# Risk Management Framework

June 2022 (slightly modified version for Council website; 06.07.2022)

July-August 2022- UPDATE - for A&R Committee Review - AUGUST 2022

October-November – incorporation of A&R Committee feedback - NOV 2022

ADOPTED - following Council approval of updated Risk Management Policy - 14th November 2022

# Preamble

The Greater Dandenong City Council (Council, CGD, GDCC) recognises that sound management of risk is an essential part of our business management processes. Effective risk management contributes to the creation and protection of value for the City of Greater Dandenong.
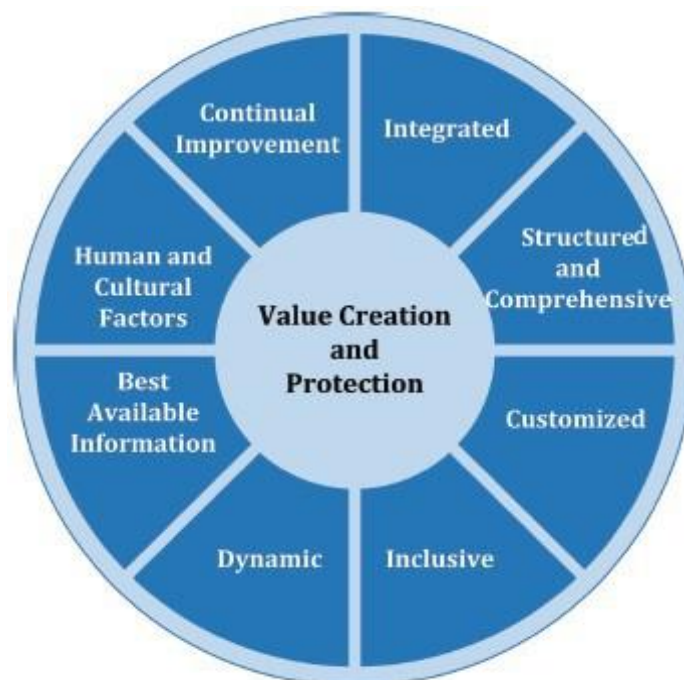
Through the Risk Management Policy, Council is committed to identifying and managing risks associated with the performance and delivery of municipal functions and services.

The purpose of this Risk Management Framework (RMF) document is to outline the key components of CGD's risk management system.

The risk management system is designed so that all operations of Council are performed within an approved risk appetite, and to promote the integration of risk management processes with planning, decision-making, budget allocation and every-day activities. This enables officers to consider the potential impact of all types of risks on all departmental processes, activities, and services, and includes "opportunity risk".

The RMF outlines the requirements and processes underpinning risk management practices across Council and is driven by a commitment to the REACH values - Respect, Engaged, Accountable, Creative, and Honest.

Council's RMF has been developed and implemented in accordance with the guidance provided in *ISO 31000:2018 Risk Management* to assist in the effective management of risk across Council.



*ISO 31000:2018 Risk Management*

# Contents

## Introduction

The *Risk Management Standard* ISO 31000:2018 states: *"the purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives."*

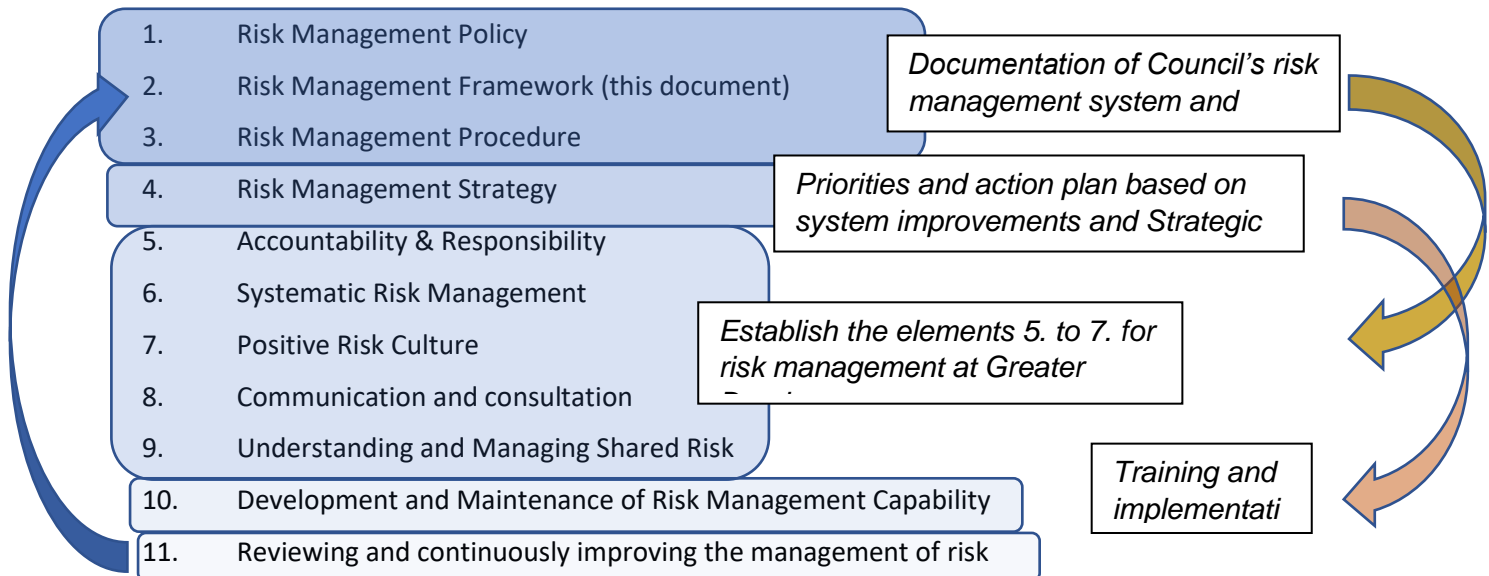This framework document outlines how risk and opportunities can be addressed effectively at GDCC to ensure:

1. Council and senior management can make informed business decisions based on sound risk assessments.

2. Risks are consistently identified, assessed and managed proactively in an effective and timely manner.

3. Strategic planning processes are improved because of robust and structured consideration of risk.

4. Opportunities that benefit the Council are identified and captured without exposing the CGD to unacceptable levels of risk.

5. Improved resident, community and stakeholder confidence and trust

6. Compliance with relevant legislation and conformance with good governance.

## Purpose of the Risk Management Framework

The Risk Management Framework is to document the risk management structure for Council, noting the necessary risk management elements.

This includes documentation, tools, systems and training, together with governance structures and mechanisms, that will serve as a guide to embed risk management in all decision-making across the organisation.

The RMF comprises the following documents and elements within Council's overall risk management system:

1. Risk Management Policy
2. Risk Management Framework (this document)
3. Risk Management Procedure

*Documentation of Council's risk management system and*

4. Risk Management Strategy

*Priorities and action plan based on system improvements and Strategic*

5. Accountability & Responsibility
6. Systematic Risk Management
7. Positive Risk Culture
8. Communication and consultation
9. Understanding and Managing Shared Risk

*Establish the elements 5. to 7. for risk management at Greater*

10. Development and Maintenance of Risk Management Capability
11. Reviewing and continuously improving the management of risk

*Training and implementati*

These elements are the principles for the development, implementation and continual improvement of the risk management system at the City of Greater Dandenong.

The Risk Management Framework refers to the relevant risk management artefacts of the risk management system, including:

- Risk Management Policy

- Risk Management Procedures

- Risk Appetite (within the Risk Management Procedures)
- an outline of the "Risk Toolkit", including:
  - o processes and procedures
  - o Forms and Templates
  - o other tools and Council systems (including software)
- Governance structures and mechanisms, including relevant stakeholders such as the Audit & Risk Committee (A&RC) and Internal Auditor
- internal escalation steps
- training arrangements and documentation

The Risk Management Framework also provides context for these artefacts and provides an order of precedence of documentation.

## Context

This section outlines the context and hierarchy of CGD's risk management artefacts and elements.

The key guiding document for risk management across the Council is the *Risk Management Policy*, supported by the *Risk Management Procedures* and *Risk Management Framework*. Additionally, a *Risk Management Strategy* (and action plan) documents the activities undertaken in support of, and to monitor and review, the risk management system.

This framework document provides a concise guide to Council's risk management artefacts, governance mechanisms, roles and responsibilities and reporting across the organisation.

The *Risk Management Framework* therefore documents how the identified risk management elements are integrated and linked, defining the approach, structures and mechanisms, processes, procedures and tools to guide risk management activities.

*Table 1: Risk Artefacts Description*

| Name of artefact | Description |
|---|---|
| Risk Management Framework ("RMF", "*Framework*") | The *Risk Management Framework* (this document) is a guide to establishing a central repository for risk management, containing references to all relevant risk management elements. These include all risk management documentation, tools, systems and training, together with governance structures and mechanisms, to assist with risk-based decision making across the COGD. The *Risk Management Framework* also provides a context in relation to these elements and, in doing so, provides an order of document precedence. |
| Risk Management Policy ("*Policy*") | A statement that defines the commitment, direction and intention of Council regarding Risk Management. The policy states the organisation's risk management objectives, providing a high-level synopsis of the roles and responsibilities for risk management This is a document distinct from the RMF, the *Risk Management Policy* |

| | |
|---|---|
| Risk Management Procedures<br><br>("*Procedures*") | A document outlining the application of the risk management process as outlined in the *Risk Management Standard* ISO 31000:2018.<br><br>The details and requirements of the risk management process at Council are provided in the *Risk Management Procedures* and *not* included in detail in this *Risk Management Framework* |
| Risk Appetite | A statement defining the types and amount of risk that Council is prepared to undertake in alignment with the *Risk Management Policy*.<br><br>This is detailed in the *Risk Management Procedures* and *not* included in detail in this *Risk Management Framework*. |
| Risk Governance | Structures, mechanisms, reporting and guidelines that provide accurate oversight of risk management at Council. |
| Processes | Defined set of activities to be followed systematically to achieve effective risk management across Council. |
| Procedures | Established methods of accomplishing a consistent result, defined as a sequence of steps that will be used to execute a process. |
| Work Instruction | General set of instructions created to help with the execution of risk management at Council. These can exist at any level of the organisation. |
| Templates | Documents in a pre-determined format that provide a defined structure for collection, organisation and/or presentation of information and data. These can be modified, with approval. |
| Forms | Like a template but used without modification e.g., an Annual Leave form. |
| Software Systems | Computer- or device-based systems (software) used for risk management across the organisation. |
| Risk Management Strategy (and action plan)<br><br>("*Strategy*") | Document detailing the activities undertaken in support of, and to monitor and review, the risk management system as part of the *Risk Management Framework*. The action plan identifies target dates, expected outcomes and resources. |

The pre-eminent Risk Management document at Council is the *Risk Management Policy.* This has been developed as a separate document and provides high-level commitment to, and the general approach for risk management at Council.

Underpinning the *Risk Management Policy* is the framework (RMF) document. The RMF cites the other relevant artefacts and establishes how they operate together. The *Policy* is supported and enacted through the application of the *Risk Management Procedures*, including the *Risk Appetite Statement*.

The Procedures provide details of many of the items that form the "*Risk Toolkit*", such as relevant Procedures, Templates, Software Systems, etc.

The *Risk Management Strategy* (and action plan) is a separate document. It includes objectives for ensuring the implementation monitoring and review of the risk management system, and to equip officers at staff to effectively manage risk. It typically identified actions across multiple years, with target dates and expected

outcomes. It also identifies the resources required to complete those activities.

The *Risk Management Artefacts Hierarchy* is the structure for describing and ordering all the risk artefacts at Council. The benefits of establishing an order of precedence to the documents are manifold, namely:

- clarity is provided regarding how these artefacts should be consulted and used

- consistency is created; and

- conflict is avoided to the extent that if any document lower in the hierarchy is inconsistent with a higher document, the higher document prevails.

As per *Figure 1: Risk Management Artefacts Hierarchy Diagram*, the *Risk Management Policy* establishes an overarching philosophy for and commitment to risk management, and reflects (with reference to the *Risk Appetite Statement*) a low appetite for risk.

The *Risk Management Procedures* give detailed instruction and information to allow the application of the *Risk Management Standard* ISO 31000:2018 at the City of Greater Dandenong.

The implementation of the *Procedures* is through the various Toolkit elements, both those provided in the *Procedures* and those that exist outside of them.

The *Risk Management Framework* summarises this hierarchy and the overall implementation of risk management at Council.



*Figure 1: Risk Management Artefacts Hierarchy Diagram*

Appendix B provides a Risk Defence and Governance Model for risk management at Council. This structure provides for continuous improvement and assurance for Council's risk management system.

# Element 1 - Risk Management Policy

## Objective

The purpose of this element is to provide a high-level commitment upon which CGD's risk management system is established.

The risk management policy sets out the overall objectives of Council's risk management and its approach and commitment to sound and effective management of risk.

## Policy Statement

The primary objective of the *Risk Management Policy* is the establishment of a risk management framework and system, and to couple the risk management approach to the achievement of Council's objectives and strategic priorities.

The *Policy* outlines the scope of application of risk management at the City of Greater Dandenong, and the key aspects of risk management and roles and responsibilities.

# Element 2 - Risk Management Process

## Objective

The management of risk should be aligned with the steps provided in the *Risk Management Standard* ISO 31000:2018 and is a reiterative process. The objective of this element is to ensure that procedures are in place to identify and assess risks in a consistent manner.

## Risk Management Process

Risk Management involves the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk (as per ISO 31000:2018).

The key steps outlined in ISO 31000:2018 are illustrated below. The *Risk Management Procedures* provide detailed explanation of how the stages are conducted at CGD.
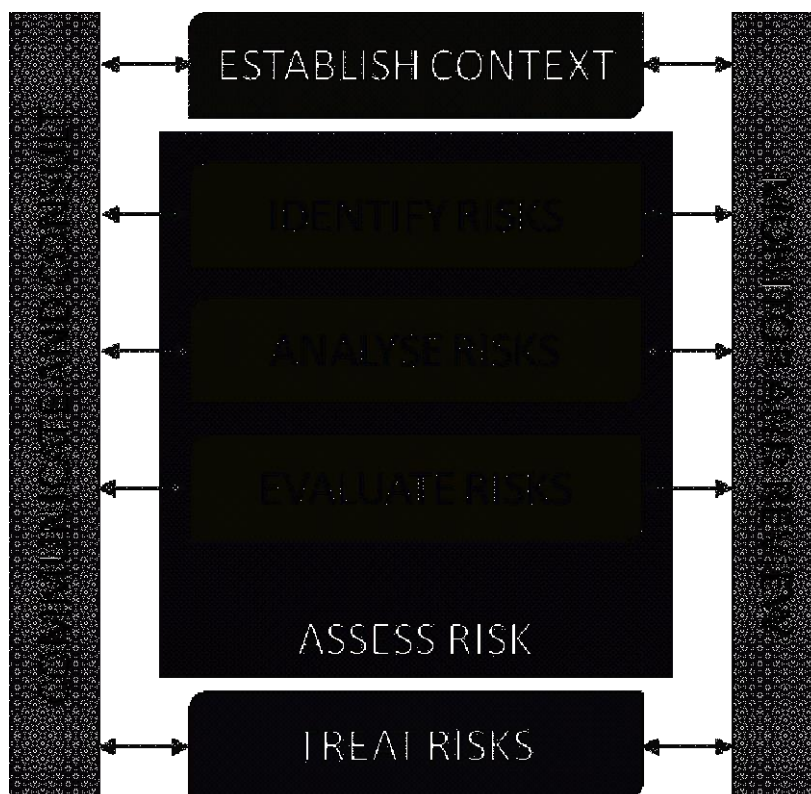
## Risk Appetite

Risk Appetite is a statement of the level of risk that an organisation is prepared to accept in pursuit of its objectives before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of innovation and the threats, that change inevitably brings.

The *Risk Management Procedures* incorporate Council's Risk Appetite and is interpreted and applied in the context of Council's priorities, resources, and capabilities.  Risk appetite constantly evolves and involves weighing up of opportunities (positive risk) with threats (negative risk).

As defined in the *Policy*, there is a generally low appetite for risk, to minimise the negative impacts on stated objectives, but will accept a degree of risk commensurate with both the potential reward and with CGD's role in the community.

Establishing a Risk Appetite provides a foundation and sets the tone of the desired risk culture at Council.

# Element 4 - Risk Management Strategy

## Objective

The objective of the Risk Management Strategy is to identify and record actions to supplement and improve the risk management system and the application of the *Policy* and *Procedures*

The *Strategy* (and action plan) aims to improve risk management skills and capability, to establish risk management as an integral and essential part of good management, corporate governance, and decision-making.  The outcome of such actions is to embed risk management as a part of Council's overall management system, rather than operating as a stand-alone process.

The *Risk Management Strategy* is regularly updated, and usually operates across multiple years, establishing target dates and expected outcomes, and identifying the resources required to complete those activities.

# Element 5 - Risk Management Framework (RMF)

## Objective

The RMF is a summary of the key features of Council's risk management system, documenting the risk management structure and the necessary risk management elements.

This *Framework* also discusses other elements, some in place and some aspirational elements, that have or will become inherent in Council's maturing risk management system (see *Other elements that support the Risk Management system…, below).*

## Risk Management Framework

The *Framework* is illustrated in Diagram 1, *above*.  It reflects the hierarchy of the documents discussed here, and shows the "why, what and how" of the risk management system, and highlights the important role of CGD's overall governance structure, and communications and training activities.

## Principles

Risk Management is integral to all decision-making processes.  CGD endeavours to embed Risk Management into all facets of service delivery, including Strategic and Operational Planning, Projects, Change Management and Reporting to ensure that risks are considered by all.

# Other elements that support the Risk Management system, *Policy*, *Procedures*, *Risk Appetite*, *Strategy* and *Framework*

## A) Risk Defence and Governance Structure

Appendix B illustrates the lines of defence and governance structure for risk management at Council.  This structure provides for continuous improvement and assurance for the risk management system.

## B) Business Planning

Business planning is undertaken to place customers and the desired community outcomes at the centre of Council's organisational planning.  Business Plans are developed for each Council Department and the corresponding service activities are documented.

For each of the service activities, owners are required to document the challenges (risks) and opportunities to achieving these service activities.  Within business planning, operational and strategic risks for the services are required to be documented.  Business planning is maintained in a dedicated module in the Pulse database.

## C) Independence of the Corporate Risk Management Team

The Risk Management Team provides an independent view of the organisation through the lens of risk management.  The team observes the organisation holistically, whilst also examining the interrelationships of its various components.  This is with the aim of identifying early signals of emerging threats that arise out of the inter-relationship of various organisational components, and the internal and external environments of Council's operations.

With this viewpoint, the team is charged with embedding risk management throughout the organisation, and CGD's management systems, processes, and practices.  Ideally, a consistent approach means that decisions and risk management operate in a similar manner at corporate, local, and cross-functional levels, and information is shared amongst stakeholders to further inform decision-making.

## D) A positive risk culture

## Objective

A positive risk culture helps to ensure that:

- – risk management is driven by active and visible leadership at all levels of the organisational structure, with demonstrated commitment from top management

- – staff are aware of the organisation's commitment to risk management, and know what is required of them when undertaking their roles

- – people are motivated to comply with the roles, responsibilities, processes, and outcomes of the risk management system

- – all staff, including contractors and volunteers, take responsibility for identifying and assessing risks as part of their service delivery requirements

- – similar practices are undertaken in relation to Safety, Health and Wellbeing, where there are also specific, legislative risk management requirements (refer to the *Occupational Health & Safety Policy*)

## E) Creating the impetus and sustaining the momentum

Culture is a localised phenomenon, and whilst an overall "corporate culture may exist", there can be variations in values, beliefs and assumptions at the individual, team, and group levels. Risk management communication and consultation must be undertaken at the local level.

Whilst culture at local level is most influential on individual and team performance, a positive organisational culture is driven by top management setting the tone for the organisation's attitudes, behaviours, and underlying assumptions for risk and risk management.

When the local government risk culture analysis tool being developed by Macquarie University's Department of Applied Finance is available, its application at CGD will be considered, and may form part of the next update to the *Strategy*. This tool is designed to provide a better understanding of risk culture at local levels and may help identify further improvements for the risk management system.

## F) Communicating and Consulting About Risk
### Objective

The objective of communication and consulting about risk is to ensure that all staff are provided with up-to-date information about current and emerging risks. Regular communication also promotes involvement in the management of risk, identifying risk management system improvements, and provides opportunities for users of the system to advise where there may be gaps or inefficiencies.

When staff are consulted and feel heard during decision making, it provides them with increased ownership and personal accountability for the decision that has made. Quality consultation with staff is essential for establishing a positive risk culture.

## G) Building strong communication and consultation channels

The *Policy* and *Procedures*, supported by this *Framework* reflects the promotion of risk management as an essential way of advancing the risk culture in the workplace, and reinforcing the concept that risk and management are inseparable. It also highlights that risk can be negative (threats) and positive (opportunities) and is essential to good decision making.

Promotional programs continue to be developed, with the aim to demonstrate a clear commitment to the establishment and maintenance of a sustainable and "risk aware" culture.

## H) Understanding and Managing Shared Risk
### Objective

The objective of understanding and managing shared risk is to ensure that risks that are shared across business units, or between Council and other stakeholders are identified, understood, and managed appropriately.

## I) Developing and Maintaining Risk Management Capability
### Objective

The objective of risk management capability development is to ensure all staff have the relevant knowledge, skills, experience, and resources available to make good decisions. Risk management capability is relative to individual roles and decision-making responsibilities.

## J) Capability Development Programs

Such programs include:

- Defining education and training requirements for effective risk management, including competency requirements (as part of the wider competency framework being developed).

- Designing education programs and training tools to impart the required knowledge.

- Tracking the progress and effectiveness of education and training in risk management.

- Defining and implementing development opportunities for staff (i.e., education and training that extends beyond their role requirements) to optimise risk management across the organisation.

## K) Induction of new employees

Risk Management is included as part of the Corporate Induction for all new staff, supervisors, managers and directors.  This training is conducted by the Risk Management Consultant, as required.

## L) Training in relation to Risk Management

Risk Management training will be provided in accordance with the Training and Development Program, and as identified in Position Descriptions and Personal Development Plans.  Risk Management is an embedded topic in other training such as Project Management training, Procurement training, and Occupational Health and Safety training.

There is ongoing professional development for the Risk Management Team members is provided, to ensure that these officers' knowledge and skills remain current, and to demonstrate that their role is strongly supported.

## M) Reviewing and Continually Improving the Management of Risk

## Objective

An annual self-assessment, audit, and review process is an aspirational goal, as part of maturing CGD's risk management system.  This would assess, amongst other elements:

- the extent to which the *Policy* and *Procedures* are implemented against the Risk Management Capability Maturity Model (*see below*)
- the degree of compliance with *Policy* and *Procedures* by Line Management and staff
- areas in which improvements are feasible
- whether previously-identified improvements and/or actions under the *Strategy* have been implemented; and
- the effectiveness of the Risk Management system at CGD.

## N) Risk Management Capability Maturity Assessment

The Council will continue to mature its risk management capability through ongoing integration of risk management into the organisational processes.  The degree of increasing maturity will be measured against the Risk Management Capability Maturity Model (Attachment 1).

Actions identified to move any component further along the maturity continuum will form part of the *Risk Management Strategy*'s action plan.

The Risk Management Capability Maturity Model contains an assessment of the overall maturity attributes.

| Fundamental | Developed | Systematic | Integrated | Advanced | Optimal |
|---|---|---|---|---|---|
| • Risk management policy and framework have been endorsed by the accountable authority, however the framework has not been integrated with operations and broader governance<br>• Inconsistent appetite for risk across the entity<br>• Absence of common risk language<br>• Communication and understanding of risk may not be widely understood<br>• Ad-hoc processes to discuss and understand shared risks<br>• Limited and/or shared resources allocated to manage risk. | • Risk management policy and framework have been communicated and implemented across the entity<br>• A common risk language is used, however not consistently understood<br>• Risk management policy defines shared risk. Informal processes are in place to discuss shared risk<br>• Accountable authority instructions and risk management policy articulate responsibilities and accountabilities for risk management, however these are shared with other responsibilities. | • Risk management framework is fully embedded<br>• Risk appetite statement is high-level and qualitative<br>• A common understanding of the importance of managing risk exists<br>• Formal arrangements exist for to discuss and understand shared risk<br>• Accountability and responsibility for managing risk is clearly defined within the overarching governance framework<br>• Dedicated staff are responsible for implementing the risk management framework. | • Risk management framework is part of the overarching governance and management framework<br>• Risk appetite statement contains both quantitative and qualitative elements which are linked to strategy and communicated to all staff<br>• The risk management program is reviewed regularly to identify improvement opportunities and assess the level of investment in risk management activities<br>• Risk information and data is stored in a readily accessible central repository. | • Risk management policy is integrated with strategic and business planning processes and reviewed and updated annually (or as changes arise)<br>• Formal arrangements facilitate identification of current, future, emerging and shared risks. These are clearly articulated across the entity<br>• A senior executive sponsor leads, promotes and drives risk management capability<br>• The risk management framework includes measures for the accountability and management of risk controls at business unit and program levels. | • Risk management policy considers management of risk as an integral part of the entity's governance system<br>• Risk appetite statement, including tolerances and limits for risk categories are used consistently to inform decision making<br>• Governance framework facilitates recording, monitoring and reporting on shared risk<br>• Performance reporting identifies examples of good risk management practices, which are communicated and rewarded<br>• Real-time risk information is readily available and used to identify, analyse and measure risks & trends<br>• Costs of risk management activities are managed within the operational budget. Risk resources are allocated based on informed analysis. |

The Maturity Model includes an assessment of the following elements:

1. Establishing a risk management policy
2. Establishing a risk management framework
3. Defining responsibility for managing risk
4. Embedding systematic risk management into business processes
5. Developing a positive risk culture
6. Communicating and consulting about risk
7. Understanding and managing shared risk
8. Maintaining risk management capability
9. Reviewing and continuously improving the management of risk

The model is used to assist Council to determine both its current state of risk management maturity and the aspirational state of maturity or capability (target state) to support its operations and the achieving objectives. Establishing a target maturity state is designed to drive future investment in risk management capabilities.

## O) Audit schedule

Council has an annual Internal Audit schedule, determined by the EMT and A&RC. Assurance mapping is undertaken by Internal Audit annually to understand the assurance mechanisms used by Council to monitor and evaluate the Strategic risks. Some risks arising from Operational, Project or other activities- if rated as Extreme, or considered intolerable, for example - are also subject to review at this level  This helps improve the understanding of risk treatment effectiveness.

## P) RMF Review

The Manager People, Culture & Innovation will perform a review of the risk management system every two years, to incorporate changes within Council, key learnings, Risk Management better practice and any changes in the Risk Management Standard.

In addition, a review of the adequacy of the risk management system and its alignment with better practice may be conducted by an external provider (ideally, every three years). This may be through Internal Audit or an appropriate consultant outside the Internal Audit programme, depending on the allocation of resources.

## Q) Self-assessment, Audit and Review Reporting

Outcomes of the internal or external review of the RMF, and the relevant recommendations are considered by EMT for action and endorsed by the A&RC. Internal Audit findings are recorded, monitored and reported upon through the *RelianSys* compliance database (managed by Governance).

## Appendix A - Risk Management Capability Maturity Model

| | Fundamental | Developed | Systematic | Integrated | Advanced | Optimal |
|---|---|---|---|---|---|---|
| **Element 1:** Establishing a risk management policy | • A Risk management policy (policy) has been endorsed by the accountable authority <br>• The Policy defines the approach and rationale for managing risk <br>• Communication and understanding of the policy varies <br>• Understanding of the entity's appetite for risk is inconsistent. | • The Policy has been communicated throughout the entity <br>• An innate understanding of risk appetite by senior executives is implied in risk documentation, in particular its consequence and likelihood tables. | • The Policy outlines the required accountability and responsibility for managing risk <br>• A common definition of risk exists and is applied throughout the entity <br>• Risk appetite statement is high-level and qualitative. | • The Policy includes a vision for the continuing development of its risk management program <br>• The Policy contains a high-level risk appetite statement with both qualitative and quantitative elements, linked to business strategies <br>• The Policy is reviewed and updated to reflect changes in the operating environment as they occur. | • The Policy defines linkages between risk and strategy <br>• The Policy is reviewed and updated on an annual basis or more regularly if needed <br>• Risk appetite statements for each source or category of risk exists and include measures that enable effective monitoring and review. | • The Policy considers the management of risk as an integral part of the governance system, reflecting the link between risk and realising strategic objectives <br>• The Policy contains information for all staff and stakeholders on resources and processes dedicated to the management of risk. |
| **Element 2:** Establishing a risk management framework | • The risk management framework (framework) is articulated at a high level, but not integrated with the operations and overarching governance practices <br>• Resources allocated to manage risk are limited and often shared across other responsibilities <br>• The Framework and systems used to manage risk may not be widely understood or practiced. | • The Framework articulates the risk management methodology and processes required to manage risk <br>• The effectiveness of the framework is reviewed on an ad-hoc or informal basis. | The Framework: <br>• Has been implemented and supports a consistent approach to risk identification, assessment, evaluation and treatment <br>• Has annually reviewed performance measures <br>• Has resources allocated to implement, monitor and review <br>• Explains requirements for reporting the status of key risks including managing shared risk. | • The Framework is embedded in the operations of the entity and is part of its overarching governance and management framework <br>• Techniques for identification, assessment, evaluation and treatment of risk are applied consistently across all business units <br>• Reporting on the status of key risks and control performance including effectiveness of the framework occurs quarterly. | • The Framework includes measures for accountability and management of risk and controls at business unit and program/project levels <br>• Key risk indicators measure the overall performance of the framework <br>• Tools exist to guide decision making and support regular risk reporting and escalation <br>• Risk management data is centrally stored and accessible. | • Techniques exist to identify, analyse and measure current, future and emerging risks <br>• Centralised real-time risk information is readily available <br>• Risk appetite informs risk related discussions <br>• Performance reporting measures and monitors risk exposures <br>• Information flows effectively as a result of no duplication of effort in risk roles. |
| **Element 3:** Defining responsibility for managing risk | • Responsibility for the management of risk has been articulated in the accountable authority instructions. | • The Risk Management Policy articulates who is accountable and responsible for the management of risk, and the implementation of the framework <br>• The Management of risk is not specified in individual's performance agreements. | • A dedicated risk manager or team is responsible for implementing the framework <br>• Accountability and responsibility for managing risk is clearly defined and linked to staff performance <br>• Accountability and responsibility for managing, or oversighting risk is included in the charters of executive committees or audit and/or risk committee. | • Formalised governance structures assess and oversee risk management at business unit and executive levels <br>• Formal governance structures assess the risks associated with the development or implementation of new policies/programs/services. <br>• The Risk manager or team coordinates the implementation of the framework, risk profiles and action plans. | • Senior leadership supports the risk manager or team to facilitate, challenge and drive capability <br>• The Risk management team regularly report to senior executive, the audit committee or the accountable authority on the performance of the framework <br>• Executives approve the entity's risk appetite and oversee the continual improvement of the framework. | • Managers and supervisors monitor the risks and risk profiles of their areas of responsibility and ensure staff adopt the framework as developed and intended. |
| **Element 4:** Embedding systematic risk management into business processes | • Branch and business unit risks are reviewed annually, however do not inform business planning, budgeting and reporting <br>• Risk definitions are inconsistently understood as there is limited guidance for identifying risk processes or differentiating between risk classes. | • Enterprise-wide risks are considered in business planning, budgeting and reporting processes <br>• There is No evidence of the identification of specialist categories of risk, such as fraud, or business continuity in these processes. | • Framework is embedded in operational, process and reporting frameworks <br>• Managing risk is part of the overarching governance framework and recognised as key to effective business planning <br>• Risk identification, assessment, monitoring, communicating and reporting processes are consistent <br>• Risk profile enables the prioritisation of audit and assurance activities. | • Risk management occurs at policy, program and/or service delivery level <br>• Risk appetite has been defined and communicated to facilitate strategic and operational planning Specialist risk programs are documented and included in regular reporting to senior executive and/or the accountable authority. | • The Entity's approach to managing risk is fully integrated with the overarching governance framework and recognised as key to effective business planning <br>• Opportunities for improvement and good practice are identified through analysing risk information <br>• A consistent set of risk appetite and tolerance statements, including KPI's, that cascade from high level down to detailed exist. | • Risk management processes are utilised at enterprise, business unit, program and project levels for all risk activities <br>• Formal mechanisms exist to build and maintain organisational resilience <br>• Risk appetite statements, including tolerance and limits are used consistently across the entity to inform decision making. |
| **Element 5:** Developing a positive risk culture | • Officials understand and agree on the need and value of effective risk management <br>• Senior executives and line managers demonstrate the importance of managing risk in line with the framework and systems. | • The Framework is integral to the entity's operating model <br>• Lessons learned are communicated to staff <br>• A Common understanding of the meaning of good risk management results in a consistent use of language and understanding of risk related concepts. | • Surveys and external reviews undertaken are analysed to provide insights into the entity's risk culture <br>• Loss incidents are analysed and areas for improvement identified. This includes acknowledging good risk management practice and speaking with staff regularly about opportunities to better manage risk. | • Senior executives are held accountable through performance agreements for managing risk including responsibility for strengthening the risk culture of their teams <br>• Risk culture is formally and regularly assessed with recommendations identified for improvement <br>• The Framework is integrated with its overarching governance framework. | • Officials are comfortable raising concerns with senior managers and those being challenged respond positively <br>• A senior executive level sponsor leads and promotes the management of risk <br>• Lessons learned from positive and negative situations. | • Culture demonstrates and promotes an open and proactive approach to managing risk that considers both threat and opportunity <br>• Demonstration of good risk management practices are communicated and rewarded. |
| **Element 6:** Communicating and consulting about risk | • No common risk language is used with limited risk reporting <br>• Branches and/or business units communicate with their stakeholders, but this information is not shared across the entity <br>• Communication of risk issues is as requested which may lead to a duplication of information across the entity. | • Communication with senior executive and/or the accountable authority is limited to specialist risks <br>• A Common risk language is used and understood by the risk management function and senior leadership teams, but these terms are not consistently understood across the entity. | • A common understanding of the principles and importance of managing risk exists <br>• Timely communication of risk information is acknowledged as important <br>• While areas for improvement are identified, feedback is not commonly used to improve <br>• External communication occurs to inform stakeholders of the management of key risks and the risk management approach. | • Risk terminology is understood by all staff, providing a consistent approach to managing risk <br>• Communicating and escalating risk issues is considered in the day-to-day activities of staff <br>• Reporting formats have been agreed and are tailored to target audiences. | • A consistent approach to communicating and discussing risk enables staff to understand how risk management contributes to achieving the objectives <br>• Staff are informed of the entity's risk appetite <br>• Evidence of the integration of risk information with key operational systems exists. | • The importance of communicating risk is apparent across the entity via - common understanding of risk management principles, escalating risk issues as they arise and informing internal and external stakeholders in a timely manner. |
| **Element 7:** Understanding and managing shared risk | • There are no formal arrangements in place to discuss and understand shared risks. | • The Policy defines shared risk <br>• The Framework reflects the requirement to consider shared risk in supporting guidance and documentation <br>• Informal arrangements are in place to discuss and understand shared risks. | • The Framework provides guidance on how to identify, assess, communicate and contribute to the management of shared risk <br>• Formal governance arrangements are in place to discuss and understand shared risks. | • Senior executive champion shared risk behaviours by demonstrating a collaborative approach to managing shared risk <br>• A common understanding of accountabilities and responsibilities for managing shared risk exists. | • The culture of the entity is one where identifying and managing shared risk is considered important <br>• Agreed governance arrangements are in place to discuss, understand and effectively manage both current and emerging shared risks. | • Shared risk and the arrangements for managing it, are reflected in the governance framework and business processes <br>• Established mechanisms and protocols for recording, monitoring and reporting on managing shared risk exist. |
| **Element 8:** Maintaining risk management capability | • There are limited resources available for the management of risk <br>• Key individuals are provided limited risk management training <br>• Informal processes exist to exchange risk information. | • The role of implementing the framework is shared with other responsibilities <br>• Staff are able to develop risk management skills through access to regular training <br>• Risk information is disseminated and shared across the entity informally. | • Dedicated resources are responsible for implementing the framework with a well-developed understanding of operations <br>• Levels of risk competence are identified for each level of the entity <br>• An effective flow of information through the entity exists <br>• Risk information is stored centrally and accessible for key staff. | • The Risk manager or risk management team is responsible for assisting branches or business units to identify and evaluate risk in a consistent structured approach <br>• A consistent approach to identifying and developing risk management skills internally exists <br>• Real-time risk information is stored centrally, accessible by all staff. | • Operational budget reflects the cost of managing key risks <br>• There is a demonstrated culture of knowledge sharing <br>• Risk management information systems are used to undertake data analysis and inform organisational decisions. | • Risk resources are allocated based on detailed data analysis <br>• Ongoing costs of implementing the framework are identified and managed within operational budgets <br>• Demonstrated understanding of the need to build risk capability, focusing on priority areas for improvement, addressing underlying issues and utilising the skills of existing resources. |
| **Element 9:** Reviewing and continuously improving the management of risk | • There is limited oversight of the effectiveness of the framework <br>• The reporting and consideration of risk issues is performed in an uncoordinated manner. | • Reviews of the effectiveness of the framework are undertaken on an ad-hoc basis by the internal audit function <br>• Accountability for the oversight of key risks is unclear. | • Reviews on the performance elements of the framework are completed and reported to senior management regularly to establish review and monitoring plans <br>• Regular reviews and evaluation of all material risks are undertaken <br>• Regular risk reporting occurs in an agreed format <br>• Dedicated staff are responsible for implementing the framework. | • Scheduled risk review and monitoring plans occurs across all branches and business units <br>• Risk reporting includes qualitative and quantitative criteria to assess performance <br>• Regular reviews of compliance with the risk framework are undertaken by internal audit <br>• Ongoing oversight and monitoring of the risk function occurs to identify opportunities for improvement. | • The Framework contains real-time validation and assurance processes <br>• Risk processes are independently assessed regularly <br>• Review and monitoring plans are established and monitored independently <br>• The Accountable authority and senior executive agree target maturity states and identify resources and investment to achieve these. | • Comprehensive data supports continuous review, monitoring and learning <br>• The allocation of resources for managing risk is considered in the business unit operating budget, including the treatment of key risks and the costing of opportunities for improved processes or additional programs. |

## Appendix B - Risk Defence and Governance Model