CLARE & GILBERT VALLEYS COUNCIL

CLARE & GILBERT VALLEYS COUNCIL

RISK MANAGEMENT FRAMEWORK

Responsible Business Unit	Corporate Services
Responsible Officer	Director Corporate Services
Date Adopted	March 2014
Review Date	16 August 2023
Next Review Date	August 2024
Previous revisions	August 2022

1. RISK MANAGEMENT FRAMEWORK

1.1 Introduction

. The Council comprises of a total area of 185,142 hectares. There are 9 Councillors, plus the position of Mayor.

The Clare & Gilbert Valleys district forms part of the traditional lands of the Ngadjuri people and their rich connection and association with this place is recognised.

Our Vision: Clare & Gilbert Valleys will grow our population while maintaining an engaged, vibrant and attractive community with a shared respect for our natural and built environment and a productive economy that fosters innovation and excellence.

The Clare & Gilbert Valley Council is committed to an integrated approach to risk management to:

- protect its workers, assets, liabilities and community against potential exposures
- minimise uncertainty in achieving its Goals, and
- to maximise opportunities to achieve Council's Strategic Objectives.

Council recognises that managing risk is part of governance and leadership, is fundamental to how the organisation is managed at all levels and will contribute to continuous improvement of its management systems.

The risk management process is not an isolated function, but rather should be integrated as part of good management practice. Effective identification, assessment and evaluation of defined risks are critical to Council achieving its strategic objectives, as outlined in the 'Strategic Plan2023-2033' and meeting overall community expectations.

Council's Framework is developed to ensure that the objectives of the Risk Management Policy are achieved. The Framework describes the key principles, elements and processes to guide all staff to effectively manage risk, as a component of day-to-day decision and business practice.

1.2 Purpose

The purpose of the Framework is to provide details of the requirements and processes supporting Council's Risk Management Policy and to maximise opportunities whilst minimising risks that may impact Council from achieving its objectives.

The Framework will:

- Align to the objectives of the Risk Management Policy;
- Ensure consistency in the risk management process & establish roles and responsibilities for managing risk;
- Establish a standardised, formal and structured process for assessment and treatment of identified risks;
- Encourage innovation by integrating risk management into the strategic and operational processes across all Departments of Council.
- Ensure that Council maximises its opportunities, whilst minimising any impacts arising from identifying and evaluating risks;
- Ensure that (standard) reporting protocols are established for information dissemination across all Council areas;
- Assist in the development of a continuous improvement culture integrating the risk management process into management structures.
- Ensure that all risks outside the defined risk tolerances are escalated to the relevant manager and additional treatment options are implemented.

1.3 Legislation and other References

- Local Government Act 1999
- Work Health and Safety Act 2012
- Civil Liabilities Act 1936
- State Records Act 1997
- Commonwealth Privacy Act 1988
- Freedom of Information Act 1991

- AS ISO 31000:2018 Risk Management Guidelines
- SA HB:436.1:2020 Risk Management Guidelines – companion to AS ISO 31000:2018, Part 1: Boards and executives
- Risk Management Policy

1.4 Risk Management Principles

AS ISO 31000:2018 describes risk as:

" the effect of uncertainty (either positive or negative) on objectives "

Risk Management describes the planned and systematic approach used to identify, evaluate, and manage the whole range of business risks and opportunities facing Clare & Gilbert Valleys Council. Risk management involves both the management of potentially adverse effects as well as the fulfilment of potential opportunities. The risk management process will enable Council to minimise losses and maximise opportunities.

The goal is not to eliminate all risks, but rather to manage risks involved in Council's functions and services and to maximise opportunities whilst minimising potential negative exposures.

ISO 31000:2018 is based on the following eight principles, which underpin this Framework and guide how we manage risk across Council:

Integrated	An integral part of all organisational processes.
Part of decision-making	Aids decision-makers in making informed choices and identifying the most effective course of action.
Structured and comprehensive	Contributes to efficiency and to consistent and comparable results.
Best available information	Based on historical and current information, as well as on future expectations, taking into account any limitations associated with such information and expectations.
Customised	Aligns with the internal and external context related to our objectives.

Human and cultural factors	Recognises that the behaviour and culture can significantly influence the achievement of objectives.
Inclusive	Requires appropriate and timely involvement of stakeholders to enable their knowledge, views and perceptions to be considered.
Dynamic	Anticipates, detects, acknowledges and responds to changes in Council's internal and external contexts that result in new risks emerging and others changing or disappearing.
Continual improvement	Learning and experience drives continuous improvement.

2. ROLES AND RESPONSIBILITIES

It is important that there are defined roles for the effective management of risk across Council's structures.

Responsibility descriptions are defined below:

Roles	Responsibilities
Council	• Endorse the systematic approach to managing risk and opportunity across Council operations. • Facilitate resources and guidance in relation to the Risk Management Policy and associated Framework. • To review and consider any report or recommendations regarding the Risk Management Framework. • Ensure there is a systematic and effective approach to managing risk and opportunity across Council operations that is implemented, monitored and communicated. • Apply risk management principles to decision making process.

Roles	Responsibilities
Audit & Risk Committee	• Review and endorse the Risk Management Framework. • Ensure a Framework is in operation and delivers a consistent approach to risk management. • Review reports from management and Auditors and monitor that effective risk and opportunity management controls have been implemented. •
Chief Executive Officer (CEO)	• Review, endorse and implement the Risk Management Policy and Framework. • Promote a strong risk management culture by providing firm and visible support for risk management including ensuring appropriate delegations for the management of risk. • Ensure a Framework is in operation and delivers a consistent approach to risk management. • Ensure Directors have the necessary knowledge and skills to effectively fulfil their risk management responsibilities and are accountable for risks arising from the activities of their departments. • Ensure annual risk management planning is undertaken. • Regularly review Council's strategic and operational risks. • Ensure that appropriate resources are allocated to manage risk.

Roles	Responsibilities
Management Team	• Commitment to and promotion of the Policy and Framework. • Monitor Council's overall risk profile and mitigation strategies. • Ensure that Risk Management is embedded into all critical functions and activities. • Ensure documentation of items on the risk register and ongoing and regular reviews of the risk register including the actioning of any overdue risk treatments. • Include any risk treatments into business plans. • Accountable for implementing the requirements of the Policy and associated Framework within their respective areas of responsibility. • Empowering staff to actively be involved in managing risk. • Reporting on the risk profile and mitigation strategies to the Audit & Risk Committee. • Include any risk treatments into business plans. • Promote a proactive risk culture in accordance with business management initiatives. • Understand and apply the Risk Management Framework within area of responsibility. • Regularly review risks on the risk register (or at least annually). • Undertake actions in relevant risk treatment plans.
Director Corporate Services	• Provide guidance and assistance to all staff in relation to the application of this framework and reporting within the Risk Register. • Ensure relevant risk information is reported and escalated to the Management Team or Audit & Risk Committee or cascaded to staff, as relevant. • Maintain the Risk Management Policy and Framework (including templates) to ensure its

Roles	Responsibilities
	currency and accuracy. • Maintain the Risk Register and timeframes as required. • Provide support and advice to Managers and staff in the application and use of the Risk Management Framework.
Employees, Volunteers & Contractors	• Understanding the risk management processes that are integrated into all Council activities. • Identifying, evaluating, reporting and managing risks in their daily activities and projects.

3. AN INTEGRATED SYSTEM

An integrated risk management system includes the methods and processes used to manage risks and seize opportunities – to achieve defined objectives. Risk Management is not just about the risk assessment process nor is it a stand-alone discipline. In order to maximise risk management benefits and opportunities, it requires integration through Council's entire operations as follows:

3.1 Enterprise Risk Management

Enterprise risk management encompasses Strategic and Operational Risk Management.

Strategic risks are identified by reference to both the external environment and Council's Strategic Management Plan objectives. Strategic risks are monitored by the Executive and Council Member body, with all risk assessments captured in the Risk Register and recorded within Council's Record Management System.

Operational Risks arise from Council's day-to-day departmental functions and operations to deliver essential services. Operational risks are monitored by Council's Executive and/or Management teams.

3.2 Budget & Strategic Planning

Strategic and budget planning considers key risks and opportunities facing the Council at a corporate level. The planning process must identify and review risks that may impact on Council's ability to meet key legislative and strategic objectives.

Council members are expected to:

a) give adequate consideration to risks when setting Council's objectives;

b) understand the risks facing Council in pursuit of its objectives;

c) oversee the effectiveness of systems implemented by the organisation to manage risk;

d) accept only those risks that are appropriate in the context of Council's objectives; and

e) Consider information about such risks and make sure they are properly communicated to the appropriate stakeholder or governing body.

3.3 Internal Audits,Internal Controls and External Audits

The audit process plays an important role in evaluating the internal controls (and risk management processes) currently employed by Council. The internal audits are conducted to provide assurance that key risks have been identified and the controls in place are reasonable. Relevant data arising from all audit functions will be presented to Council's Audit & Risk Committee.

If the council does not have an internal audit function, Council must review and comment in an annual report provided by the chief executive officer in relation to the policies and processes adopted by the council to evaluate and improve the effectiveness of its internal control practices and procedures; and review and evaluate the effectiveness of policies, systems and procedures established and maintained for the identification, assessment, monitoring, management and review of strategic, financial and operational risks on a regular basis; and reviewing any Prudential review

3.4 Business Continuity Plan / Information Technology Disaster Recovery Plan

Council has obligations to ensure that business continues as efficiently and promptly as possible as a result of an interruption. The Business Continuity Plan (BCP) is designed to manage risk by limiting or reducing the impact of a disruption, and to enable the resumption of critical business functions/services of Council.

The main objective of a BCP is to ensure that critical business functions are identified, considered and strategies are employed to ensure that the functions continue in case of a disaster, emergency or major disruption/crisis. A BCP will also assist Council in maintaining its reputation by ensuring that the delivery of critical services is maintained during identified disruptions.

The Information Technology Disaster Recovery Plan is intended to protect and recover Council's Information Technology infrastructure and data in the case of a disruptive event, (such as cyber attack or loss of infrastructure) by defining actions to be taken before, during and after an event.

3.5 Information / Data Management

Not only is it critical to the achievement of objectives that data and corporate knowledge is retained, there are regulatory requirements to do so (eg compliance with the State Records Act 1997, Commonwealth Privacy Act 1988 and Freedom of Information Act 1991).

Council may be vulnerable to cyberattack, malicious intent or unauthorised release should appropriate risk mitigation strategies not be in place.

3.6 Work Health Safety

The Work Health Safety (WHS) system is implemented to manage health and safety risks to people (workers/volunteers) whilst they undertake their role. Work Health and Safety is a critical component of the risk management system and will address risks facing employees conducting their specified duties.

Council has in place an overarching WHS and Injury Management System with a suite of policies and procedures to assist in managing work related risk.

3.7 Local Government Act & Other Legislation

The Local Government Act 1999 applies to the functions of Councils and Prescribed Bodies in South Australia, however due to the diversity of functions provided, a rage of other Act and Regulations apply.

3.8 Coverage & Claims Management – Local Government Risk Services (LGRS)

From the perspective of the Local Government Sector, certain *insurable* risks have been transferred to a number of self-managed Schemes managed by Local Government Risk Services (LGRS) – via payment of an annual contribution. The Schemes are:

- **Local Government Association Mutual Liability Scheme** (LGAMLS) for the purposes of civil liability coverage & claims management;
- **Local Government Association Workers Compensation Scheme** (LGAWCS) for the purposes of workers compensation coverage & claims management;
- **Local Government Asset Mutual Fund** (LGAMF) for the purposes of asset and fleet coverage & claims management.

As a Member of all the above Schemes and Fund, Council must ensure that WHS, Asset and risk management protocols are developed, endorsed and implemented across all departments.

Both the LGAMLS and LGAWCS require member Councils to participate in a Risk Evaluation and WHS evaluation programme, which provides the Sector with profiling data and annual Action Plans for internal continuous improvement.

3.9 Council and Committee Reporting

Risk Management is a part of everyday organisational and strategic decisions – as a part of this Risk Management should be included in Council Reports and decision making process. The Risk Assessment process is adapted into Council and Committee reports, to be used when making decisions.

3.10Risk Management Awareness

The Risk Management Framework, and supporting policies and tools are made available to all workers through the intranet. Risk management awareness

strategies, including training and workshops; will be completed by workers - to increase the Council's risk management culture.

3.9 Emergency Management

Council plans for, and undertakes, prevention, preparedness, response and recovery activities to support its community in the event of emergencies and natural disasters. This process includes alignment and co-operation with lead agencies and other Councils in the region as well as providing information and training for workers to protect them from harm whilst responding to emergencies and natural disasters.

3.10 Performance Management

Both risk management and performance management start with the establishment and communication of corporate goals and objectives, and development of strategies which are then cascaded throughout the organisation. Appropriate measures and reporting structures will be put in place to monitor the effectiveness of Council's risk management processes, (at an individual and organisational level), which will in turn assist in identifying gaps or emerging risks.

4. THE RISK MANAGEMENT PROCESS

The Risk Management process for managing Clare & Gilbert Valleys Council risks is consistent with the Risk Management Guidelines AS ISO 31000:2018. It involves five key steps and two additional steps to ensure feedback through monitoring and a review process; and appropriate communication and consultation. Opportunities are also undertaken in the following manner.

4.1 Communication & Consultation:

Communication and consultation are important elements in 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 interested, understand the basis on which risk management decisions are made and why particular actions are required.

It is important that the communication approach recognises the need to promote risk and opportunity management concepts across all management and staff.

Council will engage with stakeholders throughout the risk management process to:

- Correctly identify risks and understand context;
- Gain a better understanding of the views and interests of stakeholders and how their expectations may be managed;
- Capitalise on the diversity of knowledge, opinions and experience to enhance identification and management of risks and opportunities; and
- Build a sense of inclusiveness and ownership amongst stakeholders.

4.2 Defining the Scope

Because the Risk Management Process is applied at different levels throughout the organisation, it is important to define the scope and its alignment with the organisation's objectives. This will include consideration of goals and objectives, proposed outcomes and timing risk management methodologies and process, activities and projects and how they interact with other processes, activities and projects.

4.3 Establish the Context:

Establishing the context is designed to get those involve in the risk management process thinking about what they are conducting a risk assessment on. Regardless of the type of risk there will always be internal and external factors that may place uncertainty on objectives. For any risk assessment, determine what the objectives of the assessment are and those of the service, activity or event.

Potential Risk Factors have been grouped into categories to assist in establishing the context, ease of identification and reporting by risk managers.

4.3 Define the Risk Criteria

Risk criteria are used to evaluate the significance of risk and are reflective of Council's values, objectives and resources and the views of its stakeholders. Council's risk criteria are documented throughout this framework and its appendices. It should be noted that, whilst risk criteria are established at the beginning of the risk management process, they are dynamic and should be continually reviewed and amended, if necessary.

5. RISK ASSESSMENT

5.1 Risk Identification

The aim of risk identification is to develop an inclusive list of events that may occur which – if they do – are likely to have an impact on the achievement of Council's objectives as stated in its Strategic Management Plans. Council identifies, assesses and treats risk in the following **three** groups:

Strategic	Risks associated with *high level* goals that align to Councils Strategic, Annual and Business Plans. Strategic risks may affect the achievement of Council's corporate objectives They are key issues for the management and impinge on the whole business rather than a business unit. These risks can be triggered from within the business or externally.
Operational	Risks associated with departmental functions and daily operations to deliver essential services. Often the risks are cost overruns, supply chain logistic issues, employee issues, fraud, WHS, non-compliance to policies and procedures.
Project	Risks associated with project management - that will affect milestones connected to delivering a specific project.

Risk identification naturally flows on from the context discussion and is a process of formally documenting the effects of uncertainty on objectives.

Each objective can be compared to the risk categories and highlight any potential uncertainty. A best practice approach to this is to engage as many stakeholders as possible in a structured identification exercise via, for example, brainstorming sessions. The aim is to generate a list of risks based on those impacts or events. It is important to identify risks with not pursuing an opportunity. All significant causes and consequences should be considered.

The process of risk identification must be comprehensive. Care must be taken to identify and define risks rather than causes or consequences.

After a risk is identified, it may be categorized and captured in the Risk Register in accordance with the following categories.

Category	Description
Asset / Infrastructure	This includes condition management, renewal, replacement and planning in relation to assets.
Budget / Financial	This includes cash flow, budgetary requirements, tax obligations, creditor and debtor management, remuneration and other general account management issues.
Community / Reputation	Associated with meeting the needs and expectations of the community
Environment	This includes risk arising from management of the environment and environmental consequences of the Council's activities.
Human Resources	This includes the recruitment, retention and remuneration of employees and volunteers and planning associated with these.
Legal / Legislation/ Compliance	This category includes compliance with legal requirements such as acts, regulations, standards, codes of practice and contractual requirements. This also extends to include compliance with Internal policies, procedures et. Including meeting Council's stated commitments,
Project	This includes the management of equipment, finances, resources, technology, timeframes and human resources associated with the project, internal or external to the organisation.

Safety (Including WHS)	This includes the safety of everyone associated with the Council. This extends from individual safety, to workplace safety, public safety and to the safety and appropriateness of services delivered by the Council.
Information Technology	This includes implementation, management, maintenance and upgrades associated with information technology.

5.2 Risk Analysis

Risk analysis involves developing an understanding of a risk. It provides an input to risk evaluation and to decisions on whether risks need to be treated, and the most appropriate risk treatment strategies and methods. The tables included in the appendix are Council's tools for expressing the Likelihood, Consequence and Level of risk as well as Council's risk tolerance.

5.3 Inherent and Residual Risk

A "risk rating" can be determined by combining the estimates of effect (consequence rating) and cause (likelihood rating). The risks are to be assessed against all consequence categories; and the highest consequence rating will be used.

The first rating obtained will be the inherent risk rating, (i.e. the level of risk at time of risk assessment with no controls.) Once further and additional controls are added to reduce the consequence and/or likelihood, the risk is rated again to determine the residual risk, (i.e. the level of risk remaining after risk treatment.

5.4 Risk Appetite

The Management Team, in consultation with Council Members, are responsible for defining Council's risk appetite, taking into consideration the nature and extent of the risks Council is willing to take in order to achieve its strategic objectives.

The following questions have been considered in arriving at Council's position for its risk appetite:

a) Do decision makers understand the degree to which they are permitted to expose Council to the consequences of an event or situation?

b) Does the Management Team understand their aggregated and interlinked level of risk to determine whether it is acceptable or not?

c) Are Council and Management Team clear that risk appetite is not constant? (i.e. there must be flexibility to adapt to changing environment and circumstances).)

d) Are risk decisions made with full consideration of reward? The appetite needs to help Council and the Management Team take appropriate level of risk for Council, given the potential for reward.

Council's risk appetite will be included in Council's regular monitoring and review process of this Risk Framework. This review of appetite will be incorporated into the structure of Council at each level of responsibility due, in part, to the differing focuses with regards to the risks that Council faces at each of these levels.

5.5 Risk Tolerance

Not all risk types for Council are the same in terms of their acceptability. Once a risk has been analysed it needs to be compared to Councils tolerance levels. Risk tolerance can be described as the boundaries of risk taking outside of which the organisation is not willing to accept in order to achieve its objectives.

The following statements are a guide to Council's tolerance of risk for its defined risk categories.

Category	Acceptance/Non-Acceptance
Asset / Infrastructure	• There is no acceptance of operational decision making that does not have a sound basis or unreasonably transfers the burden of asset management to future generations.
Budget / Financial	• There is no acceptance of decisions that have a significant negative impact on Council's long term financial sustainability.

Category	Acceptance/Non-Acceptance
Customer Relations / Community / Reputation	• There is unqualified acceptance for improvements to service to service delivery or efficiency of Council operations. • There is no acceptance for damage to the reputation of Council. • No 'justifiable' adverse media coverage is acceptable.
Environment	• Decisions that promote ecologically sustainable development are a high priority. • There is no acceptance of decisions that cause environmental harm requiring remediation or irreversible damage.
Human Resources	• There is no acceptance for the preventable loss of valued staff due to unreasonable management action.
Legal/ Legislation/ Compliance	• There is no acceptance of any non-compliance with legal, professional and regulatory requirements.
Project	• There is no acceptance of project plans with objectives that have a low level of certainty.
Safety	• There is no acceptance for compromising workers' health and safety • There is no acceptance of knowingly compromising the safety of members of the public
Information Technology	• There is no acceptance for privacy breech, or a reduction in cyber security

5.6 Risk Evaluation:

Risk Evaluation is the process used to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organisation that benefits from the risk. There are also circumstances whereby, despite the risk level, risks cannot be treated.

RISK LEVEL	MANAGING RISK – PRIORITY RATING

EXTREME	• Add risk to Council's Risk Register
	• Escalate risk issue immediately to CEO
	• CEO / Management Team to:
	  o Refer risk to risk owner
	  o Identify and develop treatment strategies for immediate action
	  o Monitor and review actions/strategies
	  o Provide direction and information to relevant stakeholders
	  o Inform the next meeting of the Audit & Risk Committee of the risk issue, the actions taken to mitigate the risk and the outcome (current status)
	• Consider cessation / suspension of the activity giving rise to the risk until such time as CEO / Management authorises its continuation and / or whilst other risks treatments are being developed / implemented

HIGH	• Add risk to Council's Risk Register
	• Escalate risk issue to Management/Risk Management area
	• Management to:
	  o Refer to relevant risk owner
	  o Identify and develop treatment strategies with appropriate timeframes
	  o Monitor and review actions/strategies to manage risk to an acceptable level
	  o Provide direction and information to relevant stakeholders
	  o Inform the next meeting of the Audit & Risk Committee of the risk issue, the actions taken to mitigate the risk and the outcome (current status)

MEDIUM	• Add risk to Council's Risk Register • Manage within Department. o Identify and develop treatment strategies (if

	required) o Monitor and review actions/strategies to manage risk to an acceptable level
LOW	• Add risk to Council's Risk Register • Undertake localised risk management & actions (if required) • Review within the Department parameters and routine procedures

5.7 Risk Treatment:

Risk treatment can be conducted using a variety of methods. When looking at negative risks, treatments are aimed at reducing or removing the potential for consequences occurring. However when looking at positive risks (opportunities), treatments look at ensuring that consequences are realised

Risk treatment involves selecting one or more options for modifying either the likelihood or consequence of risks , and implementing those options. Once implemented, treatments provide or modify the controls. An action (s) should be implemented to treat certain risks.

Justifications for risk treatment is broader than solely economic considerations and should take into account all of Councils obligations, volunteer commitments and stakeholder views. Appropriate risk treatment options should have regard to Council's objectives, risk criteria and available resources.

Council will tolerate a level of risk, in accordance with the risk tolerances set out in section 4.8. Any risk that is rated above a tolerable level of risk should be escalated to the appropriate level as set out in 4.9 to have treatment plan put in place.

Risk treatment options are not necessarily mutually exclusive in all circumstances. Options may include:

Eliminate	Remove the asset or service completely so as to eliminate the risk altogether.
Transfer	Allocate risk to a third party, such as through the purchase of insurance/ appropriate contactor management etc.
Mitigate	Implement a type of treatment control to reduce or remove the risk. This may include but is not limited to options such as substitution (swapping), isolation (barricade), engineering (modify by design) or administration (policy/process).
Accept	Risk can be accepted for a number of reasons including: • No extra treatments are available, • Meets the stated target for the type of risk, • Informed decision has been made about that risk, and • Risk treatment is worth more that the risk exposure.

Risk treatments need to be designed in a manner to ensure they are sufficient to mitigate that risk, and have some of the following characteristics if they are to become an adequate control:

a) Documented (eg Policies, procedures, task lists, checklists)

b) Systems-oriented (eg integrated and/or automated)

c) Preventative (eg system controls)

d) Consistent and regular (including during staff absence)

e) Performed by competent and trained individuals

f) Clear responsibility and accountability

g) Create value (ie benefits outweigh costs)

h) Achievable for the organisation (based on available resources)

i) Evidenced

j) Confirmed independently

5.8 Monitor and Review:

The risk management process is not static; by ensuring risks are monitored and reviewed, any changes in risks through the process and after its completion can be recorded. Due to the dynamic nature of most projects, a risk may change over the lifecycle of the management process. The monitor and review process allows for validation of risks to ensure that they remain relevant.

Monitoring and Review must be a formal part of the risk management process and involves regular checking or surveillance. It is essential to monitor all procedures in order to capture any new risks arising from changing business environment and review risk mitigation strategies.

A monitoring and review process will:

- Ensure that implemented controls are effective;
- Provide further information to improve risk assessment;
- Allow for the identification of emerging risks;

- Monitor any (new) activities that may influence established strategies to mitigate risks.

6. RISK REGISTER

Ultimately, recording risks in a central register allows the Management Team to determine the Clare & Gilbert Valley Council risk profile and provide direction on how to improve our risk management. Using the approach outlined in this framework, the risk management process for opportunities should result in an increasing trend in the potential for success and less risk with negative consequences.

The Risk Register enables Council to document, manage, monitor and review strategic, project and operational risk information. The Register also provides the opportunity to monitor and review risks in alignment with various plans

6.1 Strategic Risks

Council will identify and record strategic risks on the central Risk Register this will address risks associated with their Strategic outcomes and strategies. Strategic level risks are identified by the Management Team and the Council, as part of an annual review at a minimum. Any risks identified at the strategic level may be reflected in other Corporate Documents eg Strategic Plan, Asset Management Plan, Long Term Financial Plan and Annual Business Plans and mitigated through action details in these documents. Recording and reporting of strategic level risks is the responsibility of the Director Corporate Services via Management and Audit & Risk Committee.

6.2 Operational Risks

Council will record and maintain all operational risks on the central-register which is reviewed annually by the Management Team. This register allows all Council personnel to record their risks and track them effectively. The Risk Register will incorporate departmental risks and proposed mitigation techniques once determined by the evaluation process.

A number of operational risks are identified through the business planning

process. These risks are ones posed directly to a department area and its operations or processes. Recording in the register and reporting of operational level risks is the responsibility of Department Directors and workers.

6.3 Project Risks

Project level risks can be identified by anyone at any time and are all stored within the central Risk Register. All project level risks are identified against specific projects undertaken by departments. Actions are identified during the business planning process, however can be added as and when necessary. Recording and reporting of project level risks rest with the identified Project Owner.

7. RISK REPORTING

Risk based reports will draw data from the Risk Register and provide monitoring and profile information to Council, Audit & Risk Committee and Management in order to:

- Understand the risk exposure of Council
- Identify the risks that require increased attention and action
- Provide risk information to Council especially anything effecting the Strategic Plan
- Provide information to all workers at all levels to make risk informed decisions and
- Improve the Risk Management awareness and culture of Council

Risk reporting will include:

Report Content	**Report to**	**Frequency**
Council reports to include discussion of potential risk, based on completed risk assessments and treatments (with the exception of routine administrative matters)	Council Members	All Council meetings
Review and update of the Risk Register by Management	Management Team	Monthly to Management team meetings (or as otherwise required)

Report by CEO on Extreme and High Risks including controls taken to mitigate the risk and outcomes of current status	Audit & Risk Committee	Each meeting
Review Risk Management Policy	Audit & Risk Committee / Council	Every 4 years or as determined

7. TRAINING

7.1 Workers

This Framework and supporting policies will be made available to all workers through the extranet.

Council's Training Needs Analysis (TNA) is a tool used to:

a) capture legislative training and/or licencing requirements, and

b) identify individual tasks within specific jobs and the core competencies required for the safe performance of those jobs.

Risk Management awareness training is captured on Councils TNA, to ensure the effective implementation of this Framework.

Risk Management should be viewed as an umbrella that is overarching across all Council functions, not as a specialist skill that is owned by a designated risk management position and, as such, Council considers it to be a skill and necessity that workers need to perform their day to day activities. Risk Management awareness training will be provided by Council to relevant workers and will take into consideration the role of the worker within the Risk Management Framework and the level of past risk management experience and knowledge.

7.2 Council Members

Council Members are key strategic decision makers and it is therefore imperative that they have an understanding of Council's Risk Management Policy and Framework and their role in informed decision making based on sound risk management principles.

Risk Management awareness training will be scheduled within 12 months of Council elections.

7.3 Audit & Risk Committee

Audit & Risk committee members should, at a minimum, have an understanding of their roles and responsibilities as outlined in Council's Risk Management Policy and Framework, including the monitoring and review of risk management reports and outcomes from management and external auditors.

8. APPENDICES

8.1 Definitions

Key Definitions	
Assurance:	A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk.
Consequence:	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Controls:	A measure that modifies risks and increases the likelihood that objectives and goals of an organisation will be achieved.
Enterprise Risk Management: (ERM)	ERM can be defined as the process affected by an organisation's board of directors (council members/Audit & Risk Committee for Councils), management and other personnel, applied in strategy setting and across the organisation, designed to identify potential events that may affect the entity, manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the organisation's objectives.
Establishing the Context:	Defining the external and internal parameters to be taken when managing risk.
Event:	Occurrence of a particular set of circumstances.
Exposure:	The risk exposure is a qualitative value of the sum of the consequence of an event multiplied by the likelihood of that event occurring.
Financial/Infrastructure Risk:	Risk relating to the organisation's financial sustainability or ability to provide or maintain services, structures and/or facilities.
Frequency:	A measure of the rate of occurrence of an event expressed as the number of occurrences of their event in a given time.
Inherent Risk:	Risk rating at time of risk assessment without existing/current controls.
Internal Audit:	An independent, objective assurance and consulting activity designed to add value and improve organisations operations. It helps the organisation to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.
IT (Information Technology) Risk:	Risks relating to loss, exploitation or ineffectiveness of the organisations hardware, software or systems, (including data retention and security).

Key Definitions	
Legal and compliance risk:	Risks relating to failure or inability to comply with legal or regulatory compliance.
Likelihood:	Chance of something happening.
Monitor:	To check, supervise, observe critically or record the progress of an activity, action or system on a regular basis in order to identify change.
Management Team	Executive employee those holding senior management level or directors
Operational Risks:	Risks associated with departmental functions and daily operations to deliver core services.
People Risks:	Risk to the organisation caused by its people, (e.g. relating to culture or behaviour,) or the risk of harming people, (whether employees or not).
Project Risks:	Risks associated with Project Management that may affect milestones or deliverables connected to a specific project.
Residual Risk:	Rating of the risk remaining after risk treatment or control has been applied.
Risk Analysis:	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk Appetite:	Is the amount of risk an organisation is prepared to accept or avoid. Broad-based description of the desired level of risk that an entity will take in pursuit of its mission.
Risk Assessment:	An overall process of risk identification, risk analysis and risk evaluation.
Risk Culture:	Risk culture refers to the behaviours that lead to how every person thinks about and manages risks,
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 Management:	Coordinated activities to direct and control an organisation with regard to risk.
Risk Management Framework:	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk Rating:	Risk priority based on consequence and likelihood assessments.
Risk Register:	Register of all identified risks, their consequences, likelihood, rating and treatments. It works well when it is a live document and the risks are reviewed on a periodic basis.
Risk Tolerance:	An organisation's or stakeholder's readiness to bear the risk after risk treatment/control has been applied in order to achieve its objectives. It also reflects the acceptable variation

Key Definitions	
	in outcomes related to specific performance measures linked to objectives the entity seeks to achieve.
Risk Treatment:	Risk treatment is a risk modification process - Usually the risk treatment means what are you going to do (modify) with the risk based on its residual risk rating, i.e. • Eliminate • Transfer • Mitigate • Accept
Risk:	An event or uncertainty that will stop a organistion to achieve its objectives.
Stakeholder:	Person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity.
Strategic risks:	Risks associated with *high level* strategic goals that align to Councils Strategic, Annual and Business Plans. Strategic risks may affect the achievement of Council's corporate objectives-They are key issues for the management and impinge on the whole business rather than a business unit. These risks can be triggered from within the business or externally. In other words they may stop the organisation from achieving its strategic goals.

8.2 Consequence Table

Level	Descriptor	Financial / Infrastructure	People	Reputation	Environmental	Legal / Regulatory / Policy	Service Delivery
1	**Insignificant**	**Negligible** Financial Loss **(> $20k)** & damage to infrastructure. No real disruption to business	No injury/first aid only. No impact on morale	No media or political attention. Some local complaints	Minor Instance of environmental damage. Can be reversed immediately	Immaterial legal, regulatory or internal policy failure. No penalty or liability	Insignificant interruption to a service – no impact to customers/business
2	**Minor**	**Minor** Financial Loss **($20k – 100k).** Minor damage to infrastructure. Minor financial disruption. Minor variation to budget for Financial Year	Minor Medical attention. Negligible impact on morale	Some Local Media or Political Attention. Community Concern – little adverse effect	Minor impact to environment. Can be reversed in the short term	Minor legal or regulatory/internal policy failure – resolved without penalty & minor liability exposure	Minor interruption to a service with minimal impact to customers/business
3	**Moderate**	**Moderate** Financial Loss **($100k - $400k**) and damage to infrastructure. Moderate impact to business operations. May impact beyond current financial period	Significant Injury requiring medical attention. Short Term effect on morale and business	Significant Media Attention. Significant Public interest. Potential for adverse local media or potential attention	Moderate impact to environment. Localised damage that has potential to spread and reversed with intensive efforts	A repeated legal, regulatory or internal policy failure. Resulting in a penalty and potential liability exposure	Moderate Interruption to service delivery. Customer impact up to 48 hrs. Partial BCP action may be needed

4	**Major**	**Major** Financial Loss **($400k - $1m)**. Major damage or loss of infrastructure. Major impact on Business Operations. Multiple financial year impact.	Serious Long Term Injury. Temporary disablement. Significant impact on morale and business	Regional or State wide media Attention. Public interest. Long term effect on reputation	Severe Loss of environmental amenity, Danger of continuing environmental damage.	Systematic legal, regulatory or internal policy failure. Major penalty requiring a full review. Significant liability exposure	Major interruption to service delivery, Customer impact > 7 days. Component of BCP action may be needed.
5	**Catastrophic**	**Significant Financial Loss (> $1m) Loss of Business Operation. Loss of significant infrastructure. Multiple Financial Year Impact**	Major Injury/disablement or death. Long term effect on morale and performance of business	Potential National Media attention. Prolonged Media or Political Attention. Irreparable damage to Reputation	Major loss of environmental amenity – irrecoverable environmental damage	Substantial failure in administrating legal, regulatory and policy requirements. Significant penalty and liability exposure	Major interruption to delivery of all or most services for more than 14 days. Full BCP action required.

8.3 Likelihood Table

Rating	Likelihood	Explanation
E	**Almost Certain**	Expected to occur at times of normal operations (daily - > 99% probability of occurrence)
D	**Very Likely**	Will occur at some stage based on previous incidents (once per month – 50-99% probability of occurrence)
C	**Possible**	Not expected to occur but could under specific circumstances (once per year 15-50% probability of occurrence)
B	**Unlikely**	Conceivable but not likely to occur under normal operations (once per 5 years – 1-15% probability of occurrence)
A	**Rare**	Only occurs in exceptional circumstances (once per decade - <1% probability of occurrence)

8.4 Risk Matrix

Consequence / Likelihood	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Significant
1. Almost Certain	High	High	Extreme	Extreme	Extreme
2 Very Likely	Medium	High	High	Extreme	Extreme
3. Possible	Low	Medium	High	Extreme	Extreme
4. Unlikely	Low	Low	Medium	High	Extreme
5 Rare	Low	Low	Medium	High	High