Enterprise Risk Management Framework

SVC-RM-Pln-002-01

TABLE OF CONTENTS

PART 1 - OVERVIEW

1.1 Scope of the Risk Management Framework

This document outlines the Enterprise Risk Management Framework for Snowy Valleys Council (Council) and all its operations. The Framework defines Council's risk management process, methodology, appetite, training and reporting, and establishes the responsibilities for implementation.

Risk management is part of the Council's day-to-day operations and is undertaken at Divisional and Directorate levels as well as more broadly at the overall Council level. The overall aim of risk management within the Council is to ensure that organisational capabilities and resources are employed in an efficient and effective manner to manage both opportunities and threats.

1.2 Objectives of the Risk Management Framework

The objective of this Enterprise Risk Management Framework is to provide a formal process to assist the Council in:

- Encouraging understanding by managers and their staff of the implications of risk exposures, opportunities and their risk management, in their day-to-day work and in strategic and operational planning activities;
- Developing and implementing procedures to ensure that risks are identified, assessed against accepted criteria and that appropriate measures are implemented; and
- Defining and documenting responsibilities and processes.

1.3 Why is Risk Management Important?

Risk influences every aspect of Council operations. Understanding the risks we face and managing them appropriately will enhance our ability to make better decisions, safeguard our assets, enhance our ability to provide services to our community and to achieve our mission and goals.

Council views the management of risks to its people, assets and all aspects of its operations as an important responsibility. Council is committed to upholding its moral, ethical and legal obligations by implementing and maintaining a level of risk management which protects and supports these responsibilities.

An effective Enterprise Risk Management Framework is not only good business practice but provides organisational resilience, confidence and benefits, including:

- Providing a rigorous decision-making and planning process;
- Providing Council with the flexibility to respond to unexpected threats;
- Taking advantage of opportunities;
- Equipping managers with tools to anticipate changes and threats that may face Council and to allocate resources appropriately;
- Providing assurance to the Executive Leadership Team and Council that critical risks are being managed appropriately; and
- Enabling better business resilience and compliance management.

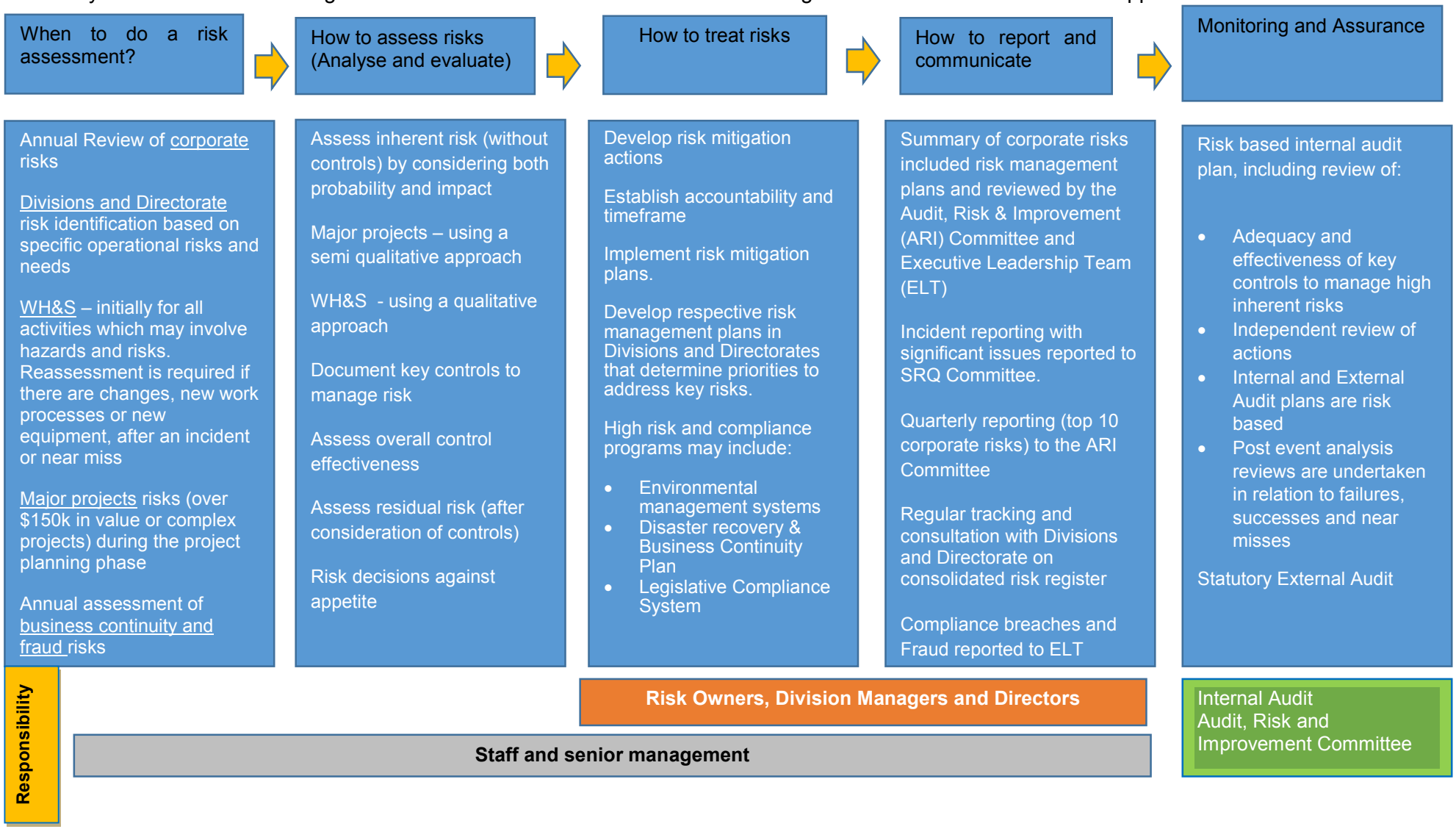
1.4 Definitions

Term	Definition
Risk	The chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood
Residual risk	The remaining level of risk after risk treatment measures have been taken into account.
Risk acceptance	An informed decision to accept the consequences and the likelihood of a particular risk
Risk analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk assessment	The overall process of risk analysis and risk evaluation
Risk control	That part of risk management which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse risks.
Risk identification	The process of determining what can happen, why and how.
Risk management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects
Risk Management process	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk
Risk treatment	Selection and implementation of appropriate options for dealing with risk
Risk Owner	Person or entity with the accountability and authority to manage a risk.

PART 2 – ENTERPRISE RISK MANAGEMENT

2.1 Risk Management Framework

Summary of Council's Risk Management Framework is below. Council's Risk Management Universe is illustrated in Appendix 1.



2.2 What is risk and risk management?

Risk is the effect of uncertainty on objectives with a likelihood and frequency that something will occur. Risk is expressed in terms of consequence or impact (i.e. how bad/good could an event be if it happens?) and likelihood (i.e. how likely is it that the event will happen?).

As outcomes of operational and business activities can be uncertain, they are said to have some element of risk. In the local government context, risks can be attributed to internal (e.g. new projects, capacity challenges etc.) and external (e.g. change in legislation, state and federal grants).

Risk management involves identifying the types of risk exposure within an organisation, measuring those potential risks and proposing means to mitigate them. While it is impossible to remove all risk, it is important for organisations to understand their risks and manage and identify the level of risk they are willing to accept in the overall context of effective operation and service provision.

Risk management is essential to good management practice and effective corporate governance and ensures decisions are made with sufficient information about risks and opportunities.

2.3 Development of risk registers

Risk registers identify and record the risks facing different areas of business. Identifying risk is a critical step in managing it. Risk registers allow Council to assess the risk in context with the overall Council strategic direction, and help record the controls and treatments of those risks. The adopted register for SVC is held within the Pulse software system. The structure that supports risk management in Council is shown below:

Enterprise Risk Management Framework Component	Objectives Considered	Report on Risk to
Corporate Risk Register	Whole of Council	Council and Audit Risk and Improvement Committee
Operational Risk Register	Individual Directorate or Major Project	Executive Leadership Team

2.4 Risk appetite and tolerance

2.4.1 Risk appetite

Once risks are identified, the adequacy of controls must be considered within the context of Council's risk appetite. The top ten (10) risks of each risk management plan will be reported to the Safety, Risk and Improvement Committee to monitor the level of acceptable risk for high risks, and extent of appropriate mitigating actions.

Risk appetite is the amount of risk, on a broad level, that Council is willing to accept in pursuit of value, and should reflect:

- Capacity to take on risk;
- Council strategic and operational objectives; and
- Evolving industry and market conditions.

Council has no appetite for risks that:

- Compromise the health, safety and wellbeing of staff, contractors and members of the community;
- Significantly disrupts essential services;

- Have a significant negative impact on its long term financial sustainability and assets;
- Constitute a serious non-compliance with its legal obligations;
- Results in significant or irreparable damage to the environment; and/or
- Results in widespread and sustained damage to its reputation.

No appetite for risk means undertaking activities in a way that avoids:

- Serious injury or death;
- Prolonged loss of essential services to the community;
- A breach of legislation; and/or
- Failure to benefit the Council or the community.

Provided that safety, environmental, financial sustainability and legislated requirements are met, Council has a strong appetite for risks that are managed to support:

- Achievement of its Delivery and Operational plan objectives;
- Improved levels of service delivery to the community;
- Innovation in general service delivery
- Reduced costs or improved efficiency;
- Generation of new income sources; and / or
- Improved customer experience.

2.4.2 Risk tolerance

Risk tolerance provides more detail about Council's risk appetite. Risk tolerance defines the absolute limits (expressed as metrics for specific performance indicators) that Council will not exceed. Risk tolerance implies that Council cannot effectively deal with risks beyond these limits.

Council generally considers "high" and "extreme" risks as not being tolerable and requires action to reduce either the likelihood of the risk occurring and or the consequences should the risk occur. In regard to "moderate" and "low" risks, reasonable and practical actions will be taken along with ongoing monitoring to ensure Council's risk exposure does not increase.

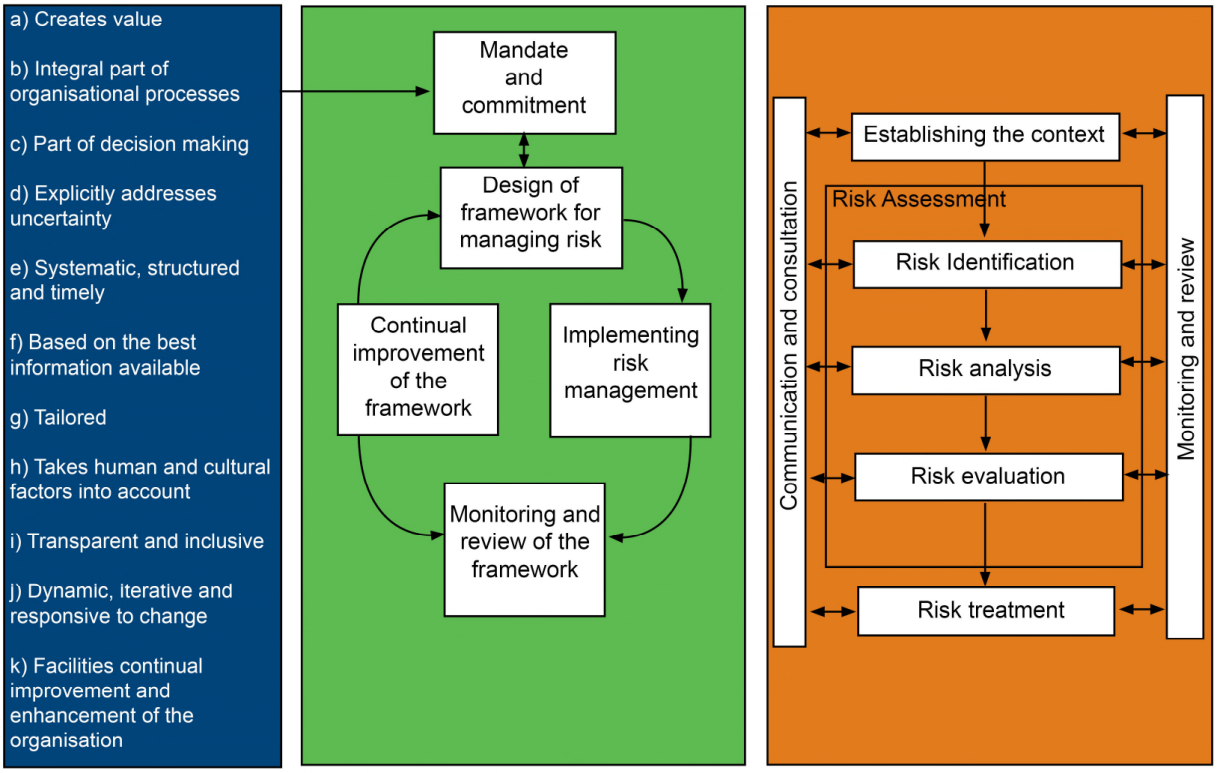
Council will not accept any residual risk that is assessed as "high" unless a documented plan has been approved by the General Manager.

Residual Risks of:

- "High" will be accepted only after a documented plan is approved by the General Manager;
- "Medium" will be managed by Division Managers, by the application of appropriate controls and procedures to reduce the likelihood and consequence of the risks; and
- "low" will be managed locally by Coordinators by the application of appropriate controls and procedures to reduce the likelihood and consequence of the risks.

2.5 Risk management methodology

Council has adopted the Risk Managaement methodology based upon Australian Standard AS/NZS ISO 31 000:2009.



(Extract from AS/NZS ISO 31000: Risk management - Principles and guidelines)

2.5.1 Communication and Consultation

Communication and consultation with stakeholders to ensure understanding of the process and its intended outcomes are key elements in every step of the risk management process. This involves collating reports, facilitating ongoing operational reviews of risk registers, coordinating risk assessments for specific projects and ongoing advice and support to ensure compliance with the Enterprise Risk Management Framework.

2.5.2 Establish context

Risk management takes place within Council's goals and objectives. Therefore, risk management must be placed into both a strategic and operational context.

2.5.2 (a) Strategic Context

Strategic risk identification involves the relationship between Council and the broad external environment/community. A range of issues should be considered in examining the strategic content, including:

- Opportunities and threats associated with the local, regional, state and national economic, social, political, cultural, environmental, regulatory and competitive environments;
- Key thrusts of stakeholder strategies; and
- Strengths and weaknesses of Council in attaining corporate objectives

2.5.2 (b) Operational Context

Operational risk identification involves gaining an understanding of the organisation's capabilities, goals, objectives, strengths and weaknesses by considering:

- Organisational structure and culture;
- Geography and demographics;
- The identity and nature of interaction with key stakeholders;
- The existence of any operational constraints;
- Objectives and key performance indicators;
- Business resilience vulnerabilities;
- Relevant issues relating to recent change management risk, performance or audit reviews;
- Relevant stakeholder community concerns or requirements;
- Regulatory and contractual requirements and constraints; and
- Business management systems.

2.6 Risk Identification and Assessment

2.6.1 Risk Identification

Council will:

- Identify those risks that can potentially impact on the achievement of Strategic objectives;
- Identify those key Operational risks that are inherent in the main functions performed by the organisation;
- Develop a common Risk Register for risk identified for specific, one-off or new projects; and
- Establish a culture where individual activities are risk assessed as part of every function performed.

A number of questions should be asked when attempting to identify risks. These include:

- What can happen? (event or cause)
- Where could it happen?
- When could it happen?
- Why would it happen?
- How can it happen?
- What does this lead to? (impact or consequence)

It is important to consider relevant objectives when answering these questions.

2.6.2 Risk Identification Methods

There are a number of different methods to identify risk, some of which may include:

- Brainstorming sessions with relevant stakeholders or staff
- Checklists developed for similar events/projects/activities
- An examination of previous events/projects/activities of this type
- Individual staff interviews
- Utilising relevant codes or standards.

Risks can be entered directly into the Pulse Risk Management solution.

2.6.3 Risk categories

Council has established a number of risk categories. These risk categories reflect the types of risk consequences to which Council is exposed, and are integrated into Council's risk assessment process. The risk categories will be applied to sort risks as a basis for comparison, reporting and decision making:

Enterprise Risk Management Categories	
Risk Category	**Broad Definition**
Service Delivery	Risks to the operation of the organisation in providing services to the community; impact on assets or infrastructure; impact on projects.
Human Resources	Risks to staff, recruitment, skill shortages, availability, management, moral, retention etc. of Council employees, inadequate resourcing.
Work Health and Safety	Risks relating to accident, injury or illness to Council staff, Councillors, contractors, visitors or members of the public.
Financial	Risks relating to any activity that results in either an increase or a decrease to expenses or revenue; fraud, impact on Delivery Program and Operational Plan.
Environmental	Risks relating to environmental impacts including pollution, climate change, natural climatic events, land use and the natural environment.
Stakeholders	Risks relating to parties external to Council and their relationship/interaction with Council; impact of change; stakeholder expectations.
Corporate Governance and compliance	Risks relating to the efficient and effective direction and operation of the organisation; risks to ethical, responsible and transparent decision making; corruption, fraud risks; risks to compliance with Council policy/procedure; risks relating to legislative compliance; legal matters.
Reputation	Risks relating to generation of positive or negative publicity; deletion or creation of goodwill.
Political	Risks relating to public reaction; risks relating to activities that cause involvement by watchdog agencies such as ICAC; public pressure that impacts on decision-making.
Projects	Risks relating to major projects - including planning, scheduling, scope, procurement, design, quality, repairs & maintenance, materials, and contractor/consultant availability and management. **Note**: consideration and ratings must be given to all other risk categories for each project.
Information, Technology and Communications	Risks relating to the resilience of ICT infrastructure and support systems

2.7 Risk Analysis and Evaluation

The objectives at this step are to separate the minor risks from major ones. The level of risk is determined by measuring the likelihood of each event arising and the associated potential consequences.

2.7.1 Measuring the Level of Likelihood and Consequence

Other than Work Health and Safety Risks, consequence will generally be assessed against the direct financial and operational impacts to Council. However, for some risks the most significant consequence is the impact on Council's reputation rather than the direct financial consequence. For such risks, the direct financial consequence of a risk may be negligible, but continuing reoccurrences may result in significant damage to Council's reputation.

Probability or likelihood estimations are established giving due consideration to the effectiveness of existing control measures.

The Consequence Rating Evaluation Criteria defines the consequence criteria, assessed against potential financial loss, reputation impact, Work health and safety, legal and regulatory compliance and management time and effort.

The limits contained in this Consequence Rating Evaluation Criteria are based on the management's assessment of Council's ability to continue operation in the event of a risk being realised.

2.7.2 Inherent risk rating

An inherent risk rating represents the level of risk in the absence of a control environment and is arrived at after measuring the likelihood and the consequence of an event occurring.

The matrix format ranking has been adopted for Council in which potential risks are ranked as Extreme, High, Moderate or Low. This is as follows:

Table of Risk Ranking

The risk matrix adopted by Snowy Valleys Council is as follows:	**Consequences**				
Likelihood	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost Certain	Medium 08	High 16	High 20	Extreme 23	Extreme 25
Likely	Medium 07	Medium 12	High 17	High 21	Extreme 24
Possible	Low 04	Medium 10	High 15	High 18	High 22
Unlikely	Low 02	Low 05	Medium 11	Medium 13	High 19
Rare	Low 01	Low 03	Medium 06	Medium 09	High 14

2.7.3 Prioritising risks

The purpose of prioritising the risk is to determine the level of action needed for the identified and assessed risks.

2.7.4 Table of Management Action

Description of Risk	Classification and Action Required	Risk Level
Risks that represent a threat beyond Council's capacity and sustainability	**INTOLERABLE OR UNACCEPTABLE RISK** Immediate action required to eliminate or reduce the risk. Must have a Treatment Plan. **Notify the GM, ELT and COUNCIL**	**Extreme 23-25**
Risks that could present a major exposure to Council and jeopardise Council's strategy associated with reputational damage	**CRITICAL OR UNACCEPTABLE RISK** Urgent action required to reduce the risk. Must have a Treatment Plan. **Notify the GM and ELT**	**High 14-22**
Risks that may cause operational problems but are within budget and manageable	**ACCEPTABLE and TOLERABLE RISK** Provided WH&S risks are "As Low As Reasonably Achievable" and other risk controls are effective. **Notify the Division Manager or delegate**	**Medium 6-13**
Risks that are monitored and controlled locally	**ACCEPTABLE and TOLERABLE RISK** Can be managed with existing procedures and controls	**Low 1-5**

2.7.5 Evaluate and record existing controls

Existing controls are identified and the control effectiveness is assessed based on management's understanding of the controls effectiveness.

Table of Control Levels

Level of Control	Audit Definition
Good	A high degree of reliance can be place on the system of internal control. Compensating controls are in place such that even if part of the system breaks down, the four control criteria will probably still be met.
Satisfactory	The controls can be relied upon; however, some improvements to controls can be made
Marginal	The system can generally be relied upon in most circumstances but there are some circumstances where one or more of the four control criteria may not be met
Weak	The system of internal control cannot be relied upon to meet the four control criteria. If there has not already been a significant breakdown, it is only a matter of time before this occurs

The four control criteria are:

- Reliable and accurate information.
- Compliance with policies, plans, procedures, laws, regulations and contracts.
- Safeguarding of assets.
- Economic and efficient use of assets.

2.7.6 Determine the Level of Residual Risk

Residual risk represents the level of risk after taking into account existing controls for each risk. By relating the likelihood and consequence ratings after considering controls for each risk, the level of

residual risk is determined. The Consequence Risk Analysis and Evaluation Criteria for Council's various categories of risk are detailed in the table shown in section 2.8.

2.8 Risk treatment

The objective of this step is to identify how the identified risks will be treated. Risk treatment involves identifying the options for treating each risk, evaluating those options, assigning accountability (for Extreme, High and Medium residual risks) and taking relevant action. The following options are available for treating risks and may be applied individually or in combination, with due consideration of risk appetite:

Avoid the risk	Not to proceed with the activity or choosing an alternative approach to achieve the same outcome. Aim is risk management, not aversion.
Mitigate	Reduce the likelihood - Improving management controls and procedures.
	Reduce the consequence - Putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts.
Transfer the risk	Shifting responsibility for a risk to another party by contract or insurance. Can be transferred as a whole or shared.
Accept the risk	Controls are deemed appropriate. These must be monitored and contingency plans developed where appropriate.

2.9 Monitoring and Reporting

The objective for this step is to monitor the risks and effectiveness of the risk treatment program. Risks should be reviewed regularly to ensure relevancy and currency.

Management carries the principal responsibility for monitoring and mitigation of risk, and of reporting to Council where lack of resources prevent adequate mitigation.

In accordance with its charter, the Audit Risk and Improvement Committee has a role in the oversight of Councils overall risk management program.

PART 3 - DEVELOPMENT OF RISK MANAGEMENT PLANS AND REPORTING

3.1 Development of risk management plans

A Risk Management Plan (or register) outlines the foreseeable risks and provides a set of actions to be taken both to prevent the risk from occurring and reduce the impact of the risk should it eventuate. More specifically, the plan includes:

- List of foreseeable significant risks;
- Rating of the Likelihood and Consequence of each risk occurring;
- Set of preventative actions to reduce the probability of the risks occurring;
- Set of contingent actions to reduce the impact should the risk eventuate; and
- Process for managing risks.

This is managed within the Pulse online system.

3.2 Project Risk Management

Major projects are subject to risk examination and will maintain sufficient risk management plans to provide an effective response in the event of significant operating risks. A major project is a project valued over $150 000 or with a score of over 13 within the adopted project management framework which is a ranking based on the assessment of the project risk, project cost and project complexity.

Projects are being managed within the new Project Management Framework implemented at Council in June 2018. Within this framework all projects require a detailed risk assessment and risks will be monitored both through the project management system and within the centralised risk register. The risk plan should be documented early in the project – during the planning phase, and prior to execution phase. This will ensure any risks identified are addressed during the execution phase.

3.3 Risk Register and Reporting

Council will maintain a central risk register which provides an accurate and complete record of risk assessment and management activities. The Risk Register is mainatined by the risk owners and administered by the Risk Officer. “living documents” which are subject to regular review and updated as risks are addressed and new risks identified, and strategies for current risks updated. Risk are developed within the two (2) classifications - corporate (i.e. Council-wide) and operational level (i.e. Directorates) and within the adopted 9 risk areas.

The Risk Register includes the following core information:

Data item	Data field explanation
Risk ID	Unique identifier which identifies the risk
Date Risk Created	Date risk was created
Risk Category	Relevant to the risk, using the risk categories listed in the Risk Matrix, each risk is to be categorised
Risk Description	A description of the risk, possible causes and impacts
Risk Owner	Risk owner by position title (only one risk owner for each risk)
Initial Risk Assessment	Before controls or mitigating action; risk rating as per Risk Matrix
Current Controls	Existing controls that are in place
Control Type	Type of control is Proactive / Reactive
Control Effectiveness	Level of effectiveness of current controls (i.e.

Data item	Data field explanation
	Substantial/Partial / Ineffective)
Current Risk Rating	Risk rating after controls
Additional Controls / Action Items to mitigate risks	
Additional Description	Identify and capture any future actions that need to be carried out to further reduce risk from “current risk rating” in order to manage the risk to an acceptable level.
Due Date	Stipulate when actions are due to be completed
Responsible Position	Risk owner by position (not name responsible for implementation)
Target Risk	Proposed risk rating after the implementation of mitigating actions

The Risk Register will include, for each risk:

- An initial risk review date within three months of the date a new risk was identified
- Subsequent risk review dates
- Current control(s) which clearly define actions / controls that are currently in place
- Additional control(s) which clearly define actions intended to be taken and a specific officer assigned to implement each additional control
- A risk assessment to determine the level of risk rating (initial, current, and projected) in accordance with Risk Matrix
- Risk review date updated with each risk review
- Any additional comments, actions or notes relevant to mitigate the risk

Risk Owners will be responsible for reviewing and moderating risks within their area of responsibility and accountability quarterly to ensure that the assessment and actions taken are acceptable and within the tolerance and level of delegated accountabilities and responsibilities of the Risk Owner.

3.4 Risk Reporting

Risk reporting supports discussion and decision making on major risk and Council priorities. A quarterly report on top 10 risks (inclusive of extreme risks) and opportunities recorded in the “Risk Register” will be presented to the Executive Leadership Team.

An extract of the risk regsiter showing:

(a) All risks with an assessed residual risk level of extreme or high and
(b) With an inherent risk of extreme or high and a residual risk of low (ie where controls are relied upon for the greatest mitigation of inherent risks)

is to be supplied to the May ordinary meeting of the Audit, Risk and Improvement Committee..

3.5 Monitor and Review

Few risks remain static. Risks will be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk treatment plans will be assessed to ensure changing circumstances do not alter risk priorities.

Feedback on the implementation and the effectiveness of the Enterprise Risk Management Framework will be obtained from the risk reporting process, internal audits and other available information.

Risks and controls will be monitored and tested on a regular basis. Key Risk Indicators (KRIs) may be developed to monitor risks on an ongoing basis. KRI's are operational in nature and should be determined by the Risk Owner once risks and their causes have been identified.

3.6 Audit, Risk and Improvement Committee Procedures

3.6.1 Audit, Risk and Improvement Committee (ARIC) will develop an overall Enterprise Assurance Map to ensure that appropriate coverage is obtained, and reporting lines established for all areas of risk affecting the Council. Development of this will be deferred pending the basic risk management processes reaching an acceptable stage of maturity.

3.6.2 ARIC will develop and annual revise a three (3) year forward Inernal Auidt Plan, based on the extract of the Risk Register (see 3.4 above) to obtain the greatest practicable assurance of council's risk mitigation practices.

3.6.3 Prior to the commencement of an Internal Audit assignment, ARIC will consider the scope of the assignment with a view to effectively targeting the controls most relied upon for risk mitigation

3.6.4 Recommendations from internal audit, external audit or other sources will be dealt with in accordance with the Business Rules for Audit Projects Policy.

3.6.5 In accordance with its charter, ARIC will report at least annually to Council.

PART 4 – AUDIT AND ASSURANCE

4.1 Internal Audit

Internal Audit is a key component of the Council's assurance framework. The primary objective of Internal Audit is to provide an assurance framework to underpin the risk management program. This includes reviews of processes and controls over high risks as determined through the risk planning process. The internal audit function provides independent appraisal of the adequacy and effectiveness of internal controls. Internal audit is responsible administratively to the General Manager and reports to ARIC

Recommendations will be provided, where applicable, for improvements to controls, efficiency and effectiveness of processes. The internal audit function reports directly to the Executive Leadership Team and General Manager. Internal Audit also provides an ongoing cycle of compliance audits of key controls, which is built into the annual audit planning process as approved by the Executive Leadership Team and General Manager.

4.2 Business Continuity Management

4.2.1 Insurance Strategy

Insurance is a means of transferring residual risk. Council's insurance program is reviewed on an annual basis, taking into account the risk profile, the prevailing status of the insurance market and Council's risk appetite at the time.

4.2.2 Disaster Recovery Planning

Operating processes will maintain plans to provide effective response in the event of a significant safety, technology, or environmental incident. Such plans will provide for expedient response to protect the safety and wellbeing of personnel, the protection of Council's assets, and strategies for recovery from unwanted events and minimising disruption to operations.

4.2.3 Business Continuity Planning

A Business Continuity Plan (BCP) will be maintained to ensure that Council is able to effectively deal with any issue that may constitute a significant risk to its reputation, or may adversely impact on the normal operation of Council. A new BCP is to be developed by the end of 2018.

4.2.4 Information Technology – Resilience and Disaster Recovery Planning

A primary objective in developing an Information and Communication Technology (ICT) strategy is to ensure the resilience of ICT infrastructure and support systems. An ICT Disaster Recovery Plan will be maintained to ensure the continuity of ICT systems availability and protection of data in the event of an unwanted event.

4.3 Compliance

Council has an effective system to ensure it is aware of and in compliance with legislative, contractual and policy requirements. The implementation of the new delegations register includes a six monthly update from Councils legal advisors on any changes or additions to council's compliance duties.

PART 5 – TRAINING AND COMMUNICATION

5.1 Training and communication

Council has clarified roles, responsibilities and accountabilities at all levels. The Risk Management Framework is embedded in operations through a number of communication, training and support systems, including:

5.1.1 Training

To ensure that adequate risk management competency levels are achieved and maintained, Council provides regular training in the risk management process and its application.

Specific risk management training sessions will be held every two (2) years, aimed at providing an overview of the Risk Management Framework. Additional ad-hoc training will be provided as required.

5.1.2 Communication of Responsibilities and Accountabilities

Risk management responsibilities, accountabilities and authorities are set out in:

- The Risk Management Policy;
- Positions descriptions;
- Delegations
- Project documentation;
- Performance planning and review documentation; and
- Risk registers.

5.2 Advice and Support

Advice and support in relation to risk management is available by consulting;

- The Risk Officers;
- Council's Risk Management Framework document.

References

1. AS/NZS ISO 31000:2009 Risk management – principles and guidelines, Standards Australia
2. Internal Audit Guidelines (2010), Division of Local Government, NSW Department of Premier and Cabinet
3. ISO 31000:2018 Risk Management Guidelines

APPENDIX 1 – RISK MANAGEMENT UNIVERSE