ENTERPRISE RISK MANAGEMENT POLICY

Adopted Date: **27 October 2010**

Policy Number: **GRC 043**

Policy Type: **Strategic**

Responsible Officer: **Chief Executive Officer**

Department: **Executive**

Version	Decision Number or CEO Approval	Decision Date	History
1	**Portfolio Meeting**	**20 October 2010**	**Draft for discussion**
2	**Ordinary Meeting**	**27 October 2010**	**(Final Draft for discussion)**
3	**Reviewed**	**January 2014**	**Review January 2015**
4	**Reviewed OM-243/19**	**December 2019**	**Review July 2020**
5	**Reviewed OM-159/20**	**September 2020**	**Review September 2023**
6	**Reviewed**	**August 2022**	**Review August 2023**
7	**Reviewed OM-166/23**	**October 2023**	**Review October 2025**

1. PURPOSE

The purpose of the *Enterprise Risk Management Policy* (policy) is to adopt guidelines to implement a consistent and rigorous risk management framework, systems, processes, and controls throughout Goondiwindi Regional Council operations.

2. BACKGROUND

Council's philosophy towards risk is not to be unduly risk averse, but to enable risks to be identified, discussed, mitigated and monitored in a balanced manner.

Council is committed to establishing and integrating our risk management systems and processes to support this philosophy without creating an unnecessary burden on the business.

This policy sets out the processes, responsibilities, and accountability for risk management of the Goondiwindi Regional Council. It recognises that risk management is a critical and integral part of good management and corporate governance practice and that, in relation to commercial strategy, an element of risk is inevitable and, in some cases encouraged.

This policy supports a structured and focused approach to managing risk to complement the strategies adopted by Council to achieve its corporate objectives, in order to increase confidence and enhance the value the Council provides to its stakeholders.

The principles behind this policy are based on the Australian Standard *AS/NZ* ***ISO 3100:2018*** *Risk management – Principles and guidelines.*

3. OBJECTIVES

Council will apply a risk management framework which will:

3.1 Incorporate a consistent, systematic process to identify, analyse, mitigate and monitor the key strategic, operational, financial, environmental and compliance risks impacting on the Council.

3.2 Align risk management with business objectives identified in Council's corporate and operational plans.

3.3 Integrate and align existing risk systems to ensure no duplications or overlap.

3.4 Ensure integration of information systems used for reporting on risk to enable aggregation and reporting at a corporate level.

3.5 Allow the necessary controls and policies to be implemented to deliver an appropriate approach to governance and best practice.

3.6 Will embed a culture of risk management throughout the Council.

3.7 Ensure that risk is considered in conjunction with the following Sections of the *Local Government Regulation 2012*:

3.7.1 Section 164 – records management risk

3.7.2 Section 175 1 b (ii) – operational plan risk

3.7.3 Section 191 – investment risk

3.7.4 Section 207 – internal audit risk

3.7.5 Section 217 – strategic approach risk

3.7.6 Section 221 – contracting risk

4. DEFINITIONS

What is Risk?

Risk is the chance of something happening that will have an impact on the achievement of our business objectives.

Risk can have a positive or negative impact.

Risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

What is Risk Management?

Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council.

Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

What is Enterprise Risk Management? (ERM)

Enterprise-wide risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance,

security and business continuity) and includes the co-ordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

5. POLICY STATEMENT

5.1 This Policy will be considered in conjunction with:

i.) *Goondiwindi Regional Council – Enterprise Risk Management Framework 2023-2025.*

ii.) *Goondiwindi Regional Council – Fraud and Corruption Prevention Framework 2023-2025.*

iii.) *Goondiwindi Regional Council Risk Register*.

iv.) AS/NZS ISO **3100:2018**, the Australian / New Zealand Standard for "Risk management – Principles and guidelines".

v.) *Local Government Act 2009*.

vi.) *Local Government Regulation 2012*.

vii.) Goondiwindi Regional Council Corporate Plan 2019-2024.

viii.) *Goondiwindi Regional Council Operational Plan 2021-2022*.

5.2 Goondiwindi Regional Council is committed to:

i.) Behaving as a responsible corporate citizen protecting employees, clients, contractors, visitors and the general public from injury and unnecessary loss or damage.

ii.) Achieving its business objectives by maximising opportunities and minimising threats through managing the impact of risks it can realistically control; and

iii.) Creating an environment where all Council employees will take responsibility for managing risk (by developing and maintaining a strong risk management culture).

5.3 Principles:

Council's risk management processes are based around the following key risk activities:

i.) Risk Identification: identify all reasonably foreseeable risks associated with its activities, using the agreed risk methodology detailed in the Council's risk protocols.

ii.) Risk Evaluation: evaluate those risks using the agreed Council criteria as depicted in Council's Risk Register.

iii.) Risk Treatment / Mitigation: develop mitigation plans for risk areas where the residual risk is greater than our tolerable risk levels.

iv.) Risk Monitoring and Reporting: report risk management activities and risk specific information in accordance with the risk protocols.

5.4 Roles and Responsibilities:

i.) Council – adopts this policy and retains the ultimate responsibility for risk management and for determining the appropriate level of risk that it is willing to accept in the conduct of Council business activities.

ii.) Chief Executive Officer - is responsible for identifying, evaluating and managing risk in accordance with this policy through a formal enterprise-wide risk management framework. Formal risk assessments must be performed at least once a year as part of the business planning and budgeting process.

iii.) Executive Management Team - Directors are responsible for implementing Council's risk management systems, policies and procedures and the accuracy and validity of risk information reported to the Council. In addition, they will ensure clear communication throughout the Council of the Council and senior management's position on risk.

iv.) The CEO and Director Finance & Corporate Services – will report to Council annually on the progress made in implementing a sound system of risk management and internal compliance and control across Council's operations.

v.) Employees – are responsible for management of risks within their areas of responsibility as determined under any risk treatment plans.

vi.) Employees will be responsible for the timely completion of activities contained within these risk treatment plans. Awareness sessions will be conducted routinely to ensure that employees are familiar with risk management and how it is applied within Goondiwindi Regional Council.

vii.) Risk Monitoring – Council utilises several functions, including its internal audit function, executive meetings to monitoring over its risk areas, including if necessary, conducting reviews over Council's operations and risk areas by external agencies.

viii.) The scope of the work undertaken by all of these functions and the reviews by external agencies will be considered in conjunction with Council's risk profile at least annually. This will assess the independent monitoring of key risk areas within Council's risk profile.

6. ATTACHMENT - Enterprise Risk Management Framework

7. REVIEW DATE

October 2025

Goondiwindi REGIONAL COUNCIL

REGIONAL AUSTRALIA *at its best!*

ENTERPRISE RISK MANAGEMENT FRAMEWORK 2023-2025

Table of Contents

1. Executive Summary 3
1.1 Purpose 3
1.2 Scope 3
2. Introduction 4
2.1 Local Context 4
3. Legislative Context 5
3.1 Legislative Requirements 5
4. Risk Management Context 7
4.1 What is Risk 7
4.2 What is Risk Management 8
4.3 What is Enterprise Risk Management (ERM)? 9
4.4 Risk Management and Fraud 9
4.5 Enterprise Risk Management Policy Statement 9
4.6 Policy Context 10
4.7 Good Governance and Integrity Framework 11
5. Risk Management Framework 12
5.1 Council's Philosophy and Commitment 12
5.2 Goals and Objectives 12
5.3 Risk Management Elements 13
5.3.1 Governing Risk 14
5.3.2 Council's Risk Appetite and Tolerance 16
5.3.3 Risk Environment 16
5.3.4 Assessing Risk 17
5.3.5 Responding to Risk 18
5.3.6 Reporting Risk 18
5.4 Responsibilities 19
Specific Responsibilities 19
6. Risk Management Process 20
6.1 Risk Management Process 20
6.2 Establish the Context 21
6.3 Risk Identification 26
6.4 Risk Analysis 27
6.5 Risk Evaluation and Treatment 27
6.7 Monitoring and Review 29
6.6 Communicate and Consult 30

Appendix 1 – Risk Matrix 31
Appendix 2 – Risk Management Action Plan – 2023-2025 33
Appendix 3 – Risk Management Framework Checklist 36
Key Element 1 – Risk Management Framework 36
Key Element 2 – Establishing the Context 38
Key Element 3 – Risk Identification 40
Potential Source of Risk 42
Key Element 4 – Risk Analysis 44
Key Element 5 – Risk Evaluation 45
Key Element 6 – Risk Treatment 46
Key Element 7 – Monitoring and Review 48
Key Element 8 – Communication and Consultation 50

Document Control

Version	Decision Number or CEO Approval	Decision Date	History
1.0	EX 034/23	25 October 2023	Review October 2025

1. Executive Summary

1.1 Purpose

The purpose of Council's *Enterprise Risk Management Framework* (Framework) is to formalise how risk and opportunities can be effectively addressed at Goondiwindi Regional Council (GRC). This Framework sets out Council's approach to manage strategic and operational risks by establishing robust internal controls and embedding a strong culture of risk management throughout the organisation.

The Framework is designed to support the achievement of Council's priorities in the Corporate Plan and annual Operational Plan, along with the operational requirements of each Department. It requires identifying, assessing, and treating risk, based on each Departments risk appetite within the context of Council's overall risk environment. This approach draws from the principles and guidelines in the international risk management standard *AS/NZS ISO 31000: 2018 – Risk Management - principles and guidelines* (ISO 31000) which states:

> *"The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives."*

The framework aims to:

1) Deliver better outcomes for the communities we serve.
2) Pursue continuous improvement in all areas of operations.
3) Minimise harm.
4) Minimise financial and reputational damage to Council.
5) Identify and manage operational and strategic risks.
6) Maintain the effectiveness of Council operations.

The Framework's implementation will ensure that our risk tolerance is managed responsibly, and our operations are provided to protect public interest from adverse risks.

1.2 Scope

The Risk Management Framework applies to all Councillors, Council employees, contractors, and volunteers.

The Framework assists every Department to apply a consistent approach to risk management.

2. Introduction

2.1 Local Context

All Council's activities involve risks and opportunities. This Framework provides a localised approach 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 GRC to unacceptable levels of risk.

5) Improved resident, community and stakeholder confidence and trust.

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

GRC 043 Enterprise Risk Management Policy (Policy) sets the strategic direction and commitment Council has made to manage risks. The strategic context is reinforced with a required statement articulating how operational risks will be managed in each annual Operational Plan.

The operational context is articulated through the Framework. Various elements work together to ensure risk management is embedded within Council's processes, planning, values, and culture.

Council's risks are managed by identifying, analysing, and evaluating whether the risk should be modified by risk treatment(s) to satisfy the risk appetite.

Most risk factors are measured in financial terms; however, risk mitigation also needs to place a 'value' against intangible measures arising from incidents causing pain and suffering to individuals, and/or reputational damage, and/or other detrimental impacts, when determining the level of risk tolerance.

To be effective at managing risk, Council must develop, implement, and continuously improve its Framework. This requires continuously improving the Framework with the integration of risk management through the Good Governance and Integrity Framework (Refer chapter 4.7).

3. Legislative Context

3.1 Legislative Requirements

The *Local Government Act 2009* does not specifically address risk management; however *Local Government Regulation 2012* (Regulation) sets out requirements for local governments to identify, record and manage risks.

Section 164 of the Regulation articulates the requirement for local governments to keep a written record of the risks their operations are exposed to, to the extent they are relevant to financial management, and to record the control measures adopted to manage those risks. Councils must keep with the record a copy of the following:

- Community Grants Policy.
- Entertainment and Hospitality Policy.
- Advertising Spending Policy; and
- Procurement Policy

Section 175 of the Regulation requires the annual operational plan to state how the local government will manage operational risks.

Each Council must have financial policies and auditing requirements that incorporate a risk component. The Regulation outlines the need for:

1) An Investment Policy that must outline investment objectives and overall risk philosophy. (*s.191* of the Regulation)
2) An Internal Audit Plan that states the way operational risks have been evaluated, determined to be most significant and the control measure adopted to manage the most significant risks. (*s.207* of the Regulation)
3) Applying a strategic approach for contracting procedures that considers potential opportunities while managing adverse risks. (*s.217* of the Regulation)
4) Significant Contracting Plans, where resolved to be used, to include a risk analysis of the market in which the contract is to happen. (*s.221* of the Regulation)
5) Quote or Tender Consideration Plans, where resolved to be used, to include a risk analysis of the market in which the contract is to happen. (*s.230* of the Regulation)
6) Control measures that are a measure that may be adopted for managing a risk. (*Schedule 8 – Dictionary* of the Regulation)

The *Work Health and Safety Act 2011* (WH&S Act) and *Work Health and Safety Regulation 2011* (WH&S Regulation) and *Codes of Practice* provide further legislative requirements for managing risks.

Every work environment has hazards that could cause harm to staff. The word risk describes how likely that harm is to happen and how severe that harm could be.

Together, WH&S Act and the WH&S Regulation require every organisation to have clear processes in place to eliminate or minimise risks to staff and contractors. This includes pursuing ways to prevent incidents before they happen, protecting staff safety, and productivity. It also requires the ability to show the regulator that an effective risk management process is in place, should an incident occur.

Section 17 of the WH&S Act sets out the duty imposed on a person to ensure health and safety requires the person to eliminate risks to health and safety as far as practicable, and if it is not practicable to eliminate those risk then to minimise them as far as is reasonably practicable.

Section 18 of the WH&S Act introduces the elements of risk and general concepts of determining levels of risk tolerance, that flow further through this framework. They include:

1) Assessing the likelihood of the risk occurring;
2) The degree of harm that may result;
3) What the person assessing the risk knows, or reasonably ought to know about the risk and how to eliminate or minimise it; and
4) After assessing the extent of the risk and available ways of eliminating, the cost associated, including whether the cost to eliminate or mitigate it are grossly disproportionate to the risk occurring.

The health and safety of workers is a primary duty of care for every organisation. The WH&S Act and the WH&S Regulations requirements in this regard are quite extensive. Rather than including all the elements of the legislation here, it is identified that Workers Health and Safety will be included as both a strategic risk for the organisation to be managed at a corporate level, as well as an operational risk to be managed by each Department at the local level.

Given the financial aspects associated with risk, *Section 23* of the *Financial and Performance Management Standard 2019* prescribes that a risk management system of an agency must provide for:

1) Mitigating the risk to the department or statutory body and the State from an unacceptable costs or losses associated with the operations of the department or statutory body; and

2) Managing the risks that may affect the ability of the department or statutory body to continue to provide government services.

Council has policies, plans, processes, and procedures in place that work towards addressing these legislative and regulatory requirements. The continuous refinement of the Framework and expansion of practical tools and staff education will be used to manage Council's risk environment.

4. Risk Management Context

4.1 What is Risk

Risk is the chance of something happening that will have an impact on the achievement of the organisation's objectives. Risk is measured in terms of consequence and likelihood and covers threats and opportunities.[1]

Risk relates to both challenges to, and opportunities for, the organisation.[2]

Risk arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

The *Financial and Performance Management Standard 2019* separates risks into two types – strategic and operational risks.

1) Strategic Risks – are those which could significantly impact on the achievement of the organisation's strategic planning and management processes; and
2) Operational Risks are those which could have a significant impact on the achievement of:
    a) the agency's strategic objectives (as documented in the strategic plan) from the perspective of the actions undertaken by a particular division, branch, or work unit; or
    b) the individual programs or project management objectives.

Operational risks generally require management by the relevant senior officers responsible for the Department.[3]

Council's application of the two types of risk:

1) Strategic Risks are generally entity wide, may impact on the organisation's ability to achieve its strategic objectives in the Corporate Plan and/or the delivery of critical services. Examples include reputational risk and Council-wide compliance risk. These require the attention of the Chief Executive Officer and Executive leadership Team. Council manages these strategic risks by:
    a) Defining its business strategy and objectives. The Corporate Plan should integrate risk at the planning stage.
    b) Establishing key performance indicators (KPI's) to measure results. Council should define KPI's that are aligned to the business strategy and objectives. They usually measure historic data.
    c) Identifying risks that can drive variability in performance. These can be the unknowns that can impact results. Examples may include future customer demand, changing climate impacts, pandemics, or disasters.
    d) Establishing key risk indicators (KRI's and tolerance levels for critical risks. KRI's are early warnings for risk exposure levels that may exceed tolerance levels and are intended to anticipate potential blockages. Tolerance levels serve as triggers for action. KRI's can be lead (forward looking such as monitoring consumer price indexes) or lag (backward looking such as monitoring lost time injuries).

[1] A Guide to Risk Management – Queensland Treasury page 27 version 1 updated 18/08/2020.
[2] A Guide to Risk Management – Queensland Treasury page 7 version 1 updated 18/08/2020.
[3] A Guide to Risk Management – Queensland Treasury page 7 version 1 updated 18/08/2020.

e) Providing integrated reporting and monitoring. This requires monitoring results and KRI's continuously to mitigate risks and manage unexpected opportunities as they arise.

2) Operational Risks are risks which may impact on the achievement of department plans, projects, objectives, or service delivery, that support the strategic objectives of Council. Operational risks are primarily the responsibility of each Department, and the management and reporting responsibilities reside with Management and Directors.

Oversight of both types of risk is provided by the Internal and External Auditors. The Three Line Model outlined in Chapter 5.3.1 sets out the governing environment utilised by Council.

4.2 What is Risk Management

Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council.

It incorporates the systematic application of processes for identifying, analysing, evaluating, treating, monitoring, and communicating the outcomes in a timely manner to those who need to understand them.

An effective risk management system:

1) Improves planning processes by enabling the key focus to remain on core business and helping to ensure continuity of service delivery.
2) Reduces the likelihood of potentially costly 'surprises' and assists with preparing for challenging and undesirable events and outcomes.
3) Contributes to improved resource allocation by targeting resources to the highest-level risks.
4) Improves efficiency and general performance.
5) Contributes to the development of a positive organisational culture, in which people and agencies understand their purpose, roles and direction.
6) Improves accountability, responsibility, transparency, and governance in relation to both decision-making and outcomes.
7) Adds value as a key component of decision-making, planning, policy, performance, and resource allocation, when subject to continual improvement.[4]

Factors that inhibit effective risk management can include:

1) A lack of support for a risk management culture from executive management.
2) A lack of time and resources allocated to risk management.
3) Difficulty in identifying and assessing emerging risks, especially cross-agency risks.
4) A lack of independent assurance over the effectiveness of the risk management framework.
5) A lack of clarity over risk ownership and the responsibility for risk management.
6) Over, or under, treatment of risks.
7) Unnecessarily complex risk documentation.[5]

[4] A Guide to Risk Management – Queensland Treasury page 7 version 1 updated 18/08/2020
[5] A Guide to Risk Management – Queensland Treasury page 7 and 8 version 1 updated 18/08/2020

When risk management has commitment from executive management by encouraging a strong organisational culture and awareness of risk, an agency should be able to overcome the factors which inhibit effective risk management.[6]

Council has assigned roles and responsibilities that work towards building a strong risk management and control culture. Risk awareness, ownership, and proactive management of key risks, along with prudent risk taking, is promoted. The roles and responsibilities are outlined in Chapter 5.4 of the Framework.

4.3 What is Enterprise Risk Management (ERM)?

Enterprise-wide risk management (ERM) encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security, and business continuity) and includes the co-ordination, integration, consolidation, and consistency of reporting by the various Council functions with identified risks.

Council's ERM is established in the *GRC 043 Enterprise Risk Management Policy* and this Framework.

4.4 Risk Management and Fraud

Risk management and fraud control are integrally linked. As an integral part of Council's *Enterprise Risk Management Framework*, the *Fraud and Corruption Prevention Policy* and the *Fraud and Corruption Prevention Framework 2023-2025* (Fraud Framework) all includes proactive measures designed to enhance system integrity (prevention measures) and reactive responses (reporting, detecting and investigative activities) to remove, or at least minimise, any fraudulent practices.

Fraudulent and corrupt conduct by public officers may fall within the category of 'corrupt conduct' under the *Crime and Corruption Act 2001* (CC Act). In addition, many forms of fraud and corruption are offences under the *Criminal Code Act 1899*. There can be significant financial and reputational losses and costs associated with fraudulent conduct.

4.5 Enterprise Risk Management Policy Statement

Goondiwindi Regional Council is committed to:

- *Behaving as a responsible corporate citizen protecting employees, clients, contractors, visitors and the general public from injury and unnecessary loss or damage;*
- *Achieving its business objectives by maximising opportunities and minimising threats through managing the impact of risks it can realistically control; and*
- *Creating an environment where all Council employees will take responsibility for managing risk (by developing and maintaining a strong risk management culture).*[7]

[6] A Guide to Risk Management – Queensland Treasury page 8 version 1 updated 18/08/2020
[7] Goondiwindi Regional Council Enterprise Risk Management Policy page 3, version 6 August 2022

4.6 Policy Context

The Framework consists of a suite of tools and resources including all Council policies; however, the following policies and tools are particularly relevant:

1) Risk Management Controls
   a) *Enterprise Risk Management Policy*
   b) *Enterprise Risk Management Framework 2023-2025*
   c) Risk Register
   d) Risk Matrix
   e) Risk Assessments
   f) Internal Audit Plan
2) Fraud Controls
   a) *Fraud and Corruption Prevention Policy*
   b) *Fraud and Corruption Prevention Framework 2023-2025*, including Control Plan and 2023-2025 Action Plan
   c) Fraud and corruption control risk assessments
3) Staff Controls
   a) *Code of Conduct*
   b) Disciplinary Procedures Policy
   c) Workplace Health and Safety Policy Statement
4) Financial Controls
   a) *Debt Policy*
   b) *Investment Policy*
   c) *Procurement Policy*
   d) *Revenue Policy*
5) Governance Controls
   a) *Advertising Spending Policy*
   b) *Competitive Neutrality Complaints Policy*
   c) *Councillor Code of Conduct (Queensland)*
   d) *Complaints Management Policy*
   e) *Councillor Remuneration and Expenses Policy*
   f) *Councillors Travel and Attendance Policy*
   g) *Entertainment and Hospitality Policy*
   h) *Information Privacy Policy*
   i) *Investigation Policy*
6) Information Technology Controls
   a) *Information Security Policy*
   b) *Back-up Policy*
7) Community Controls
   a) *Community Grants Policy*

4.7 Good Governance and Integrity Framework

Risk management at Council forms part of the organisation's broader good governance processes and integrity responsibilities. These in summary include:

Council's overarching *Enterprise Risk Management Framework* is interrelated with the following strategic documents and good governance policies:

- *Goondiwindi Regional Council Corporate Plan 2019-2024*
- *Goondiwindi Regional Council Operational Plan 2023-2024*
- *Goondiwindi Regional Council Enterprise Risk Management Policy 2022*
- *Goondiwindi Regional Council Internal Audit Policy 2023*
- *Goondiwindi Regional Council Fraud and Corruption Prevention Policy*
- *Goondiwindi Regional Council Fraud and Corruption Prevention Framework 2023 - 2025*
- *Goondiwindi Regional Council Employee Code of Conduct 2019*
- *Goondiwindi Regional Council Business Continuity Plan*
- *Councillor Code of Conduct (Queensland) 2020*

5. Risk Management Framework

5.1 Council's Philosophy and Commitment

Council's philosophy towards risk is not to be unduly risk averse, but to enable risks to be identified, discussed, mitigated, and monitored in a balanced manner.

Council is committed to establishing and integrating our risk management systems and processes to support this philosophy without creating an unnecessary burden on the business.

Council recognises that risk management is a critical and integral part of good management and corporate governance practice and that, in relation to commercial strategy, an element of risk is inevitable and, in some cases, encouraged.

5.2 Goals and Objectives

Council will apply a Framework which will:

1) Incorporate a consistent, systematic process to identify, analyse, mitigate, and monitor the key strategic, operational, financial, environmental, and compliance risks impacting on the Council.

2) Align risk management with business objectives identified in Council's corporate plans and annual operational plans.

3) Integrate and align existing risk systems to ensure no duplications or overlap.

4) Ensure integration of information systems used for reporting on risk to enable aggregation and reporting at a corporate level.

5) Allow the necessary controls and policies to be implemented to deliver an appropriate approach to governance and best practice.

6) Embed a culture of risk management throughout the Council.

7) Ensure that risk is considered in conjunction with the following Sections of the *Local Government Regulation 2012*:
   a) Section 164 – records management risk
   b) Section 175 1 b (ii) – operational plan risk
   c) Section 191 – investment risk
   d) Section 207 – internal audit risk
   e) Section 217 – strategic approach risk
   f) Section 221 – contracting risk

5.3 Risk Management Elements

This diagram identifies the key elements of Council's approach to manage risks.[8]

We govern risk through Executive and Council oversight of organisational strategic and departmental operational risks.

Risk Appetite – outlines the level of risk that can be taken.

We manage risks that emerge from our operating environment.

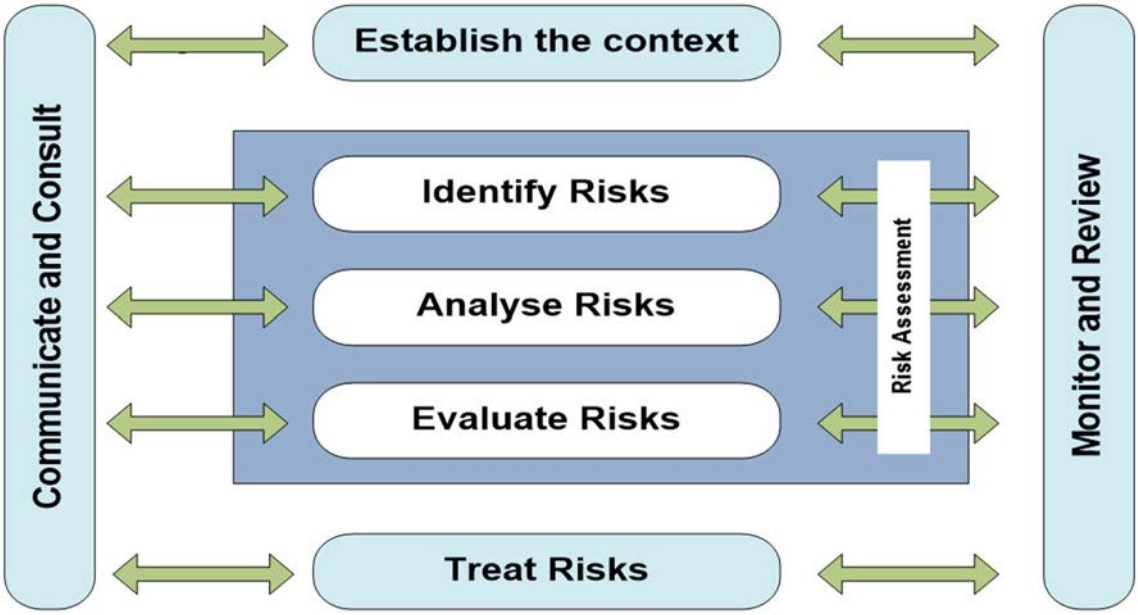
We provide assurance that risk is reported so it can be managed, escalated, treated, mitigated, and monitored.

We regularly assess our risks, identify trends, and respond to risks and opportunities for continuous improvement.

We assess risk using a structured process.

[8] Modified from the Queensland Government Enterprise Risk Management Framework Department of Education – Elements of the Enterprise Risk Management Framework, Feb 2023

The following Risk Management Process diagram outlines the steps to be taken in identifying and responding to risks. Further details are contained in Chapter 6.

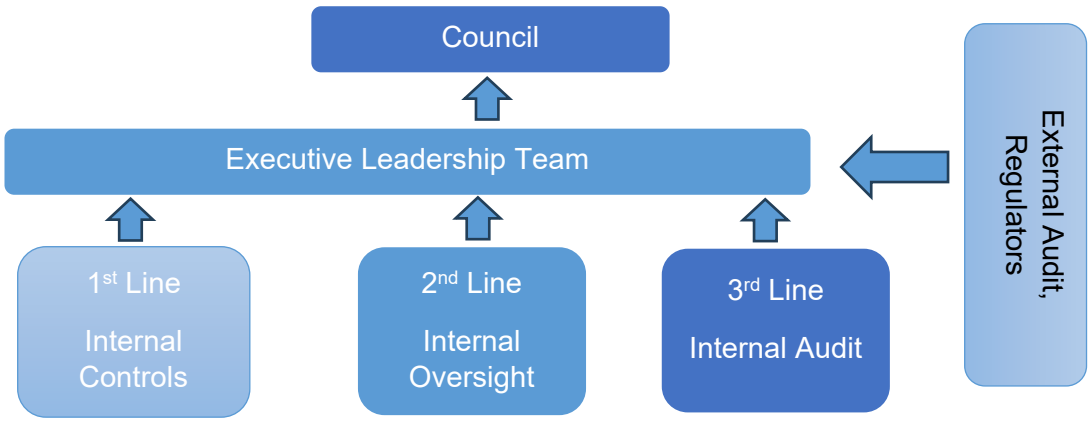


5.3.1 Governing Risk

Risk management begins with alignment to the Council's overall business strategy and objectives, as outlined in the five-year Corporate Plan. This component incorporates establishing the context, risk appetite, risk tolerance and risk environment that need to be considered.

Risks are identified as either Strategic Risks, or Operational Risks, as outlined in Chapter 4.1. The following Three Line Model provides a governing environment for managing risk.

The Three Line Model[9]



[9] Modified from the South Gippsland Shire Council Risk Management Framework 2022.

The responsibilities of each line are outlined below:

Council and Executive Leadership Team

Council and the Executive Leadership Team are the primary stakeholder served by the Three Lines Model and are the best parties to ensure that the three lines are reflected in Council's risk management and control processes. The Executive Leadership Team and Council have responsibility and accountability for setting Council's objectives, strategies and governance structures to best manage the risks in accomplishing these objectives.

1st Line – Internal Controls

The responsibility of each Department, with process (risk) owners, whose activities create and/or manage the risks that can facilitate positive or prevent negative outcomes from being achieved. Operational management are responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.

There should be adequate management and supervisor controls in place to ensure compliance and to highlight control breakdowns, inadequate processes, and unexpected events. Departments are responsible for implementing corrective actions to address process and control deficiencies.

2nd Line Control – Internal Oversight

The second tier supports management by bringing expertise, process excellence, and management monitoring alongside the first line to help ensure that risk is effectively managed. The second line is essentially a management and/or oversight function that sets direction and defines policy, identifies known and emerging issues, identifies shifts in risk appetites, guidance/training and internal reporting. This includes risk management and compliance functions such as:

- Governance / Legal
- Delegations
- Financial Control
- Workplace Health and Safety
- Environmental Health
- Disaster Management

3rd Line Control – Internal Audit

Internal audit is the third line offering independent challenge to the levels of assurance provided by Internal Control and Internal Oversight functions. Internal auditors provide the Executive Leadership Team and Council with comprehensive assurance based on the highest level of independence and objectivity within the organisation.

Internal audit can provide assurance on the effectiveness of governance, risk management and internal controls. The Internal Auditor receives access to Council's risk registers and assists in informing the Internal Audit Plan and Internal Audit Scopes. Specific risks addressed are included within the Internal Audit Plan Scopes.

External Auditors and Regulators

External auditors and regulators reside outside of Council's structure but play an important role in Council's overall governance and control structure and can provide additional assurance to the Executive Leadership Team and Council. Given the specific scope and objectives of their roles, results in information gathered are generally less extensive than Council's internal lines.

5.3.2 Council's Risk Appetite and Tolerance

Risk Appetite

Risk Appetite is the level of risk that Council is prepared to accept in delivering its key strategic objectives. The key strategic objectives for Council are outlined in the five-year Corporate Plan. Council faces multiple internal and external factors and influences that make it uncertain whether, when and to what extent it will achieve or exceed its objectives.

Council recognises that all activities involve risk because outcomes of operations are not always certain. Council also recognises risks are not all equal in terms of likelihood or consequence. The costs to minimise some risks may be more detrimental than the risks they are seeking to minimise. To this end, Council manages its risk appetite in a balanced way.

The strongest appetite for risks thereby requiring greater controls are associated with:

1) Workplace health and safety of Councillors and staff.
2) Health and safety of the community.
3) Security of confidential and personal information held by the organisation.
4) Fraud and corruption.
5) Legislative and Regulatory compliance

As a requirement, Council has a core requirement to comply with and meet its legislative obligations. Monitoring and responding to changes in legislation requires vigilance to ensure Council remains compliant.

The Council is willing to accept a reduced appetite of risk when pursuing innovation and opportunities that further its strategic corporate objectives. These include pursuing opportunities that benefit the community but not at the expense of its responsibilities to ethical leadership, regulatory compliance, health and safety, financial sustainability, or environmental responsibility.

Council's risk appetite varies according to the activity undertaken. It is recognised that acceptance of risk is subject to always ensuring the potential benefits and risks are fully understood before activities are authorised, and that sensible measures to mitigate risk are established.

Risk Tolerance

Council's risk tolerance will vary depending on the challenge, or opportunity at the time. The tolerance levels may, for example, change from project to project based on the cost of the project, the political issues surrounding the project, and/or the inherent safety concerns that have been determined.

Each risk identified by Council will be individually assessed by the risk owner to determine whether the risk is within Council's tolerance and will be actioned accordingly. Risk tolerances are included in the Risk Register. They are also included with the Risk Matrix in Appendix 1.

5.3.3 Risk Environment

The risk environment is important as it sets the parameters within which risks are identified, assessed, and managed. As such, it must be sufficiently broadly defined to include a wide range of trends, influences, and time horizons. It needs to consider the internal and external environment that Council operates within.

Council will need to collect information at both the strategic and operational levels and include both the external and internal risks facing the agency.

The primary influences on the external environment relate to the social, cultural, political, legal, regulatory, financial, technological, supply chain and economic environments within which Council operates. Legislation and regulation will play an important part in considering the external environment. Consideration is needed for the influences occurring at a local, regional, industry-based, state, national and international level.[10]

The internal environment may include:

1) Council's strategic objectives in the Corporate Plan.
2) Council's priority actions in the annual Operational Plan.
3) Strategic directions in adopted Council plans and policies.
4) Individual projects of the organisation.
5) Service and program delivery by each Department.
6) Resources available within the organisation.
7) Knowledge, skills and capability of Council staff.
8) Risk management knowledge and practices.
9) Business Continuity Plans.

Both the external and internal environments are constantly changing so both should be regularly monitored and examined to pick up and respond to changing trends to remain relevant and stay abreast of changes to risks.

5.3.4 Assessing Risk

Assessing risks incorporates identifying, analysing, and evaluating risks. The risks identified, along with the analysis and treatment plans are captured within the Risk Registers; one spreadsheet for Organisational Strategic Risks, and another for Departmental Operational Risks.

Council uses a risk matrix to combine the likelihood of a risk occurring and a consequence should it occur. Together these result in a risk rating to be used in treating and monitoring the risk. Parameters have been applied for each 'likelihood' and 'consequence' in the matrix. The same risk criteria are to be used by the whole organisation. The full matrix is contained within Appendix 1.

'Likelihood' considers the chance the Council will be exposed to each risk. Frequency of it potentially occurring provides the 'likelihood' measure on the Risk Matrix. Risk management seeks to reduce the likelihood of potentially costly 'surprises', and assists with preparing for challenging and undesirable events and outcomes.[11]

'Consequence' considers the outcome of an event which affects the Council's ability to achieve its objectives. Potential outcome, and its severity, provide the 'consequence' measure on the Risk Matrix. Risk management treatments are focused on reducing the severity of any undesirable outcomes.

The two ratings together determine the overall level of risk, and thereby the risk tolerance applicable to it. There are four levels: low, moderate, high and extreme.

[10] A Guide to Risk Management – Queensland Treasury pages 14 and 15 version 1 updated 18/08/2020
[11] A Guide to Risk Management – Queensland Treasury page 5 version 1 updated 18/08/2020

Each Department will give each of their identified risks a rating using ‘likelihood’ and ‘consequence’ both before any treatments are considered, and after treatments are taken into account. This double rating shows how effective the treatments may be on the outcome after treatments are applied.

5.3.5 Responding to Risk

Responding to risks incorporates treating risks, or determining if the risk fits within the risk tolerance range without any specific treatments. Risks could potentially result in major adverse consequences for Council if not adequately managed.

Each Department, having identified, analysed, and established a treatment plan need to ensure the treatments are well-known by those needing to enact them. These risks need to be actively responded to and monitored.

It is important to be aware that there is likely to remain a residual risk even after identifying, analysing, and treating the risk.

Some risk treatments may create their own risks.

5.3.6 Reporting Risk

Internal reporting forms part of the ongoing monitoring of risks. Regular reviews are needed to monitor progress, assess the effectiveness of controls and report on the achievements. Several reporting approaches are used within the organisation.

Departmental risks are reviewed annually with any significant changes brought to the attention of the Executive Leadership Team. Managers are required to monitor their higher risks throughout the year to identify any changes in trends that may require further assessment and treatment plans.

Annually the Executive Leadership Team review the strategic risks and monitor any changes. At the same time the Executive consider which risks require assessment by the Internal Auditor. A report containing the proposed annual Internal Audit Plan and the strategic risk review are provided in a report to Council.

Internal audit reports provide an independent assessment of operational areas with various potential risk. A minimum of four areas are reviewed each year. The areas and scope of audits are set by Council. Each report captures an analysis of the factors discovered and recommendations to address concerns identified. The recommendations are captured in a Risk Register spreadsheets that assists with monitoring and capturing progress against actions from each of the reviews. These spreadsheets are referred to the Executive Leadership Team as one of the reporting mechanisms.

External reporting of performance is provided to Council quarterly on the progress of achieving the annual *Operational Plan*. This report provides a report on how effectively Council is delivering on its adopted priority outcomes.

The Council’s *Annual Report* each year provides the community with an end-of-financial year account of the organisation’s effectiveness in achieving its adopted priorities.

5.4 Responsibilities

The responsibility for risk management rests with all levels of management, Councillors, employees, volunteers and contract staff who collectively work together to manage and minimise negative risks impacts.

Specific Responsibilities

Role	Responsibilities
Council	Council adopts the revised *Enterprise Risk Management Policy* and Framework. Council retains the ultimate responsibility for risk management and for determining the appropriate level of risk that it is willing to accept in the conduct of Council business activities. This includes adoption of the five-year Corporate Plan and annual adoption of the Operational Plan, Budget, and Internal Audit Plan for each financial year.
Chief Executive Officer	The CEO is responsible for identifying, evaluating, and managing risk in accordance with the Risk Management Policy through a formal enterprise-wide Risk Management Framework. The most significant strategic risks and risk profile will be reviewed, reassessed, and determined annually as part of the formal risk assessments that must be performed at least once a year as part of the business planning and budgeting process. These reviews will take into consideration recommendations from the Internal and External Auditors and any significant changes in operational risks.
Executive Leadership Team	Directors are responsible for implementing Council's risk management systems, policies and procedures and the accuracy and validity of risk information reported to the Council. In addition, they will ensure clear communication throughout the organisation of the Council and Executive Leadership Team's position on risk
CEO and Director Community & Corporate Services	The CEO shall report to Council annually on the progress made in implementing a sound system of risk management and internal compliance and control across Council's operations.
Leadership Group	All managers and supervisors are responsible for identifying, evaluating, treating, and monitoring potential and actual risks within their operations. Managers are to critically examine their areas of responsibility and business processes to document their operational risks. They are to develop, maintain and monitor work practices to minimise the likelihood and negative consequences of their various risks.
All employees, volunteers and contractors	All Council officers, volunteers and contractors are responsible for management of risks within their areas of responsibility as determined under any risk treatment plans, and/or contractual agreements. All Council officers will be responsible for the timely completion of activities contained within these risk treatment plans. Awareness sessions will be conducted routinely to ensure that employees are familiar with risk management and how it is applied within Goondiwindi Regional Council.

Health and Safety Committee	The Health and Safety Committee will be responsible for overseeing workplace health and safety concerns across the organisation and act in an advisory capacity to make recommendations to management.
Goondiwindi Regional Local Disaster Management Group	The Disaster Management Committee is responsible for planning the combined responses to potential disasters and emergency management responses.
Risk Owner	The Council officer assigned as the responsible owner of each individual risk. This person is the primary person responsible to regularly review and monitor the risk, and implement treatments as determined through the assessment.
Legal Officer	Council's Legal Officer is responsible for the coordination of Council's *Enterprise Risk Management Framework* and assisting areas with risk assessments, and staff awareness.
Internal Auditor	Council Internal Auditor's responsibilities include: • The consideration, recommendation and reporting of operational activities within the *Enterprise Risk Management Framework*, as part of internal audits. The audits to be conducted are adopted by Council annually. • Raising awareness and providing advice to the CEO, Executive Leadership Team, Legal Officer and Managers on risk management related matters. • Support the CEO and Legal Officer in the planning, development and delivery of the *Enterprise Risk Management Framework* and *Fraud and Corruption Prevention Framework.*
External Auditor	External Auditors conduct reviews of various Council operations and risk areas predominantly focusing of financial functions. Other areas of interest to the External Auditor's may also be explored.

6. Risk Management Process

6.1 Risk Management Process

The risk management process provides guidance to Department Managers and the Executive Leadership Team in undertaking their risk assessments. The checklist in Appendix 3 – Key Element 1 may assist in critical thinking for this component of the process.

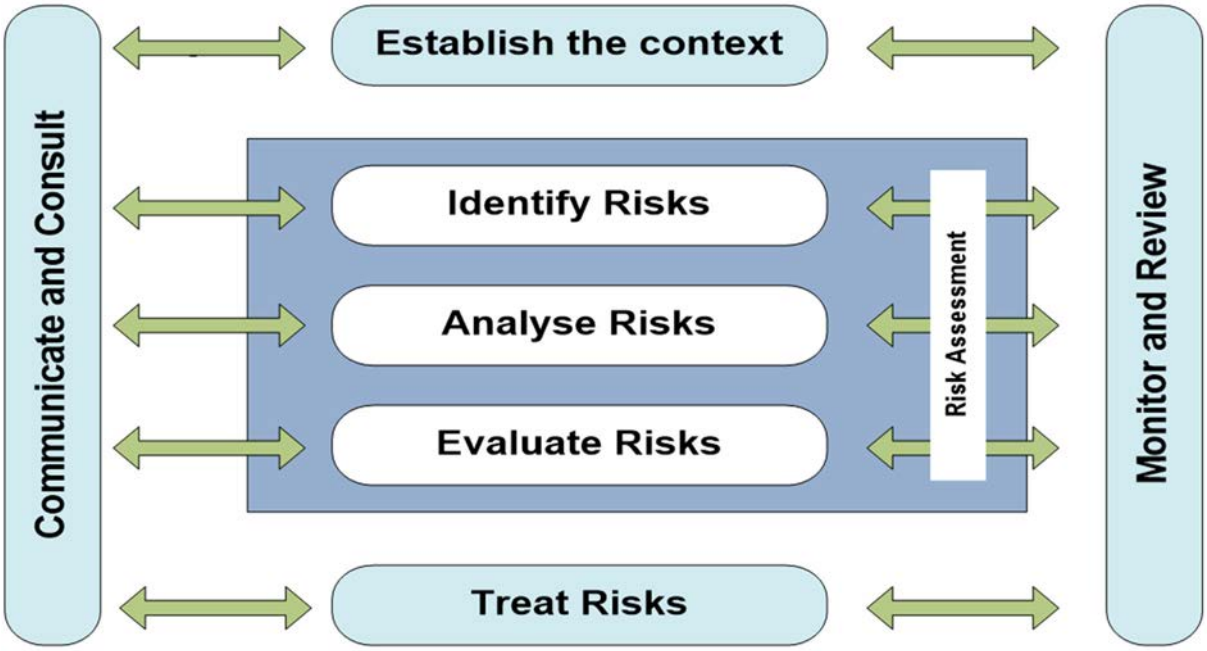
The process followed by Goondiwindi Regional Council to manage risks is in accordance with *AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines*. This process is the application of the structured risk management methodology to be used to assess, prioritise, treat and monitor risks identified. The risk management process will capture inherent risks (prior to considering controls in place) and the residual risks (after considering controls are in place).

The main elements include:

1) Establish the Context
2) Analyse the Risks

3) Undertake a Risk Assessment
4) Identify Risks
5) Analyse Risks
6) Evaluate Risks
7) Treat Risks
8) Communicate and Consult
9) Monitor and Review

The following diagram represents the components of the risk management process. Each of these components is explained further below.



6.2 Establish the Context

Establishing the context sets some parameters within which the Department operates and the capacity of the Department, and/or wider organisation to successfully address them. These limitations will be identified in more detail for each risk during the assessment phase.

The Department, in establishing the context, should consider:

1) The external and internal environment.
2) The risk profile.
3) Risk appetite and risk tolerance levels.
4) Risk matrix and responsibilities.
5) The business continuity plan.

The organisational context needs to be reviewed on a regular basis to identify changes that may in turn require the context and risk profile to be amended.

The checklist in Appendix 3 – Key Element 2 may assist in critical thinking for this component of the process.

External and Internal Environment

Establishing the external and internal environment is the first step in the process. It involves considering both challenges and opportunities at both an organisational level and at a department level. These need to be considered in the context of the Council's vision, strategic objectives, operating environment, and key stakeholders. Together these guide the parameters needed to identify, assess, and manage risks.

Council needs to establish these at a strategic level as it sets the Corporate Plan. The Executive Leadership Team needs to factor these considerations in when putting forward the annual Operational Plan. Departments consider these factors at an operational level, keeping in mind the strategic environment established by Council. Once defined, both internal and external environments should be examined regularly, and considered in setting annual and longer-term operational plans and budgets. These influences may be relevant from international, national, state, regional or local levels.

External environment influences may consider:

1) Social
    a) Socio-economic factors
    b) Capacity of community members
2) Cultural
    a) Demographic influences
    b) Community interests and aspirations
    c) Volunteering capacity and capability
3) Political
    a) Perceptions of Council
    b) Community influencers
    c) Councillors interests and aspirations
    d) Political party influences
    e) Developer influencers
    f) Local Government sector
    g) State and/or Federal Government policies and directions
    h) Home-land security, wars, and international tensions,
4) Legal
    a) Legislative requirements
    b) Contractual requirements
    c) Legal challenges
    d) Litigious demands
5) Regulatory
    a) Regulatory controls
    b) Delegation of powers
    c) Industry changes
6) Financial
    a) Community capacity to fund works, services and capital
    b) Grant reliance and relevance
7) Technological
    a) Emerging technology and software
    b) Cyber security and threats
    c) Artificial intelligence
8) Economic
    a) Potential of recessions

   b) Inflation, cost of living and/or costs from the supply chain
   c) Availability and capability of suppliers, contractors, and consultants
   d) Waste management impacts
9) Geographic location
10) Natural environment
   a) Climate impacts from drought, heat, flood, earthquakes
   b) Soil conditions and stability
   c) National and/or state climate targets

Internal environment influences consider:

1) Council's Corporate Plan incorporating the five-year strategic objectives
2) Adopted directions established in Council and operational policies
3) Adopted plans, planning schemes and longer-termed planned outcomes
4) Department business plans and budgets
5) Existing and planned individual projects and programs
6) Council's governance and accountability structures, including:
   a) Organisation structure
   b) Delegations
   c) Procedures and processes
7) Resources available in the organisation, including:
   a) Information systems
      i) Existing systems and program
      ii) Emerging technology
      iii) Skills and knowledge to utilise systems
      iv) Capacity and capability of the IT network
   b) Staffing;
      i) Capability
      ii) Team culture
      iii) Perceptions
      iv) Turn-over
   c) Human resources;
      i) Training and development
      ii) Management and leadership capability and capacity
      iii) Workplace health and safety
   d) Funding capability:
      i) Level of debt – Council and outstanding community debt
      ii) Financial policies
      iii) Sources of revenue generation
8) Existing risk management expertise and practices:
   a) Strategic risks at Organisation level
   b) Operational risks at Department level
   c) Risk culture and awareness

Risk Profile

Risk management underlies all aspects of priority setting, planning and resource allocation. Establishing an interrelationship between Council's risk profile and the planning process is required to build a robust strategic and operational planning process.

At an organisational level, Councillors and the Executive Leadership Team need to consider the strategic risks when developing and adopting the Corporate Plan, Budget, Annual Operational Plan, and longer-term strategic plans.

When setting the strategic directions, consider the following:

1) The outcomes Council, and/or the Department, is aiming to achieve, and the extent to which the strategic direction will assist in achieving them.
2) Whether the risks associated with implementing the strategic directions can be tolerated, along with determining if the benefits to the community exceed the costs of implementing the direction.
3) If the strategic directions are a Council responsibility and priority. If so, to what extent they align with other adopted plans and directions already established by Council.
4) If the current timing is appropriate for setting and implementing the strategic directions, taking into consideration the internal and external environmental factors identified.
5) Will the new strategic directions place in jeopardy the success of other priorities of Council. If so, what new risk will this introduce?

At a Departmental level, Managers and Directors need to consider their operational risks, and strategic risks relating to their area, when they consider the priorities for setting their budgets, determining their resource requirements, setting their annual projects and recruit staff.

Together, the risk profile and strategic planning documents and processes feed from, and into, each other. The better these are both considered when setting priorities, the more robust the planning processes and outcomes will be.

Risk Appetite and Risk Tolerance Levels

When determining the risk appetite and tolerance levels for both the organisation and for each Department, it is important to consider 'lessons learned', both positive and negative, from the past and to use these to enhance current practices and processes.

In considering each strategic and operational risk to determine its potential tolerance level, consideration should be given to the following aspects:

1) Commitments made/adopted by Council.
2) Performance expectations expressed in the Corporate Plan, Operational Plan and Budget.
3) How customers, and/or the wider community have reacted to past local events and issues.
4) How the local government industry has reacted to previous events and issues.
5) How stakeholders, including other levels of government, have responded to similar situations in the past.
6) What feedback received from wider stakeholders or community engagement activities would influence our risk tolerances and performance targets.

Every risk will require its own tolerance level to be set. This level may fluctuate over time as situations change, treatments are applied, events play out, or legislative change requires tolerances to be changed.

As the 'consequence' and 'likelihood' measures are applied the tolerance level is identified. The tolerance levels are:

1) Extreme Risk – Require immediate and on-going attention and actions by the Executive Leadership Team, and others associated to mitigate the risk occurring.
2) High Risk – Require frequent/regular Senior Management and Management attention and actions to mitigate the risk.

3) Moderate Risk – Require Management attention, with general Senior Management oversight, to address the risk treatments and monitor changes to ensure treatments are effective.
4) Low Risk – Require general Management oversight, with Coordinators and staff managing the risks with routine procedures.

Section 5.3.2 outlines the overall context Council considers in managing the organisation's broader risk appetite.

Risk Matrix

Each risk needs to consider first the 'likelihood' of it occurring, followed by the 'consequence' of it occurring, without any treatments in place. The Matrix in Appendix 1 provides criteria to consider when determining consequences and likelihood of various types of risk. All risks are to be analysed using the same risk criteria.

Each possibility is given a corresponding number. Lining up the number for the 'likelihood' and the number of the 'consequence' on the matrix will provide the 'inherent' rating of the risk prior to any treatment. These two numbers multiplied also provide the appetite/tolerance score on the matrix. The higher the score the greater emphasis required to reduce or remove the risk.

Consideration is then given to recording the different treatments that are either in place or can be implemented easily to mitigate the risk in full or part. Consider what can be done to:

1) Avoid
2) Control
3) Transfer; or
4) Finance the risk treatment.

A vast range of treatments can be considered and included to reduce the risk. Resources needed to make the required changes should be identified. Part of the risk tolerance needs to determine if the financial costs to reduce the risk, is greater than the 'value' of reducing the risk. This is also where the risk appetite for each risk will come into play.

Once the mitigation treatments have been determined, the risk is re-assessed to determine any changes to the likelihood and/or consequence. These are recorded and multiplied to determine the 'residual' risk and tolerance level once the treatments are considered.

Any treatments that are identified but are not yet in place, become a requirement for action.

Business Continuity Plan

Council needs to recognise that some risk is unavoidable and not within the ability of the organisation to completely manage these risks within an acceptable risk appetite. In many cases for these risks Council, including each Department, can only prepare and establish a business contingency plan for each Department, and the organisation. The business continuity plan needs to include relevant crisis management plans that can be activated as required. Testing of these plans periodically is essential to ensure they will be effective if/when a crisis occurs.

Crisis events could include natural disasters, terrorist events, loss of main office buildings, pandemics and/or loss of key staff.

Business continuity plans needs to consider various factors including:

1) Critical staff for key roles required during and/or after the crisis.
2) Staff that can be deployed to key areas.
3) Alternative venues to conduct business.
4) Interim technology solutions.
5) Interim payroll continuity.
6) Counselling and support for staff.
7) Potential partner organisations required during and/or after the crisis.

6.3 Risk Identification

The identification of individual risks involves generating a list of threats and opportunities based on events that might create, enhance, prevent, degrade, accelerate, or delay the achievement of the Council's strategic objectives, and/or Department's operational objectives. Follow-on impacts, cascading and cumulative effects should also be considered. Both factual and subjective information increase awareness of key risks.[12]

Key considerations when undertaking environmental scanning include:

1) The type of risk – political, legal, economic, environmental, socio-cultural, technological.
2) The source of the risk – external (political, economic, natural disasters), or internal (reputational, security, knowledge management).
3) The causes of the risk.
4) The impacts/effects of the risk – type of exposure (people, reputation, program/project results, priorities, funding, assets).
5) The level of control – the degree to which the agency can influence, affect, or manage the risk. [13]

Comprehensive identification is crucial, because a risk not identified at this stage will not be included in further analysis.[14]

Consider positive risks as opportunities worthy of identification. Also consider if any threats or challenges may be converted into opportunities if identified early.[15]

A list of potential sources of risk is detailed at the end of Appendix 3 – Key Element 3. Department managers may find this list useful when identifying their risks.

In identifying risks, it is important to articulate the risk as a short statement that may contain the 'cause' and the 'effect'. For example: 'project implementation failed due to inadequate preparation planning', or 'injuries to staff through inadequate health and safety practices', or 'reputational damage caused by adverse media'. Some statements may just contain the effect; however, it is best to articulate a cause wherever practical.

Often numerous risks can be identified; however it is important to refine many similar, or interrelated risks, into one decisive descriptive risk. Too many risks become cumbersome to manage and monitor. The intent is to identify the main significant risks likely to have the greatest impact on achieving the Council's, and/or Department's, objectives.

[12] A Guide to Risk Management – Queensland Treasury pages 18 version 1 updated 18/08/2020
[13] A Guide to Risk Management – Queensland Treasury pages 18 version 1 updated 18/08/2020
[14] Standards Australia, AS/NZS ISO 31000:2008 Risk management – principles and guidelines
[15] A Guide to Risk Management – Queensland Treasury pages 20 version 1 updated 18/08/2020

6.4 Risk Analysis

Risk analysis will use the two-step approach of assessing the 'inherent risk' before treatments are in place, and the 'residual risk' after treatments are actioned, as outlined above in 6.2 – Risk Matrix. The detailed Risk Matrix is contained in Appendix 1 – Risk Matrix, along with a checklist to consider under Appendix 3 – Key Elements 4 and 5.

Advantages of using this approach include:

1) Assisting management with identification of excessive or ineffective controls; and
2) Ensuring management is aware of the agency's exposure if the control fails.

Both inherent and residual risks will need to be re-assessed whenever the controls are adjusted, or environmental scanning indicates that circumstances may have changed.[16]

The analysis will identify what might happen if the risk event happens and any sources that identify how the risk may occur.

6.5 Risk Evaluation and Treatment

Once risks have been identified and analysed, they need to be evaluated to determine which risks require treatments and the priority to be applied to those treatments. This step in the process is the risk evaluation. Risks identified as 'High' or 'Extreme,' should be treated as the highest priority. 'Moderate' risks should be monitored for potential shifts.

In evaluating each risk consider:

1) The 'internal and external environment', with particular focus on the Council's strategic directions established as part of the 'setting the context stage'.
2) The 'risk appetite of the Council' established as part of the 'setting the context stage'.
3) The 'risk appetite of other stakeholders', including other government agencies, surrounding councils, members of the community, or others likely to be affected by the risk.
4) Any legal, regulatory, government guidelines or other requirements which may exists, particularly for higher priority risks if their probability of occurrence is high.
5) The cost / benefits of treating the risk.

Once evaluated, appropriate treatments need to be identified and actioned to reduce the risk to an acceptable level. Treatments can fit within four types of controls:

Treat the Risk

1) Preventative methods – designed to limit the possibility of an undesirable outcome being realised. The more important the undesirable outcome, the more important it is to implement appropriate preventative controls. Examples may include:
   a) Separation of duties.
   b) Installing security cameras to deter criminal activity.
   c) The use of contract terms and conditions to recover over-payments or safeguard against breaches of project over-runs.
2) Corrective controls – designed to correct undesirable outcomes which have been realised. Examples include:

[16] A Guide to Risk Management – Queensland Treasury pages 20 version 1 updated 18/08/2020

a) Rotating staff positions.
b) Internal audit review of preventative and detective controls.
c) Change to management procedures.

3) Directive controls – designed to ensure that a particular outcome is achieved. They are particularly important when it is critical that an undesirable event is avoided, particularly in health and safety. Examples include:
   a) A requirement that staff wear protective clothing.
   b) Staff are trained before working unsupervised.
4) Detective controls – designed to identify unfavourable events that have occurred. As they are 'after the event' controls they are only appropriate when it is possible to accept the loss or damage incurred. Examples include:
   a) Inventory and stocktakes.
   b) Bank reconciliations.
   c) Monitoring activities which detect changes that should be responded to.

Transfer the Risk

1) Risk transfer may be achieved by taking out insurance to facilitate financial recovery against the realisation of a risk, or by compensating a third party (potentially another agency) to take the risk because the other party is more able to effectively manage the risk. Risk may be wholly transferred, or partly transferred (that is, shared). For example:
   a) A Council may enter a shared purchasing scheme with other Council's, or an industry sector group, to offset costs for services that would be too costly for one Council on its own.

Terminate the Risk

1) Some risks may only return to acceptable levels if the activity is terminated. The opportunities to terminate an activity may be limited due to the nature of local government responsibility. That is, the Council may only be involved in delivering a service which is required for the public benefit because the associated risks are too great for the private sector to be involved.[17]

Take the Opportunity

1) There may be opportunities for Council to take advantage of a risk event. For example:
   a) The Council may identify that a reduction in over-the-counter payments may result in reduced opening hours. Opportunities, however, may arise where one Department could partner with another Department, or other agency such as Australia Post, to combine counter services (thus maintaining opening hours but reducing personnel costs) or transfer some of the resources to improve other areas of service delivery.

It may be appropriate, in some circumstances, to accept the risk rather than treat the risk. A risk may be accepted because:

1) The probability or consequence of the risk is low or minor.
2) The costs of treating the risk outweighs any potential benefit.
3) The risk falls within the agency's risk appetite and/or tolerance levels.
4) Whole-of-government policy requires acceptance of the risk.
5) The agency has limited or no control over the risk. These should be covered by a Business Continuity Plan.[18]

[17] A Guide to Risk Management – Queensland Treasury pages 21 version 1 updated 18/08/2020
[18] A Guide to Risk Management – Queensland Treasury pages 22 version 1 updated 18/08/2020

Risk Treatment Plans are incorporated into the Risk Register spreadsheets. This section of each spreadsheet will normally include:

1) The identification of the officers assigned responsibility for implementing the plan.
2) Proposed treatment actions and timeframes, including a cost-benefit analysis of alternatives.
3) The physical and human resource requirements to implement the actions.
4) Performance indicators that will be used to measure, review, and evaluate the effectiveness of the treatment/action.
5) Ongoing monitoring and reporting.[19]

Appendix 3 – Key Elements 5 and 6 can assist Managers in evaluating and treating the risks.

Council's Risk Register spreadsheets allows interrelated processes for the risk analysis, risk evaluation, risk treatment and review components, to be considered and recorded simultaneously. The Departmental Operational Risk Register/spreadsheet will be made available to Managers.

6.7 Monitoring and Review

The primary purpose of monitoring and review is to determine whether risks still exist, whether new risks have arisen, whether the likelihood or impact of risks have changed, and to re-assess the risk priorities within the internal and external context of the organisation. The result of monitoring the process also contributes to the review of the overall risk management framework.

When monitoring and reviewing the risks other organisational factors should be considered including:

1) The recommendations of internal audits associated with the functional area. Have these been actioned, are gaps still present, or have enduring changes been made?
2) Have all the relevant treatment plans been actioned? Are the changes to procedures being followed? Are these effective in mitigating the risk?
3) Are the risks considering any changes made to Council's directions in plans, policies or practices? Does this require an interim review of the risk and its treatment plan?

Appendix 3 – Key Elements 7 can assist Managers in monitoring and reviewing the risks.

Continuous improvement of the processes and framework will lead to improvements to the overall management of risk and the organisation's risk culture.

Extreme risks need to be monitored monthly to ensure the controls are working effectively. Any change in the environment that may elevate the likelihood of an event should be reviewed to determine if further controls are required. The Executive Leadership Team are to be alerted as soon as practicable by the responsible Manager if the likelihood of an event appears to be escalating.

High risks should be monitored every three to six months by the Manager. Any additional treatments implemented need to be assessed for their effectiveness and the risk register updated accordingly. This step may also include actioning Intern Audit recommendations that work towards reducing or eliminating risks.

[19] A Guide to Risk Management – Queensland Treasury pages 22 version 1 updated 18/08/2020

Moderate risks should be monitored on an annual basis, or more regularly if the environment shifts and the risk levels increase. Treatments should be considered for their effectiveness.

Low risks are to be monitored annually. Treatments should be considered for their effectiveness.

A six-month update to the Chief Executive Officer and Directors on extreme and high risks will keep them informed of the effectiveness of the risk management framework. They may require further information on changes to the strategic risks that are likely to disrupt the achievement of Council's objectives and plans and seek more details on a regular basis to monitor potentially escalating situations.

6.6 Communicate and Consult

Communication

An important requirement through each step of the process is to communicate the reason for risks to be identified and assessed, the process for doing so, discussing the effectiveness of treatments, and sharing the role to monitor trends, including changing environments that may in turn change the risk rating.

The communication component assists in identifying who should be consulted. Consultation supports determining the nature of each risk with the people involved. They can identify potential risks and opportunities.

All staff, based on their role, require an understanding of the organisation's risk strategy, what the priorities are and how their role and responsibilities fit within that framework. They need to be involved in identifying, analysing, managing, and reporting on risks.

Consultation

Internally, risk communication promotes action, continuous learning, innovation, and teamwork. It can demonstrate how management of a localised risk contributes to the overall achievement of the Council's Corporate Plan.

External stakeholders, including contractors, other government agencies, local businesses, specialists, interest groups and community members, can also provide information about risks that may affect the organisation. They may also be able to assist in managing some of the known risks.

Reporting

To be effective, formal communication through structured reports helps to close the loop in the process steps. It also ensures the significant risks are repeatedly brought back to the attention of the CEO, Directors, and Council. A report by the CEO to Council annually will focus consultation at a strategic level with Councillors so that the annual Internal Audit Plan, Operational Plan and Budget can take into consideration a current risk profile of the organisation.

The communication, consultation and reporting elements are a critical component in building a pro-active, balanced, organisational risk management culture.

Appendix 3 – Key Elements 8 can assist the Executive Leadership Team and Managers to communicate and consult on their strategic and operational risks.

Appendix 1 – Risk Matrix

Risk Assessment Matrix									
Risk Acceptance / Tolerance Levels				Consequences of Event					
Level of Risk	Delegation	Acceptance / Tolerance Level	Review Period	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)	Event
Extreme Risk	CEO / Directors Immediate Action Required	Exposure to this risk level requires immediate and critical attention to reduce or mitigate the risk.	Review period should not exceed 1 month	Negligible impact of Council, brief service interruption for several hours to a day.	Temporary and recoverable failure of council causing intermittent service interruption for several days.	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service interruption for a week.	Widespread failure to deliver several major strategic objectives and service plans. Long-term failure of Council causing lengthy service interruption	The continuing failure of Council to deliver essential services. The removal of key revenue generation	Operational / Business Continuity
High Risk	Director / Manager Senior Management Attention Required	Exposure to this risk level requires attention to reduce or mitigate the risk.	Review period should not exceed 3 to 6 months	Brief, non-hazardous, transient pollution or damage.	Minor environmental damage such as remote temporary pollution.	Moderate impact on the environment; no long term or irreversible damage. May incur cautionary notice or infringement notice	Severe environmental impact requiring significant remedial action. Penalties and/or direction or compliance order incurred.	Widespread and irreversible environmental damage attributed by the courts to be negligent or incompetent actions of Council.	Environmental
Moderate Risk	Manager Management responsibility must be specified	Acceptable with periodic reviews.	Review period should not exceed 12 months	Damage where repairs are required however equipment still operational	Minor loss/damage. Repairs required	Short to medium term loss of key IT network/hardware	Widespread, short to medium term loss of IT network/hardware	Widespread, long-term loss of IT network/hardware.	Information Technology
Low Risk	Coordinator / Staff Member Manage by routine procedures	Acceptable with periodic reviews. Exposure to this risk level is acceptable without additional risk treatments.	Review period required every 12 months	Transient matter, e.g. Customer complaint, resolved in day-to-day management. Isolated matter no reputational impact Negligible impact from another local government.	Minor local community concern manageable through good public relations. Short term localised reputational impact Adverse impact by another local government.	Significant statewide concern/ exposure and short to mid-term loss of support from Shire residents and reputational damage State-wide media exposure Adverse distraction to service provision Adverse impact and intervention by another local government & LGAQ.	State media and public concern/ exposure with adverse attention and long-term reputational damage and loss of support from Goondiwindi Regional Council residents. National media exposure. Significant distraction to service provision Adverse impact and intervention by State Government	Loss of State Government support with scathing criticism and removal of the council. National media exposure. Loss of power and influence restricting decision making and capabilities. Perpetual community anger negatively influencing multiple Council elections.	Reputational / Political / Engagement

				Minor breaches of policies, procedures rules or regulations with negligible impact.	Breaches of policies, procedures, rules, or regulations that are isolated with limited legal or regulatory impact.	Breaches of policies, legislation or regulations that are systemic or likely to result in legal or regulatory action.	Breaches of policies, regulations or laws that will result in legal or regulatory action including investigations and/or significant penalties.	Breaches of policies, regulations or laws that will result in significant penalties, loss of funding, significant legal implications /costs and/or criminal investigations.	Strategic / Corporate Governance and Compliance
				Staff issues cause negligible impact of day-to-day service delivery	Staff issues cause several days interruption of day-to-day service delivery	Staff issues cause failure to deliver minor strategic objectives and temporary and recoverable failure of day-to-day service delivery.	Staff issues cause widespread failure to deliver several major strategic objectives and long-term failure of day-to-day service delivery.	Staff issues cause continuing failure to deliver essential services	Human Resources
				Damage where repairs are required, facility or infrastructure is still operational	Minor loss/damage. Repairs required	Short to medium term loss of key assets and infrastructure	Widespread, short to medium term loss of key assets and infrastructure.	Widespread, long-term loss of substantial key assets and infrastructure.	Infrastructure, Assets and Property
				No injury.	First aid treatment. No lost time.	Medical treatment. Lost time of up to 4 working days.	Extensive injuries. Lost time of more than 4 working days.	Fatality or significant irreversible disability.	Workplace Health and Safety
APPLY ALARA - As Low as Reasonably Possible				Less than 2 % of annual revenue (excluding capital revenue) ($48.3M) = $ 9.66K 2023/24	Between 2-6% of annual revenue (excluding capital revenue) ($48.3M) = $ 9.66K 2023/24	Between 6-10% of annual revenue (excluding capital revenue) ($48.3M) = $ 9.66K 2023/24	Between 10-20% of annual revenue (excluding capital revenue) ($48.3M) = $ 9.66K 2023/24	Above 20% of annual revenue (excluding capital revenue) ($48.3M) = $ 9.66K 2023/24	Financial & Economic
Likelihood of occurring				Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)	
	Almost Certain (5)	Event may occur within one year	The event is expected to occur in most circumstances	Moderate (5)	High (10)	High (15)	Extreme (20	Extreme (25)	
	Likely (4)	Event may occur in every 1 - 2 years	The event will probably occur in most circumstances	Moderate (4)	Moderate (8)	High (12)	High (16)	Extreme (20)	
	Possible (3)	Event may occur once in every 2-5 years	The event should occur at some time	Low (3)	Moderate (6)	High (9)	High (12)	High (15)	
	Unlikely (2)	Event may occur in every 5 - 10 years	The event could occur at some time	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)	
	Rare (1)	Event may occur once in every 10+ years	The event may only occur in exceptional circumstances	Low (1)	Low (2)	Moderate (3)	Moderate (4)	High (5)	

Appendix 2 – Risk Management Action Plan – 2023-2025

This action plan provides a mechanism for the oversight and conduct of risk management within Goondiwindi Regional Council for the next two years. It is aimed at raising awareness, identifying the key strategic and operational risks and promoting a balanced approach to managing risks.

The Risk Management Action Plan is designed to work concurrently with the Fraud and Corruption 2023-2025 Action Plan, allowing assessment of these interrelated functions of Council.

For the financial year 2023/2024 and 2024/2025, it is proposed to complete the following actions.

	Schedule	Strategy	Actions	Completion Timeline
1	July to December 2023	Prevention	Develop Council's *Enterprise Risk Management Framework*.	By 31 October 2023
2		Prevention	The *Enterprise Risk Management Framework* to be finalised and presented to Council for consideration and adoption following a process of review and refinement.	Presented to Council for adoption by 31 December 2023

	Schedule	Strategy	Actions	Completion Timeline
1	January to December 2024	Prevention	The Councillors Induction/Transition Program shall include awareness and understanding of the *Enterprise Risk Management Framework 2023-2025*, including the *Fraud and Corruption Prevention Framework 2023-2025*.	Councillors inducted in Risk and Fraud by 30 June 2024.
2		Prevention	A corporate staff induction and staff training program for new staff and existing staff to be developed. Inclusions as a minimum to include: • Code of Conduct, • conflicts of interest, • fraud and risk management, • OH&S, • use of Council equipment • information technology, • receipt of gifts and hospitality, and • reporting requirements. Other additional induction and training such as learning and development, role specific training, systems training would be provided based on the position.	By 30 June 2024

3		Prevention	The Council elected in March 2024 is required to review and adopt the following Councillor related risk management policies including: • Councillor Code of Conduct • Councillor Remuneration and Expenses Policy • Councillor Travel and Attendance Policy • Entertainment and Hospitality Policy • Gifts and Benefits Policy (new policy) • Councillor Contact with Lobbyists, Developers and Submitters Policy.	Councillors to review policies scheduled for consideration and adoption by 31 December 2024
4		Detect	Council to respond promptly to any Auditor-General's audit findings and recommendations.	By 30 June 2024
5		Monitor and Review	Executive Leadership Team to respond promptly to internal audit findings and recommendations, particularly those listed as high risk, and review the list of outstanding items annually as a minimum.	Following each audit report and then annually for the full list
6		Review	Consider high risk and high fraud areas, as important aspects to determine the Annual Internal Audit Plan	By 30 June annually

	Schedule	Strategy	Actions	Completion Timeline
1	Annually or as scheduled	Prevention	Executive Leadership Team and Council to review the *Enterprise Risk Management Framework* and the *Fraud and Corruption Prevention Framework* to identify refinements or changes. Amend, re-adopt and publish on Council's website.	By the end of their designated framework term. Initially this will be by 31 December 2025.
2		Prevention	The Council to review and adopt the following Councillor related risk management policies including: • Councillor Travel and Attendance Policy • Entertainment and Hospitality Policy • Gifts and Benefits Policy (new policy – consider conjoining with Entertainment and Hospitality Policy). • Risk Management Policy and Framework	Councillors to review policies and schedule these for consideration and adoption in accordance with their scheduled review date.

			• Fraud and Corruption Policy and Framework	
3		Prevention	Every position description needs to contain a statement requiring clear risk accountability and reporting responsibilities. Each position description being reviewed should be updated to include the statement if missing	Position descriptions to be updated prior to advertising positions.
4		Prevention	All staff to undertake corporate training in the following areas as a minimum: Code of Conduct, conflicts of interest, fraud and risk management, OH&S, use of Council equipment and information technology, receipt of gifts and hospitality, and reporting requirements.	By 30 June every two years
5		Monitor and review	Executive Leadership Team to respond promptly to internal audit findings and recommendations, particularly those listed as high risk, and review the list of outstanding items annually as a minimum.	Following each audit report and then annually for the full list
6		Review	Consider high risk and high fraud areas, as important aspects to determine the Annual Internal Audit Plan	By 31 May annually
7		Monitor and review	CEO to provide an update to Council on the management of risk and prevention of fraud and corruption.	Annually

Appendix 3 – Risk Management Framework Checklist

The following checklists are sourced from the Queensland Treasury – *A Guide to Risk Management Version 1 – 18/06/2020*. They are provided for government agencies to use as a guide. Some questions may not be relevant for every Department; however Managers are encouraged to consider the intent of each question and how it may be applicable to their risks.

Key Element 1 – Risk Management Framework

Question	Yes	No	N/A
• Has the accountable officer or statutory body developed and implemented a robust risk management framework appropriate to the size of their agency?	❑	❑	❑
• Does the agency have the necessary policies and procedures in place to support risk management?	❑	❑	❑
• Does the agency ensure all staff are informed of the risk management framework?	❑	❑	❑
• Does the agency have an explicitly stated risk management policy that complements their vision and strategic objectives?	❑	❑	❑
• Is there a designated risk management champion or unit to oversee the implementation of integrated risk management?	❑	❑	❑
• Does risk management have the demonstrated support and ongoing attention of executive management?	❑	❑	❑
• Does the agency have a risk management committee, or similar?	❑	❑	❑
• Is risk management communicated, understood, and applied throughout agency processes?	❑	❑	❑
• Is risk management integrated into existing governance and decision-making structures and performance-reporting systems?	❑	❑	❑
• Have control and accountability systems been adapted to account for risk management processes?	❑	❑	❑
• Have key performance indicators and critical success factors been identified and included in agency reports?	❑	❑	❑
• Does reporting on risk and risk management take place through existing management processes (e.g. performance reporting, ongoing monitoring, appraisals, internal auditing)?	❑	❑	❑
• Has the agency put in place effective initiatives to build risk management awareness?	❑	❑	❑
• Is written guidance (framework, policy, or operating principles) communicated throughout the agency to support individual units in building risk management into day-to-day operations?	❑	❑	❑

Question	Yes	No	N/A
• Is the risk management process integrated into strategic and operational planning?	❑	❑	❑
• Does the agency identify and encourage education, training and development in risk management?	❑	❑	❑
• Is the risk management framework reviewed at least annually?	❑	❑	❑
Notes:			

Key Element 2 – Establishing the Context

Question	Yes	No	N/A
• Has the agency implemented appropriate processes to identify both the internal and external context within which the agency operates (for example, use of environmental scanning)?	❑	❑	❑
• Has the risk been established with reference to the agency's objectives and strategic planning?	❑	❑	❑
• In determining the context, has the agency considered both challenges and opportunities?	❑	❑	❑
• Does the agency's environmental scanning process include a wide range of influences, trends and time horizons?	❑	❑	❑
• Does the agency consider both its external and internal contexts in relation to risk management?	❑	❑	❑
• Has the agency determined and documented its risk tolerances for the various components of its environment?	❑	❑	❑
• Is the context regularly reviewed to ensure it remains correct/appropriate to the agency's systems or controls?	❑	❑	❑
• Has the agency determined appropriate risk criteria that align with its objectives?	❑	❑	❑
<u>Agency-level risks</u>			
• Have the objectives of individual projects been considered as part of the risk management context?	❑	❑	❑

Question	Yes	No	N/A
• Has the agency considered its capabilities and capacities (for example, funding, staff and technology)?	❑	❑	❑
Cross-agency risks			
• Does the agency consider the risk management practices of other agencies with which it delivers services?	❑	❑	❑
• Does the agency consider cross-agency risks and communicate these risks with relevant agencies?	❑	❑	❑
Whole-of-Government risks			
• Does the agency consider the wider political and public sector environment?	❑	❑	❑
• Does the agency consider strategic risk issues (for example, climate change) that require coordination with other relevant agencies?	❑	❑	❑
• Does the agency consider the potential impact of risks on industry and the community?	❑	❑	❑
Notes:			

Key Element 3 – Risk Identification

Question	Yes	No	N/A
• Are risks identified with reference to the agency's strategic plan, that is, the objectives and deliverables of the agency?	❑	❑	❑
• Are risks identified with reference to the agency's operational plans?	❑	❑	❑
• Are risks identified with reference to the agency's program and project plans?	❑	❑	❑
• Is risk identification linked to whole-of-Government policy and stakeholders?	❑	❑	❑
• Does the agency consider risks at the agency, cross-agency and whole-of-Government levels?	❑	❑	❑
• Does the agency identify both challenges and opportunities?	❑	❑	❑
• Does the agency consider both internal and external risks?	❑	❑	❑
• Does the agency have ongoing, comprehensive and systematic processes for identifying risks?	❑	❑	❑
• Are identified risks recorded in a risk register?	❑	❑	❑
• Are the staff involved in risk identification knowledgeable about the process or activity being reviewed and about the risks that must be managed as part of that activity?	❑	❑	❑
• Does risk identification involve appropriate stakeholders?	❑	❑	❑

Question	Yes	No	N/A
• Are strategic risks sourced from/reflected in the agency's strategic plan?	❑	❑	❑
<u>Agency-level risks</u>			
• When identifying risks, does the agency consider the findings from past audits, evaluations and other assessments?	❑	❑	❑
• Does the agency review relevant corporate records to determine if a pattern exists (for example, financial or property losses, data/record losses, workplace health and safety reports)?	❑	❑	❑
• Does the agency consider risks identified from past learning?	❑	❑	❑
• Does the agency undertake a gap analysis (that is the difference between existing practice and strategic plans, policies and practices)?	❑	❑	❑
<u>Cross-agency risks</u>			
• Does the agency consider how risks within the agency may affect other agencies?	❑	❑	❑
• Does a cross-agency committee assess risks associated with joint projects?	❑	❑	❑
• Is there a process for notifying relevant stakeholders of cross-agency risks?	❑	❑	❑
Notes:			

Potential Source of Risk

Agency risk	Cross-agency risk	Whole-of-Government risk
○ policy and strategy	○ policy and strategy	○ policy and strategy
○ agency reputation	○ agency reputation	○ political factors
○ political factors	○ political factors	○ machinery of Government changes
○ machinery of Government changes	○ machinery of Government changes	○ public expectations
○ public expectations	○ public expectations	○ stakeholder relations
○ stakeholder relations	○ stakeholder relations	○ media relations
○ media relations	○ media relations	○ changing demographics
○ industry developments	○ industry developments	○ globalisation
○ changing demographics	○ program activities	○ security threats
○ globalisation	○ program delivery	○ terrorism
○ security threats	○ service delivery	○ emergency preparedness
○ terrorism	○ major projects	○ natural disasters
○ business continuity	○ structure and reporting relationships	○ economic trends
○ emergency preparedness	○ planning and priority setting	○ competitive trends
○ technology trends	○ project management	○ service delivery
○ competitive trends	○ environmental protection	○ major projects
○ business line activities	○ accountability	○ budgeting and resource allocation
○ program activities	○ transparency	○ financial management
○ program delivery	○ natural disasters	○ performance management
○ service delivery		○ project management
○ alliances, partnerships		○ environmental protection
○ major projects		○ security, privacy and confidentiality
○ structure and reporting relationships		○ legal liabilities and litigation
○ planning and priority setting		○ accountability
○ budgeting and resource allocation		○ transparency
○ expenditure management		○ Whole-of-Government reputation
○ revenue and cost recovery		
○ procurement and contracting		
○ financial management		

Agency risk	Cross-agency risk	Whole-of-Government risk
○ performance management ○ project management ○ change management ○ inventory management ○ asset management ○ human resources ○ information and knowledge ○ information technology ○ communications ○ statutory reporting ○ compliance with laws, regulations and policies ○ agreements and contractual obligations ○ workplace health and safety ○ environmental protection ○ security, privacy and confidentiality ○ legal liabilities and litigation ○ accountability ○ transparency ○ natural disasters		

Source: Based on examples provided in Treasury Board of Canada Secretariat, Integrated Risk Management Implementation Guide

Key Element 4 – Risk Analysis

Question	Yes	No	N/A
• Does the agency have documented procedures to analyse the likelihood and consequence of each risk?	❑	❑	❑
• Does the agency conduct appropriate analysis of the nature and extent of the causes and impacts of the risks?	❑	❑	❑
• Are all risks analysed using a consistent methodology?	❑	❑	❑
• Are risk analyses adequately documented?	❑	❑	❑
• Has the agency examined and evaluated existing controls for the identified risks in terms of their strengths and weaknesses?	❑	❑	❑
• Are risk management controls regularly monitored?	❑	❑	❑
• Are appropriate levels of management and employees involved in the risk analysis process?	❑	❑	❑
• Does risk analysis include ensuring that the agency is not 'over-controlled' for the risks it faces?	❑	❑	❑
Notes:			

Key Element 5 – Risk Evaluation

Question	Yes	No	N/A
• Are risks found during the analysis process compared with the risk profile, risk appetite and risk tolerance established when the agency context was considered?	❑	❑	❑
• Has the agency fully integrated risks into their strategic and operational plans or established risk treatment plans for the management of risks, where necessary?	❑	❑	❑
• Are all risks within the agency evaluated using a consistent methodology?	❑	❑	❑
• Are evaluated risks prioritised to ensure treatment of the highest risks is considered first?	❑	❑	❑
• Are evaluated risks reviewed by an independent person to ensure risks are treated consistently?	❑	❑	❑
• Are risks re-evaluated over time to determine if priorities need to change?	❑	❑	❑
• Are risks reviewed or evaluated as part of the agency's own strategic and operational planning processes?	❑	❑	❑
Notes:			

Key Element 6 – Risk Treatment

Question	Yes	No	N/A
• Are risks treated in accordance with the pre-determined risk criteria established by the agency?	❑	❑	❑
• Do proposed risk treatment plans include cost/benefit analyses of alternative courses or action?	❑	❑	❑
• Is the managing of risks and associated controls assigned to particular officers within the agency?	❑	❑	❑
<u>Agency-level risks</u>			
• Does the agency have formal, documented contingency plans for disaster recovery and business continuity?	❑	❑	❑
• Does the agency regularly review and test risk controls and contingency plans?	❑	❑	❑
• Are internal controls developed and documented to treat identified risks?	❑	❑	❑
<u>Cross-agency risks</u>			
• Does the agency have contractual agreements in place to manage cross-agency projects and their related risks?	❑	❑	❑
• Is there collaboration between agencies to agree risk treatments attached to identified cross-agency risks?	❑	❑	❑
• Are processes in place to ensure cross-agency risks and risk treatments are monitored over time?	❑	❑	❑
• Are Treasury and DPC informed of risk treatments, particularly if there are budget or policy implications?	❑	❑	❑

Question	Yes	No	N/A
Whole-of-Government risks			
• Is there collaboration between agencies to agree on risk treatments attached to whole-of-Government risks?	❑	❑	❑
• Are processes in place to ensure whole-of-Government risks and risk treatments are monitored over time?	❑	❑	❑
• Are Treasury and DPC informed of risk treatments, particularly if there are budget or policy implications?	❑	❑	❑
• Have strategic risks been assigned specific risk treatments and are these shared with other agencies?	❑	❑	❑
Notes:			

Key Element 7 – Monitoring and Review

Question	Yes	No	N/A
• Does the agency have a regular monitoring and review process to evaluate the:	❑	❑	❑
○ relevance of the risks to the achievement of the agency's objectives?	❑	❑	❑
○ effectiveness of existing governance controls?	❑	❑	❑
○ application of risk treatment plans in practice?	❑	❑	❑
○ continuing relevance of the risk treatment plans to the agency's strategic and operational objectives?	❑	❑	❑
• Does the agency have policies and procedures in place for the reassessment of its risk profile and the opportunities provided by changes to the agency's internal and/or external environments?	❑	❑	❑
• Are adequate management information systems in place to facilitate risk monitoring and review requirements?	❑	❑	❑
• Is risk appetite assessed in light of changing circumstances (for example, at regular intervals, as well as at trigger points such as a State election)?	❑	❑	❑
• Are higher rated risks and associated current controls, and new controls/treatments reviewed regularly?	❑	❑	❑
<u>Agency-level risks</u>			
• Is there regular reporting of the status of risks (for example, to senior or executive management, risk management committee)?	❑	❑	❑

Question	Yes	No	N/A
• Does the Head of Internal Audit (where established) provide assistance in risk management and identifying deficiencies in risk management? (refer section 78 of the *Financial Accountability Act 2009*)	❑	❑	❑
• Does the internal audit unit undertake regular reviews of the risk management process?	❑	❑	❑
<u>Cross-agency risks</u>			
• Do processes exist to ensure ongoing monitoring and reporting of cross-agency risks?	❑	❑	❑
<u>Whole-of-Government risks</u>			
• Do processes exist to ensure ongoing monitoring and reporting of whole-of-Government risks?	❑	❑	❑
• Are strategic risks reviewed and evaluated through engaging appropriate processes such as environmental scanning?	❑	❑	❑
• Are the results of any strategic risk review process shared with other agencies facing similar risks?	❑	❑	❑
Notes:			

Key Element 8 – Communication and Consultation

Question	Yes	No	N/A
• Are all staff aware of their responsibilities with respect to risk identification, treatment and management?	❑	❑	❑
• Does the agency's risk management framework promote continuous improvement through learning and innovation?	❑	❑	❑
• Within the risk management framework, is there a process to ensure all stakeholders are identified?	❑	❑	❑
• Where appropriate, is a communication plan developed (for example, where a large number of stakeholders are involved)?	❑	❑	❑
• Are all key stakeholders consulted throughout the risk management cycle?	❑	❑	❑
• Are stakeholder perceptions of risk addressed?	❑	❑	❑
• Does the agency have processes to obtain input from Ministers and/or Cabinet on risks, their treatment and the Government's appetite for risk?	❑	❑	❑
• Are the agency's risks discussed regularly with Department of the Premier and Cabinet and Treasury?	❑	❑	❑
<u>Agency-level risks</u>			
• Is there regular communication between the Head of Internal Audit and the risk management committee (or equivalent)?	❑	❑	❑

Question	Yes	No	N/A
• Does the risk management champion have direct access to the risk management committee (or equivalent) to raise concerns?	❑	❑	❑
• Is there a risk management reporting system in place that ensures all relevant parties are kept informed of the risks faced by the agency?	❑	❑	❑
<u>Cross-agency risks</u>			
• Are effective communication strategies implemented for cross-agency risks (for example, multi-agency committees, and regular executive management forums)?	❑	❑	❑
• Do risk management champions communicate with their counterparts in other agencies?	❑	❑	❑
• Does the lead agency advise the appropriate risk analysis matrix to be followed for the cross-agency risk, and establish clear lines of communication and consultation?	❑	❑	❑
<u>Whole-of-Government risks</u>			
• Does the agency have processes to ensure Ministers and/or Cabinet are informed of high-risk or whole-of-Government risks?	❑	❑	❑
• Are effective communication strategies implemented for whole-of-Government risks (for example, multi-agency committees, and regular executive management forums)?	❑	❑	❑
• Do risk management champions communicate with their counterparts in other agencies?	❑	❑	❑
Notes:			