources, time and budget to manage all aspects of its activities. It is therefore vital that Council apportion resources into the areas of most need, or that will have the greatest impact. Council will therefore take a risk based approach to managing operational risks as follows:

- Risks are initially identified and assessed on an Inherent basis - the risk that an activity would pose if ***no controls*** or other mitigating factors were in place. Determining the Likelihood and Impact of the risk occurring allows Council to understand which risks are of greater concern and must therefore be mitigated accordingly.
- The Residual Risk - the risk that remains ***after the effectiveness of controls*** are taken into account (the risk after controls) - can then be determined by assessing the effectiveness of controls in place to mitigate the Likelihood and Impact of the risk occurring.
- All risks will be captured in an organisational Risk Register (Excel spreadsheet) and reported regularly through the various Management and Committee structures.

7. RISK APPETITE

Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that the City of Port Phillip is willing to accept in pursuit of its objectives. 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 by considering:

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

Risk appetite should be set for each individual strategic risk and tolerance levels agreed, using relevant performance indicators which are monitored through the monthly enterprise reports.

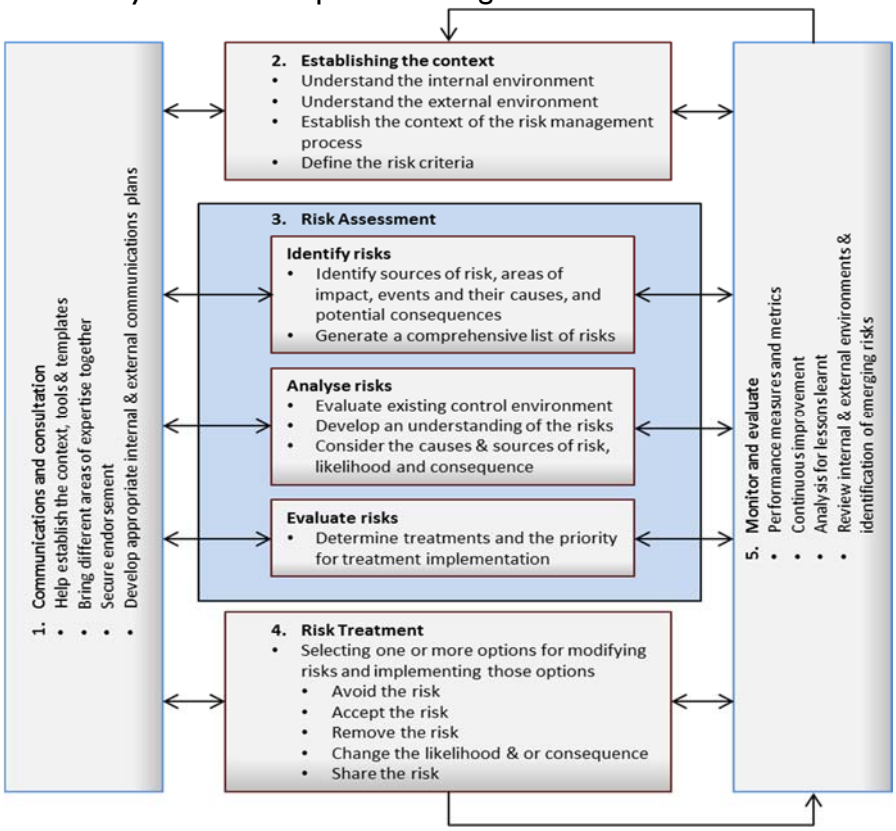
For operational risks, Council's risk appetite will inform the annual risk process, controls and assurance activities and is generally defined as follows:

Risk Rating	Minimum treatment required	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.

8. RISK MANAGEMENT PROCESS

The risk management process is the "how to" element of the Framework and is defined in the ISO Standard as "the systematic application of management policies, procedures and practices to the task of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk." 1

City of Port Phillip: Risk Management Framework 2016



8.1 Communication and consultation

Communication and consultation with internal and external stakeholders are important elements at each step of the risk management process. Effective communication is essential to ensure that those responsible for implementing risk management and those with a vested interest understand the basis on which risk management decisions are made and why particular actions are required.

Key direction over a four year period is set through the adoption of the Council Plan, which is reviewed annually to ensure it continually reflects community priorities. Council is dependent on the Framework to be used at the strategic and departmental business level to improve performance by the organisation in the achievement of Council's strategies and actions as detailed in the Plan.

8.2 Establish the context

Establishing the strategic and operational context, in which the risk management process will take place, defines the parameters within which risks must be managed, the criteria against which risk will be evaluated and the structure of the analysis.

8.3 External context

In addition to considering the external environment, this also includes the relationship or interface between the Council and its external environment. This may include:

- Business, social, regulatory, cultural, competitive, financial and political environment;
- International, National, State, Industry and Community impact, trends and practices;
- Council's external opportunities and threats
- Health and Safety;
- Media;
- Legal and Regulatory obligations; and
- Strategic relations with external or stakeholders and key 3rd party service providers.

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 properly taken into account.

8.4 Internal context

An understanding of Council as an organisation is important prior to understanding the risk management process, regardless of the level. Areas to consider include:

- Goals and objectives and the strategies that are in place to achieve them;
- Culture;
- Strategic Council Plan, budget and drivers;
- Internal stakeholders;
- Occupational Health and Safety;
- Governance and structure;
- Capabilities in terms of resources such as people and systems;
- Processes; and
- Council's internal strengths, weaknesses, opportunities and threats (SWOT)

8.5 Risk management context

The level of detail that will be entered into during the risk management process must be considered prior to commencement and should be commensurate with the extent and nature of the inherent level of risk. The extent and scope of the risk management process will depend on the goals and objectives of the Council activity that is being addressed, as well as the budget that has been allocated to that activity.

In each instance, consideration must also be given to the roles and responsibilities for driving and undertaking the risk management process. The next phase involves three interconnected stages - Risk Identification, Risk Analysis and Risk Mitigation.

8.6 Risk identification

The purpose is to identify all risks: the what, when, why and how incidents might impact on the achievement of objectives. Comprehensive identification using a well-structured systematic process is critical, as a risk not identified will be excluded from further analysis, so identification should include all risks, whether or not they are under the control of Council.

An incident relates to the failure of people, processes, systems or from external factors (e.g. fire, flood, assault or damage). In other words, something has gone wrong: a control failed to operate as expected, was not performed, was circumvented or perhaps there was no control in place. Incidents can have multiple and varied impacts:

- Financial (e.g. Losses, Costs, Fines, Penalties)

- Non-Financial (e.g. Customer, damage to Reputation/Assets, Regulatory, Business interruption)

Depending on the circumstances, incidents will typically be captured or identified as:

- IT outages/incidents
- Customer complaints
- Fines/Penalties
- Insurance claims
- Litigation/Legal related incidents
- OH&S incidents/breaches/concerns
- BCP related incidents/breaches/concerns
- Fraud (internal or external)
- HR related incidents / concerns such as termination issues or staff complaints
- Vendor / Third Party failure

Capturing, understanding the root causes and investigating incidents is critical as these provide us with important and timely information on the operation and effectiveness of our controls, threats to our business operation and the extent and nature of our risks.

A comprehensive risk identification process is delivered through consideration of the potential influence of each of the elements on the internal and external operating environment on Council objectives.

A systematic process includes working through each goal, objective or planned implementation action, identifying the things that may inhibit, detract from or prevent the achievement of the goal or enhance the opportunity to meet the objective.

Documentation of identified risks occurs through the development of a description of the risk and entry into the Council Risk Register (Microsoft Excel Spreadsheet). The risk description should contain a statement of the risk and include those factors which could cause or contribute to the occurrence of the risk event. A risk, by definition, is a potential for something to happen/a possibility not an actuality and consequently the language used to describe risks should express this element of potentiality.

The Council may use a range of tools and approaches to determine potential risks, including:

- Team based brainstorming with experienced and knowledgeable staff;
- Structured techniques (such as SWOT analysis, process mapping, flow charting, systems analysis or operational modelling);
- Annual strategic, council planning, budget and risk identification workshops,
- Examination and analysis of past reports and incidents;
- Regular compliance reviews (internally and externally);
- Internal review by the ARCo Committee; and
- Reviews by external service providers.

The organisational strategic risks are developed annually in conjunction with the ELT and Councillors, using Council's strategic objectives and plan as a starting point. The organisational operating risks are identified in conjunction with Department managers on an annual basis as a minimum, at meetings with Insurance and Risk staff which run parallel with the organisation's annual business planning cycle. Output from both the Strategic and Department Risk Assessments are to then be used as input to the Business Planning Process.

8.7 Risk analysis

Analysis involves developing an understanding of the risk, the likelihood of the risk occurring and the full range of potential impact/consequences. Identification of likelihood and impact is not scientific: it is a qualitative exercise based on perception and history.

The initial analysis provides the Inherent Likelihood, the Inherent Impact and the Inherent Risk Rating. At this stage, the analysis assumes that all controls have failed or there were no effective controls in place. Whilst this is unlikely, this allows the Council to understand which risks have the greatest potential for disrupting the business operation and therefore require strong and effective controls with appropriate and ongoing oversight.

8.8 Risk registers

Risk registers provides a mechanism for documenting, managing, monitoring, reviewing, updating and reporting risk information. Risk Register design, use and related processes are developed and maintained by the Risk and Compliance Advisor. Council has adopted several risk register templates, each tailored to the classification of risks being managed

8.9 Inherent likelihood

The Inherent Likelihood of a risk occurring is defined as the probability and frequency of its occurrence. It may be easier to ask: 'How likely is it that the risk event would occur?'

The table below is a commonly used format with five levels of Likelihood from Rare (an event that occurs only in exceptional circumstances) to Almost Certain (occurring frequently within a year). Each criterion is assigned a number from 1 to 5. (See Appendix 2- Risk Likelihood Matrix)

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

8.10 Inherent impact

This is defined as the potential impact or consequence of a risk occurring and is generally expressed as being a financial loss, non-financial loss (e.g. damage to reputation, client impact, regulatory impact) or occasionally a gain. Asking 'what would be the impact/consequence of risk XYZ occurring?' may elicit a better response. (See Appendix 1 - Risk Impact Matrix)

Accurately determining the possible multiple impacts can be achieved by utilising the Impact table, which is divided into nine categories and five levels of impact:

Impact Categories:

- Service delivery
- Natural environment/sustainability
- Organisation Wellbeing
- Health & Safety
- Reputation
- Finance
- Legal/Regulatory
- Infrastructure/Assets
- Corporate Information/Systems

Impact Levels:

- Insignificant (1)
- Minor (2)
- Moderate (3)
- Major (4)
- Extreme (5)

A risk may fit into a single category or fall across multiple types and similarly the level of impact may fit into more than one column. It is up to management (with assistance from risk specialists) to determine the type with the highest consequence for inclusion into the risk register.

This consequence matrix document should be reviewed at least every two years with business subject matter experts as part of the Framework review to ensure that categories and descriptions are relevant and reflective of Council's internal and external environments.

8.11 Inherent risk rating

For each of the risks listed from the Risk Identification process, the likelihood of the risk occurring and its impacts can be plotted using the criteria matrices (see below) by multiplying the numbers associated to each criteria of Likelihood and Impact. For example the 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) with the Impact assessed as being 'Major' (= 4).

The resulting level of risk will be shown as the intersection of the two dimensions on the Risk Level Matrix (see below and Appendix 3). This provides the Inherent Risk Rating of 16 = High.

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

= Low Risk

= Medium Risk

= High Risk

= Extreme Risk

8.12 Risk mitigation/treatment

Risk mitigation/treatment involves identifying the most appropriate responses to reducing the inherent risk level to a status acceptable within the Council's risk tolerance. Both controls and treatments are designed to mitigate the risk by reducing the likelihood of negative risks occurring and/or reducing the impact of risks should they occur.

There are a number of treatment options available (See Appendix 4 - Risk Treatment Matrix) and more than one can be applied to any 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. Most risks will have multiple different controls in place, some intended to prevent a risk occurrence, some will detect an occurrence whilst others are designed to respond to an occurrence. Controls are not always performed by the risk owner. For example, Departments will have a key reliance on Technology to manage controls to ensure systems are available and operating as required.

A. Directive Controls are those designed to establish desired outcomes. Examples:

- Setting Council policies, Departmental policy/procedures
- Setting spending limits
- Setting IT configuration standards
- Laws and regulations
- Training seminars
- Job descriptions
- Meetings

B. **Preventive Controls** are designed to discourage errors or irregularities from occurring. They are proactive controls that help to ensure departmental objectives are being met. Examples:

- Training on applicable policies, Department policy/procedures;
- Review and approval for purchase requisitions to ensure they are appropriate before purchase;
- IT access authorisations to ensure access is appropriate;
- The use of passwords to stop unauthorised access to systems/applications;
- Segregation of duties (authorisation, recordkeeping & custody of the related assets should not be performed by the one same individual)
- Physical control over assets
- Locking office door to discourage theft
- Using passwords to restrict computer access
- Shredding documents with confidential information

C. Detective Controls are designed to find errors or irregularities after they have occurred. Examples:

- Cash counts; bank reconciliation;
- Review of payroll reports;
- Compare transactions on reports to source documents;

- Monitor actual expenditures against budget;
- Review logs for evidence of mischief;
- Exception reports which list incorrect or invalid entries or transactions
- Reviews and comparisons
- Physical counts of inventories

D. **Corrective Controls** are intended to limit the extent of any damage caused by an incident e.g. by recovering the organisation to normal working status as efficiently as possible. Examples:

- Submit corrective journal entries after discovering an error
- Complete changes to IT access lists if individual's role changes
- Anti-virus
- System upgrades
- Additional training
- Changes to procedures

E. Transfer the risk

- Risk transfer may be achieved by taking out insurance to facilitate financial recovery against the realisation of a risk
- Compensating a third party to take the risk because the other party is more able to effectively manage the risk
- Risk may be wholly transferred, or partly transferred (that is, shared)
- It is important to remember that it is almost impossible to transfer risk completely. In almost all risk sharing arrangement, a degree of the original risk remains and there is inevitably financial or other consideration for the sharing of the risk. In addition, a new risk is inherited; that of being dependent on a third party to manage the original risk

F. **Eliminate the risk.** Some risks may only return to acceptable levels if the activity is terminated.

G. Accept the risk. A risk may be accepted because:

- the probability or consequences of the risk is low or minor,
- the cost of treating the risk outweighs any potential benefit,
- the risk falls within the agency's established risk appetite and/or tolerance levels, or
- Council has limited/no control over the risk. E.g. natural disasters, international financial market impacts, terrorism and pandemic illnesses. To manage such risks, Council should have a business continuity plan in place to provide effective prevention and recovery

When determining the most appropriate treatment, Council should consider:

- How will the treatment modify the level of risk?
- How do costs balance out against benefits?
- How compatible is the treatment with the overall business objectives?
- Does it comply with legislation?
- Does it introduce new or secondary risks?

Often more than one response may be necessary to address an identified risk. In those cases a combination of responses (controls / mitigations) should be taken into consideration.

Current control environment

To understand the extent to which the likelihood and impact of a risk occurring is being mitigated, the full suite of controls in place must be documented and assessed for effectiveness of design and operation. The assessment should only assess controls that are currently in operation, not those that are planned

Where controls are operated by a third party (e.g. Technology), discussions with the control owner should take place to ensure there is an appropriate assessment of the control that takes into consideration the views of the control owner and the risk owner.

Control Rating

The table below should be provided to assist in the assessment of the controls in use. The Control Rating is the subjective view of the Risk owner and the Control owner(s) and is reflective of the effectiveness of all the controls i.e. controls are not rated individually.

Control Rating	Description
Excellent	• Controls are well designed, documented 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 in place, documented and effective • Some work needs to be done to improve operating effectiveness • Management has some doubts about operational effectiveness or reliability
Fair	• Design of the controls may be largely correct in that they treat most of the causes of the risk, they are currently not effective, or • Some controls are not correctly designed - 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
Unknown	• Controls and status are unknown

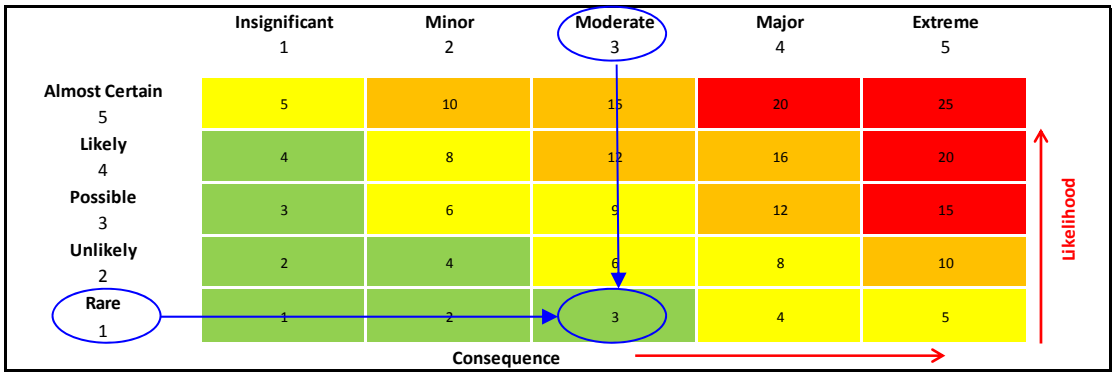
8.13 Residual risk

When the controls have been assessed and rated, the Residual Risk (the amount of risk left over after inherent risks have been reduced by controls) rating can be determined.

For each of the risks listed from the Risk Identification process, the Residual Likelihood of occurrence and potential impacts can be plotted by multiplying the numbers associated to each criteria of Likelihood and Impact. For example the risk of a Fraud occurring in the Payroll process, taking into consideration the effectiveness of controls in place (considered 'Good'), could now be reassessed as follows:

The Likelihood is Rare (= 1) with the Impact assessed as now being Moderate (= 3).

The resulting residual risk (1 x 3 = 3) will be shown as the intersection of the two dimensions on the matrix (see below). This provides the Residual Risk level of 3 = Low. It is likely that no further actions would be required to further mitigate this risk. (See Appendix 3)



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

= Low Risk

= Medium Risk

= High Risk

= Extreme Risk

Alternatively, if controls in place to mitigate a Fraud occurring in the Payroll process are determined to be 'Poor', the inherent risk could be reassessed as follows:

The Likelihood is Possible (= 3) with the Impact assessed as still being Major (= 4).

The resulting residual risk (3 x 4 = 12) would be High. In these circumstances, the Residual risk would be outside of appetite and would require actions to address the controls gaps or weaknesses to further mitigate the likelihood or impact of the risk occurring.

8.14 Residual risk evaluation

This step prioritises the **Residual** risks to be addressed. ELT will set a threshold (Risk Appetite) every two years whereby risks above the threshold are unacceptable and must be addressed and risks below the threshold are treated differently (i.e. recorded/recorded & monitored). The Council has also set criteria for responses to the range of Residual Risk Level ratings. Those criteria are contained in Risk Treatment Matrix (see Appendix 4).

Using the example above – the Residual risk of a Fraud occurring is assessed as being High. Naturally, this is unacceptable so actions are required to develop or enhance controls to mitigate the likelihood and impact of a Fraud from occurring.

- Residual Risks assessed as 'Catastrophic', are likely to impact on strategic objectives and are unacceptable and must be immediately and actively mitigated, managed and monitored by the risk owner.
- Residual Risks identified as 'High' are likely to impact Division or possibly strategic objectives and therefore the ELT are likely to view these risks as unacceptable. The risk owner must actively mitigate, manage and report with ongoing monitoring by the ELT.
- Residual Risks identified as 'Medium' should be assessed on a case by case basis to understand the nature of the risk and whether the strengthening of controls is required, otherwise this can be tolerated if it is determined that impacts won't adversely affect organisational objectives. Medium risks can be managed with controls but must be monitored to ensure the risk exposure is effectively managed and doesn't worsen.
- Residual Risks identified as 'Low' are within operational and organisational tolerances and can be accepted. Low risks must still be recorded.

8.15 Action plans

Where control weaknesses are identified and the decision is taken that further mitigation is required (i.e. the residual exposure is not accepted), an action plan must be established.

All actions must be:

- **Owned**: who is responsible for ensuring the action is addressed
- **Specific**: the exact activities that will be undertaken
- **Timely**: must be completed within appropriate time frames, commensurate with the significance of the gap/weakness
- **Achievable**: the action/activities must be realistic to ensure appropriate mitigation
- **Measurable**: it must be possible to quantify the action or have a means of assessing progress
- **Justified**: can demonstrate a further reduction in the Residual Likelihood and/or Impact
- **Governed**: tracked, managed and reported

8.16 Monitor and review

The risk assessment process provides a snap shot of the Council's risks, controls and action plans at a given point of time – the Risk Register. 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.

As the external and internal environment in which we operate is fluid, therefore the influences on our objectives continue to ebb and flow. In addition, assumptions have been made in relation to both the quality of response strategies which are already in place and the implementation and quality of proposed responses. As a result, the risk management process is iterative and should be the subject of a structured monitoring and review process.

8.17 Ongoing review of material risks

Risk and the effectiveness of control measures to manage risk need to be monitored on an ongoing basis to ensure changing circumstances, such as the political environment and the Council's strategic objectives and risk appetite do not alter the risk evaluation profiles and adequacy assessments. New risks or deficiencies in existing mitigation strategies may be identified via a number of sources:

- changes in the strategic objectives;
- Regular review of the identified risks and mitigation strategies;
- The annual Internal Audit program;
- Ongoing monitoring by various Committees, including ELT and ARCo;
- New legislation;
- New accounting standards, guidelines or information from any regulator
- IT outages
- Complaints
- Regulatory / Compliance breaches
- Incidents
- External Audit

- Projects or Change Initiatives

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 at least quarterly. The effectiveness of risk responses will be continuously monitored by the responsible manager/officer and reviewed six monthly.

8.18 Alignment to the strategic plan

For risk assessments associated with the whole of Council or individual departments, the review process will be built into the business planning process.

Output from the Strategic Risk Assessment and Business Unit Risk Assessments are to be used as input to the Business Planning Process. That input will include risk response plans. Internal Audit will use the information from the Business Planning Risk Assessments, in particular the risk response plans, to assist with development of the Internal Audit plan.

To ensure that the identified strategic risks, and measures in place to manage them, remain aligned to the Council's strategic objectives, any material change to the Strategic Plan will trigger a review of the RMF, most particularly the RAS and the Risk Management Process.

9. PROJECT RELATED RISKS

In relation to project based risk assessments, the risk treatment plan provides the project manager with a tool to continuously monitor project improvement through the implementation of the plan. Issues and delivered risks identified through the course of the project must be assessed and included in the project risk register, having gone through the full risk assessment process outlined above. This will ensure the continuing relevance of the risk assessment.

10. RISK REPORTING

Reporting associated with the Risk Management Framework is structured to satisfy two criteria:

a) Information relating to the City of Port Phillip's existing risk profile; and
b) Information relating to the City of Port Phillip's implementation, performance and status of the Framework.

The table below indicates the reporting responsibilities and frequency

Report Name	Author	Recipient	Frequency
Strategic Risk Assessment	Service & Business Improvement	• Council • Executive Leadership Team (ELT) • Audit & Risk Committee	Annually + 3 monthly check in
Divisional Risk Register Status Report	Risk & Assurance Team	ELT Audit & Risk Committee	Monthly Quarterly
Department Risk Assessment(s)	Managers (facilitated by Risk & Assurance Team)	ELT	Annually + Monthly check in for High / Catastrophic risks
Risk Treatment Actions on Track	Responsible risk action owners (facilitated by Risk & Assurance Team)	ELT Audit & Risk Committee	Quarterly
** Attestation of control effectiveness	Risk & Control owners	ELT Audit & Risk Committee	Annually

** In the process of implementing this Audit recommendation

11. RISK TRAINING

To ensure the successful implementation of risk management throughout the organisation, it is planned that appropriate training in risk management will be provided to staff and managers. Training should encompass the risk management process, application of risk management tools, assistance with identification and analysis of Council's risk exposures, risk profiling and reporting.

In addition, the organisation's Risk Management Team will coordinate with People and Organisational Development Department and all Work Units to work towards ensuring:

- Induction training will include Risk Management, Fraud awareness and Employee Code of Conduct.
- Employees receive regular Risk Management awareness and Fraud awareness update training (at minimum, a half-day refresher course once every two years for those staff directly involved in financial and/or cash transactions).
- Any updates and changes to the Risk Management Policy, Framework, Fraud related policies, procedures; Codes of Conduct, ethics etc. are circulated to all employees via the Intranet or email where deemed necessary.

12.ROLES AND RESPONSIBILITIES

The Responsible, Accountable, Consulted, Informed (RACI) table (see Appendix 5) illustrates accountabilities across the varied risk roles at Council.

Risk Management within the Council is an integral element of good business practice. The Strategic and Operations Risk Assessment Processes are integrated with the Strategic Planning and Business Planning processes.

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 Risk Management Framework has specific elements which require defined alignment of roles and responsibilities. The responsibilities for each of the roles identified are as follows:

12.1 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 and Risk Committee.

12.2 Audit and risk committee

- Oversee 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.

12.3 Executive leadership team (ELT)

- The CEO, supported by the General Manager Organisational Performance, 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 and approved quarterly (monthly for high> risks);
- Report expeditiously to ARCO on any fraud and corruption incidents or material risk mitigation failures and actions taken.

12.4 Internal audit

- Consider strategic and operational risks in the development and implementation of the Internal Audit and Compliance Plan and recommending improvements.
- Periodically auditing Council's Risk Management practices and providing recommendations on improvement to management and the Audit and Risk Committee.

12.5 Executive manager, service & business improvement

- 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.

12.6 Risk & assurance coordinator

- Lead 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, 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 Audit and Risk Committee.
- Measure enterprise risk management maturity and report on the implementation of actions to achieve target maturity.

12.7 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 Compliance Advisor.

12.8 OHS manager

- 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.

12.9 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.

12.10 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 icw Control owner

12.11Control 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 icw 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.

12.12 Risk champions

- Person of Coordinator level who takes risk responsibility for a Department or Division;
- Ensures coordination of activities such as risk assessments and reporting are completed;
- Liaises with Risk & Compliance advisor;
- Identifies gaps in areas such as training / awareness; and
- Assists with communications and training.

12.13 Staff, contractors and service providers

- Applying risk management practices in their area of work and ensuring that management are aware of risks associated with council's operations.
- Recommending or providing suitable plans to manage risks; obtaining appropriate approval prior to action (where required); and reporting on risk management practices.

13. PERFORMANCE MONITORING

Risk management performance indicators include:

- Monthly report to ELT on status High > rated risks
- Monthly report to ELT on % Audit Actions completed on time
- Quarterly reports to ELT / Audit & Risk Committee on status High > rated risks
- Quarterly report to ELT on % of Catastrophic & High Risk Control Actions On Track
- Quarterly report to ELT on Risk Management Maturity Improvement Targets Met

14. LIST OF APPENDICES

14.1 APPENDIX 1: IMPACT MATRIX

	INSIGNIFICANT	MINOR	MODERATE	MAJOR	EXTREME
SERVICE DELIVERY	Inability to deliver non-essential services within specification for a period of < 3 days.	Inability to deliver non-essential services within specification for a period of > 3 days but < 1 week.	Inability to deliver essential services within specification for a period of < 3days or Inability to deliver non-essential services within specification for a period > 1 week.	Inability to deliver essential services within specification for a period of > 3 days but < 1 week. or Inability to deliver critical service within specification for a period of < 3 days	Inability to deliver essential services within specification for a period of > 1 week or Inability to deliver critical services within specifications for a period of > 3 days
	"Critical Services" include those which directly impact the immediate health& safety of the community and include Information, home care, Meals on Wheels "Essential Services" include those which have a longer term (not immediate) impact on immediate health / safety and includes waste collection and disposal (and fill), essential				
NATURAL ENVIRONMENT / SUSTAINABILITY	Single occurrence which causes environmental harm with no ongoing affect.	Repeated occurrences which cause environmental harm with no ongoing affect.	Single or repeated occurrences which cause ongoing environmental harm which is able to be remediated in < 2 years.	Single or repeated occurrences which cause ongoing environmental harm which is able to remediated in > 2 years but < 5 years	Single or repeated occurrences which cause ongoing environmental harm which cannot be remdiated in under 5 years.
ORGANISATION WELLBEING	Localised employee dissatisfaction resulting in a Staff Satisfaction rating drop of 5% Increase in turnover of personnel or absenteeism of < 5%	Localised employee dissatisfaction resulting in Staff Satisfaction rating drop of >5% but <10% Increase in turnover of personnel or absenteeism of >5% but <10%	Localised employee dissatisfaction resulting in Staff Satisfaction rating drop of > 10% but <15% Widespread employee dissatisfaction resulting in Staff Satisfaction rating drop of <5% Increase in turnover of personnel or absenteeism of >10% but <15%	Localised employee dissatisfaction resulting in Staff Satisfaction rating drop of > 15 Widespread employee dissatisfaction resulting in Staff Satisfaction rating drop of >5% but <10% Increase in turnover of personnel or absenteeism of >15% but < 25%	Widespread employee dissatisfaction resulting in Staff Satisfaction rating drop of >10% Increase in turnover of personnel or absenteeism of > 25%
HEALTH AND SAFETY	Any injury or disease which required first aid treatment only – no lost time.	Injury or disease requiring medical treatment and which is likely to result in a person being incapacitated from normal activity for a continuous period of less than 7 days.	Injury or disease requiring medical treatment and which is likely to result in a person being incapacitated from normal activity for a continuous period greater than 7 days.	Total or permanently disabled.	Fatality
REPUTATION	Complaint by one or a number of un-associated members of the general community.	Complaint by a group from the community which is escalated into the public arena. Or Minor adverse local media attention.	Serious attention / concern from the public, State media or stakeholders which will be overcome within < 3 month.	Significant attention / concern from the public, National media or stakeholders which will take longer than 3 months to overcome.	Ministerial intervention / Appointment of Commissioners.

14.1 APPENDIX 1: IMPACT MATRIX continued

	INSIGNIFICANT	MINOR	MODERATE	MAJOR	EXTREME
FINANCE	Negative financial impact (increased costs , lost revenue of direct loss) of < $5k	Negative financial impact (increased costs, lost revenue or direct loss) of > $5k and < $250k.	Negative financial impact (increased costs, lost revenue or direct loss) of >$250k and < $1M	Negative financial impact (increased costs, lost revenue or direct loss) of >$1M and <$10M	Negative financial impact (increased costs, lost revenue or direct loss) of >$10M
LEGAL / REGULATORY	Civil litigation or breach of contract which results does not result in legal remedy or Statutory breach which results in issue of a PIN notice.	Civil litigation or breach of contract which results in non-material legal remedy or Statutory breach which results in non-material fine or Imposition of Prohibition Notice	Civil litigation or breach of contract which results in material legal remedy. or Statutory breach which results in a material fine. or Suspension of a non-material licence, permit etc.	Civil litigation or breach of contract which results in action taken in the Supreme Court or Federal Court. Or Statutory breach which results in a significant fine. Or Suspension of a material licence, permit etc.	Civil litigation or breach of contract which results in action taken in the Full Court. or Statutory breach which may result in imprisonment.
INFRASTRUCTURE / ASSETS	Localised damage to a single general asset which can be remedied within a short time frame.	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.	Localised damage to a single critical 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.	Localised damage to a single critical 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.	Wide spread damage to a number of critical assets which can be remedied over a long time frame or Total and permanent destruction of one or more critical assets.
CORPORATE INFORMATION / SYSTEMS	Loss of Low Risk data / information or systems	Loss of Moderate Risk data, information or systems for a period of < 7 days	Loss of Moderate Risk data, information or systems for a period of > 7 days	Loss of High Risk data, information or systems for a period of < 24 hours Or Unauthorised access to sensitive / private information for < 1 week	Loss of High Risk data, information or systems for a period of > 24 hours Or Unauthorised access to sensitive / private information for > 1 week

14.2 APPENDIX 2: LIKELIHOOD MATRIX

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

14.3 APPENDIX 3: RISK LEVEL MATRIX

		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 4: RISK TREATMENT MATRIX

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

14.5 APPENDIX 5: RACI Matrix

	Responsible (R) - Accountable (A) - Consulted (C) - Informed (I)											
Activity	**Staff (includes volunteers /**	**Coordinator / Team Leader**	**Manager**	**Risk Champion**	**Risk Management & Insurance**	**Risk Owner**	**Control Owner**	**ELT**	**CEO**	**ARCo**	**Council**	**Audit**
Risk Culture	I	I	C	C	C	R	R	R	A	I	A	
Risk Appetite setting	I	I	C	C	C	R	R	R	A	A	A	
Risk Policy & Risk Framework	I	I	I	C	R	C	C	A	A	I	A	
Risk tools / matrices	I	I	I	C	R	C	C	I	I	A	I	
Communication	I	I	R	R	R	R	R	C	A	I	I	
Training / Awareness	I	I	I	C	R	C	C	A	A	I	I	
Hazard identification	R	R	R	R	R	R	R	R	R	R	R	
Risk Assessment / Evaluation	I	C	C	R	R	C	C	A	A	I	I	
Out of cycle risk assessment	C	C	R	R	C	R	C	A	A	I	I	
Risk treatment strategies / action plans	I	C	C	R	C	C	A	A	A	I	I	
Monitoring	I	R	A	C	C	A	A	A	A	A	I	I
Reporting	I	C	R	R	R			A	I	I	I	I
Assurance	I	I	C	R	R	C	C	A	A	C	I	R
Attestation	I	R	C	R	C	A	A	I	I	I	I	
BCP / Emergency Management	I	R	R	R	R	R	R	R	A	C	I	
Post incident reviews	C	C	C	R	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

14.6 APPENDIX 6: RISK DEFINITIONS

Council has adopted the following Risk Management definitions from the Australian/New Zealand Standard ISO31000:2009

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 consequence.
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 what events may occur, the likelihood of occurrence and the magnitude of their consequences.
Likelihood	The possibility of an event happening (probability).
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.

14.7 APPENDIX 7: 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		