7.6. RISK MANAGEMENT FRAMEWORK, RISK APPETITE STATEMENT AND CORPORATE RISK REGISTER

REPORT AUTHOR	Governance and Information Officer
EXECUTIVE	General Manager Corporate and Communities
DEPARTMENT	Corporate and Communities
TEAM	Governance
DATE	27 July 2026

RECOMMENDATION

That Council adopt the Risk Management Framework, Risk Appetite Statement and Corporate Risk Register.

EXECUTIVE SUMMARY

The Risk Management Framework, Risk Appetite Statement and Corporate Risk Register are an integral component of Council's Enterprise Risk Management Framework (ERMF). These key documents will enable Council to identify, discuss, mitigate, and monitor its corporate risks in a balanced and proactive manner.

PREVIOUS COUNCIL CONSIDERATIONS / RESOLUTIONS

There are no previous council considerations associated with this report.

REPORT / BACKGROUND

Council's philosophy towards risk is not to be unduly risk averse. Council is committed to establishing and integrating its ERMF and processes to support this philosophy without creating an unnecessary burden on the business.

Council began an uplift of its risk management approach in 2025 to align with contemporary practice, ISO 31000 principles, and sector expectations: integrated, aligned to the organisational business, transparent, and evidence based.

The development of the ERMF has been guided by the following:

- ISO 31000 incorporating risk identification, analysis, evaluation, treatment, monitoring, and reporting.
- Top down and bottom-up integration, beginning with strategic risks, then corporate risks, and operational/business unit risks to ensure full organisational coverage.

- Control based assessment to evaluate inherent versus residual risk and to understand the effectiveness of current controls.

- Consultative design, recognising that risk ownership and capability uplift must be shared across ELT, SLT, and business units across Council.

- Continuous improvement orientation, enabling the framework to evolve as Council's governance, systems, and external operating environment mature.

FINANCIAL AND RESOURCE IMPLICATIONS

Robust risk and audit assurance underpins and sustains Council's service-delivery and financial sustainability goals. The development of these key ERMF documents provides staff with guidance and structure when undertaking their risk management obligations and activities. Risk management activities are to become embedded in core business-as-usual for management and staff and as such are funded and resourced within baseline Operating and Capital Budgets.

RISK MANAGEMENT IMPLICATIONS

This work will establish clear, measurable risk boundaries for Council and guide decision making, investment prioritisation, and strategic planning.

ENVIRONMENTAL IMPLICATIONS

There are no environmental implications associated with this report.

SOCIAL IMPLICATIONS

There are no social implications associated with this report.

CORPORATE AND OPERATIONAL PLAN

This report has been prepared in accordance with the following:

Corporate Plan 2025-2030 Initiatives:

Theme 3 - Service Delivery
We deliver Council services effectively and efficiently to meet community expectations, focusing on the wellbeing of both the community and our employees.
3.7 - *Identify and manage risk.*

Operational Plan 2026-2027 Actions:

Legislative requirement.

LEGISLATION AND POLICY

- *Local Government Act 2009.*
- *Local Government Regulation 2012.*
- Enterprise Risk Management Policy.

CONSULTATION

Internal Consultation:

- Elected members
- Members of the Executive Leadership Team and Senior Leadership Team.

External Consultation

- Endorsement by the external members of the Audit and Risk Committee.

CONCLUSION

It is the recommendation for the Ordinary meeting that Council adopt the Risk Management Framework, Risk Appetite Statement and Corporate Risk Register.

ATTACHMENTS

1. Risk Management Framework [**7.6.1** - 15 pages]
2. Risk Appetite Statement [**7.6.2** - 9 pages]
3. Strategic and Corporate Risk Register [**7.6.3** - 4 pages]

DOUGLAS SHIRE COUNCIL

Risk Management Framework

RISK MANAGEMENT FRAMEWORK

Contents

1. Purpose and Scope

This Framework sets out how Douglas Shire Council (Council) identifies, assesses, treats, monitors, and reports risk to achieve strategic objectives and comply with legislative requirements and deliver best practice.

It applies to all Councillors, employees, volunteers, contractors, and committees. It integrates risk into strategy, planning, projects, disaster management, procurement, asset management, WHS, cyber-security/privacy, and financial stewardship in line with ISO 31000:2018 principles, framework, and process.

2. Council's Philosophy and Commitment

Council's risk management adheres to ISO 31000 principles—creating and protecting value, being integrated, structured, inclusive, dynamic, informed by best information, and continuously improved.

For disaster risks, Council adopts the Emergency Management Assurance Framework (EMAF) principles (public safety, leadership, partnership, performance) across prevention, preparedness, response, and recovery (PPRR).

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.

2.1 Goals and Objectives

Council will apply a Framework which will:

- Incorporate a consistent, systematic process to identify, analyse, mitigate, and monitor the key strategic, operational, financial, environmental, and compliance risks impacting on Council.
- Align risk management with business objectives identified in Council's corporate plans and annual operational plans.
- Integrate and align existing risk systems to ensure no duplications or overlap.
- Ensure integration of information systems used for reporting on risk to enable aggregation and reporting at a corporate level.
- Allow the necessary controls and policies to be implemented to deliver an appropriate approach to governance and best practice.
- Embed a culture of risk management throughout Council.

2.2 Governance, Roles and Accountabilities

Mayor

- Provides strategic leadership and supports good governance.

Council (Elected Members)

- Set tone and direction: endorse this Framework, Risk Appetite & Tolerance statements, Corporate Plan risk references, and material risk reports.

- Oversee compliance with relevant Acts and standards and hold management to account for risk performance.

Chief Executive Officer (CEO)

- Accountable for implementing the Framework, ensuring resources, capability, and monitoring systems exist across Council. Ensures the internal audit plan addresses key operational risks and controls.

Executive Leadership Team (ELT)

- Own enterprise risks; approve risk registers; ensure WHS due diligence processes.

Audit and Risk Committee (ARC)

- Provide independent oversight of risk, internal controls, internal audit, external audit matters, and improvement actions. Review risk maturity progress.

Business Units and Project Leads (First Line)

- Identify, assess, and manage operational and project risks; update registers; embed controls; escalate issues.

Coordinator Governance, Strategy and Risk (Second Line)

- Maintain this Framework, enterprise risk registers, methodology, risk reporting, and alignment to ISO 31000 and Queensland Treasury guidance. Coordinate internal audit planning with key risks.

Internal Audit (Third Line)

- Independently assess adequacy/effectiveness of controls and risk processes, report to ARC, and meet LGR 2012 s207 obligations.

Local Disaster Management Group (LDMG)/Disaster Management Unit

- Maintain LDMP and sub-plans, conduct training/exercises, and drive continuous improvement.

2.3 Risk Appetite and Tolerance

Council articulates qualitative appetite and quantitative tolerance by risk category. Appetite/tolerance calibrates decision rights, escalation, and residual risk acceptance thresholds. Best practice calls for clear appetite statements and dashboards to monitor breaches/exceedances.

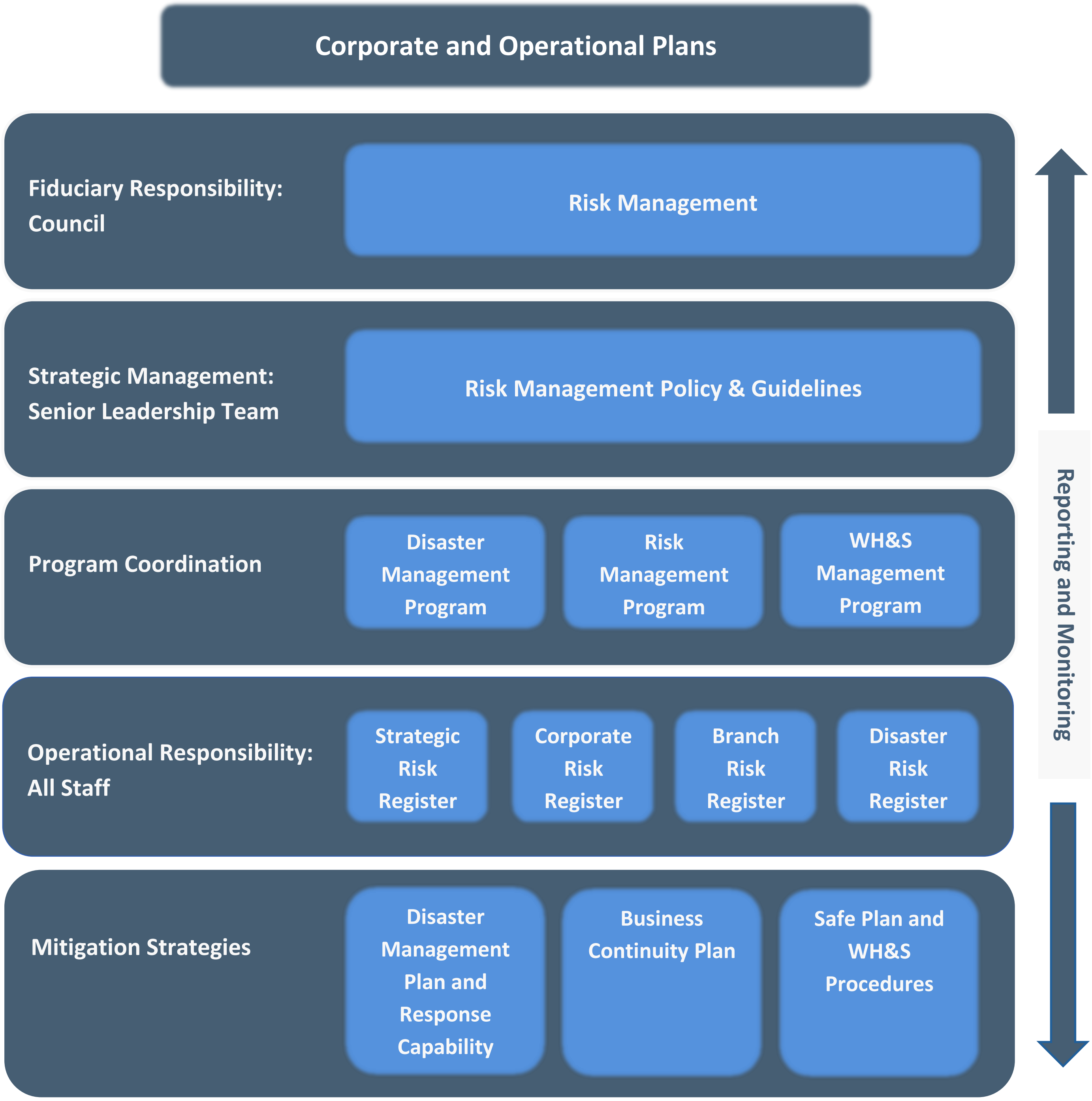
Council has adopted a risk appetite statement.

2.4 Risk Registers

Council's risk register is the key data source and tool for the management of identified risks and facilitates structured reporting. There are three types of risk recorded in the register being Strategic, Corporate and Business Unit.

3. Risk Management Framework

The Risk Management Framework explains the relationship between Council's risk management components and other management systems and frameworks.


Corporate and Operational Plans
Fiduciary Responsibility: Council
Risk Management
Strategic Management: Senior Leadership Team
Risk Management Policy & Guidelines
Program Coordination
Disaster Management Program
Risk Management Program
WH&S Management Program
Operational Responsibility: All Staff
Strategic Risk Register
Corporate Risk Register
Branch Risk Register
Disaster Risk Register
Mitigation Strategies
Disaster Management Plan and Response Capability
Business Continuity Plan
Safe Plan and WH&S Procedures
Reporting and Monitoring

4. The Risk Management Process

The risk management process provides guidance to officers in undertaking their risk management activities.

The process followed by Council to manage risks is in accordance with AS/NZS ISO 31000: 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).

COUNCIL'S RISK MANAGEMENT PROCESS

4.1 Establish Context

Stage one of the process establishes the strategic, organisational and risk management context in which the rest of the process will take place. This includes the criteria against which risk will be evaluated, the risk appetite assigned, and corrective actions determined.

In considering context, it is necessary to consider the broader external environment in which Council operates and not just internal matters.

Action

Define internal/external context, stakeholders, objectives, regulatory constraints, and criteria (scales, matrix, appetite/tolerance).

4.2 Risk Identification

At this stage, Council identifies what, why and how things can arise, that may affect the organisation, as the basis for further analysis. This is done at both strategic and operational levels of Council.

Action

Identify events, causes and consequences using workshops, data, incident reviews, audits, KRIs, disaster risk studies, climate models, cyber-security threat intel, and privacy impact assessments.

4.3 Risk Analysis

This stage determines the inherent risks and then calculates any residual risks taking into consideration any existing controls in place (existing processes and procedures). Risks are analysed in terms of consequence and likelihood in the context of those controls. The analysis will consider the range of potential risk exposure consequences and how likely those consequences are to occur.

The consequence and likelihood are then combined to produce an estimated level of risk known as the Overall Risk Rating.

Action

Using the adopted risk assessment tools assess consequence and likelihood considering existing controls; evaluate uncertainty and interdependencies; quantify where feasible; include WHS reasonably practicable tests and privacy harm considerations.

4.4 Risk Evaluation

Risks need to be evaluated and prioritised to ensure that management effort is directed toward resolution of the most significant organisational risks first. The initial step in this Risk Evaluation stage is to determine the effectiveness, and or existence of, controls in place to address the identified risks.

Action

Compare analysed risk to appetite/tolerance and legal minimums (e.g., WHS, privacy, disaster). Decide to retain, control, avoid or transfer the risk.

4.5 Risk Treatment

Following the process of identification, analysis and evaluation of risks and controls, the outcomes are to be communicated with all relevant stakeholders and agreements reached with the various risk owners prior to being documented in the Risk Register.

Action

Select proportionate controls (preventive, detective, corrective) and embed assurance lines (1st/2nd/3rd).

4.6 Monitoring and Review

This stage establishes a process to monitor and review the performance of the risk management system implemented and changes that might affect the performance or give rise to new risks that will require assessment.

Both monitoring and review are a planned part of the risk management process and tailored to the needs of Council and the significance of the risks identified. Monitoring and review will be undertaken on at least an annual basis.

The continual process of monitoring and review is required to ensure ongoing effective risk treatments and continual improvement.

- Monitoring – assess whether current risk management objectives are being achieved. Council can use inspections, incident reports, self-assessments, and audits to monitor its risk management plan.
- Review – assess whether the current risk management plan still matches Council's risk profile. The risk management plan may be reviewed by studying incident patterns, legislative changes, and organisational activities.

Action

Use risk registers, control effectiveness reviews, testing, assurance maps, and ARC oversight. Integrate QAO risk maturity self-assessments annually.

4.7 Reporting

Officers who are risk owners will report on the management of their risks in alignment with the operational plan reporting cycle. This reporting will include any incidents, new or changed risks, the success of mitigation strategies and any suggested changes to the risk register.

At a higher level the Governance, Strategy and Risk team will provide reporting to Council and the Audit and Risk Committee.

Any serious incidents will be escalated immediately by the risk owner through the appropriate channels.

4.8 Communication and Consultation

The Risk Management Framework, Policy, Risk Registers and associated documents and procedures will be held in a secure central repository and will be accessible to stakeholders according to their authority levels.

The existence, nature and location of the central repository will be shared with staff at all levels to encourage their awareness of how the organisation is managing its risks.

Following reviews of the framework and guidelines as specified, any changes will be communicated to the relevant risk owners and other stakeholders to ensure that the Enterprise Risk Management process remains dynamic and relevant.

Action

Engage staff, LDMG partners, suppliers, and community as appropriate.

5. Methodology and Tools

5.1 Risk Scales and Matrix (Appendix B)

Council adopts a 1–5 likelihood and 1–5 consequence scale, generating a 5×5 matrix (Extreme/High/Medium/Low). The matrix is category-aware (e.g., separate consequence tables for Operational – Business Continuity, Environmental, Information Technology, Strategic/Corporate Governance – Reputation – Political, Human Resources, Infrastructure, Asset & Property, Workplace Health & Safety, Financial and Economic). Risk criteria must be reviewed annually or on trigger events (legislative change, reorganisation, major incident).

5.1.1 Risk Register

Council maintains a register of Strategic and Corporate risks which includes assessment of inherent and residual risks, risk appetite, treatment, and responsible officer.

5.2 Integrated Assurance

Council uses a Three Lines approach:

1. Management owns risk/controls.

2. Risk & Compliance provide frameworks/monitoring and policy oversight (privacy, cyber-security, disaster governance).

3. Internal Audit tests effectiveness and reports to the Audit and Risk Committee; External Audit/QAO provide independent external assurance/maturity insight.

5.3 Specific Domain Requirements

5.3.1 Work Health and Safety (WHS)

The Executive Leadership Team (ELT) and Senior Leadership Team (SLT) must show due diligence, maintain WHS knowledge, understand operations/risks, ensure appropriate resources, implement incident/hazard processes, and verify compliance.

5.3.2 Disaster and Climate Risk

Maintain LDMP and sub-plans, capability/exercises, lessons management, and report against EMAF standards. Integrate climate adaptation considerations into asset planning and risk treatment.

5.3.4 Information Privacy and Cyber Security

Comply with mandatory requirements including breach assessment, record-keeping and notification timeframes.

Adopt cyber-security governance checklists/role capability guides and maintain a current asset and risk view.

5.3.5 Procurement, Contracts and Projects

Embed risk allocation, probity, and performance monitoring. For major projects, apply Queensland Treasury Project Assessment Framework (PAF) for staged assurance and benefits realisation.

5.3.6 Financial Sustainability

Link risk to the Long-Term Financial Forecast and Asset Management strategies; monitor liquidity, debt, revenue, and asset renewal risks.

5.4 Reporting and Escalation

The table below sets out the minimum requirements for risk management reporting.

TIMEFRAME	RESPONSIBILITY	REPORTING ACTIVITY
Quarterly	Primary Risk Owner	In line with the business unit operational plan reporting cycle, each risk will be reviewed, and reports made on risk updates, breaches of appetite, incidents, emerging threats, and effectiveness of treatment measures.
Annual	Coordinator Governance, Strategy and Risk.	Provide report to Council with enterprise risk profile, appetite breaches, maturity trend (QAO model), and improvement plan status. Provide Q4 reporting to the Audit and Risk Committee.
Immediate Escalation	Primary Risk Owner	WHS notifiable incidents; suspected privacy/data breaches; critical cyber-security events; disaster activations.

5.5 Capability, Culture, and Training

Actions

Ensure that annual Risk/WHS/Privacy/Cyber-security/Disaster training is included in the organisation training and development plan for Councillors, executives, managers, and staff as required.

Monitor to ensure that officers evidence due diligence through meeting reporting requirements and application of risk consideration in reports to Council.

Promote a positive culture of risk management through feedback on reporting and proactive enhancement of risk registers to drive continuous improvement.

5.6 Continuous Improvement and Maturity

Actions

Conduct an annual self-assessment against QAO's Risk Management Maturity Model and take positive action to lift maturity.

Facilitate a biennial independent review (internal audit or peer review).

Update this Framework for legislative changes and lessons from incidents/exercises.

5.7 Related Documents

- Enterprise Risk Management Policy.
- Risk Appetite Statement.
- Internal Audit Charter.
- Fraud & Corruption Prevention Policy.
- Workplace Health and Safety General Policy.
- Douglas Local Disaster Management Plan.

Appendix A - Risk Appetite Ranges

DEFINITION	TYPICAL CHARACTERISTICS	USE CASES
1. Averse Appetite	*Avoid risk entirely*	*Strict compliance, zero tolerance*
Council is **not willing to accept any meaningful level of risk**, except in situations where eliminating the risk is impossible. Decisions prioritise full compliance, strict controls, and avoidance actions.	Zero tolerance for breaches, misconduct, or illegal activity. Preference for highly reliable, proven methods. Focus on preventing loss or harm over pursuing opportunity.	Governance, integrity, fraud, and compliance-related controls.
2. Minimal Appetite	*Very low risk acceptance*	*Strong controls, high caution*
Council is willing to accept **very low levels of risk**, and only where the potential benefits clearly outweigh the exposure. Controls must be strong and consistently applied.	High emphasis on safety, wellbeing, and quality. Preference for predictable, low-variance processes. Limited experimentation or innovation.	Community safety, workplace health and safety, public health obligations.
3. Cautious Appetite	*Low–moderate risk acceptance*	*Evidence-based decisions, controlled innovation*
Council is willing to accept **small to moderate levels of risk**, provided risks are well understood, managed, and monitored. Some innovation is supported, but within a structured framework.	Decisions supported by evidence and robust analysis. Moderate tolerance for delays, cost variations, or uncertainty. Innovation allowed if risks are controlled.	Environmental programs, infrastructure projects, reputation management.
4. Open Appetite	*Moderate–high acceptance*	*Encourages innovation, accepts uncertainty*
Council is willing to accept **higher levels of risk** where potential benefits are significant. Innovation, pilot programs, and new ways of working are encouraged, as long as risk controls are reasonable.	Flexibility and experimentation. Acceptance of potential setbacks; provided learnings are captured. Balanced pursuit of opportunity and service improvement.	Digital transformation, service innovation, workforce initiatives.

Appendix B – Risk Scales and Matrix

DESCRIPTION	FREQUENCY	PRESUMPTIONS
Almost Certain (5)	Event may occur within one year	The event is expected to occur in most circumstances
Likely (4)	Event may occur every 1 - 2 years	The event will probably occur in most circumstances
Possible (3)	Event may occur once every 2 - 5 years	The event should occur at some time
Unlikely (2)	Event may occur every 5 - 10 years	The event could occur at some time
Rare (1)	Event may occur once every 10+ years	The event may only occur in exceptional circumstances

Consequence Definitions

Consequence	Rating	Operational – Business Continuity	Environmental	Information Technology	Strategic/Corporate Governance – Reputation - Political	Human Resources	Infrastructure, Asset & Property	Workplace Health & Safety	Financial and Economic
Catastrophic	**5**	The continuing failure of Council to deliver essential services. The removal of key revenue generation.	Widespread and irreversible environmental damage attributed by the courts to be negligent or incompetent actions of Council.	Widespread, long-term loss of IT network/hardware.	Loss of State Government support with scathing criticism and removal of Council. National media exposure. Loss of power and influence restricting decision making and capabilities.	Staff issues cause continuing failure to deliver essential services.	Widespread, long-term loss of substantial key assets and infrastructure.	Fatality or significant irreversible disability.	Above 20% of Council's annual revenue (excluding capital revenue) = $4million.
Major	**4**	Widespread failure to deliver several major strategic objectives and service plans. Long-term failure of Council causing lengthy service interruption.	Severe environmental impact requiring significant remedial action. Penalties and/or direction or compliance order incurred.	Widespread, short to medium term loss of IT network/hardware.	State media and public concern/exposure with adverse attention and long-term loss of support from Douglas Shire residents. Adverse impact and intervention by State Government.	Staff issues cause widespread failure to deliver several major strategic objectives and long-term failure of day-to-day service delivery.	Widespread, short to medium term loss of key assets and infrastructure.	Extensive injuries. Lost time of more than 4 working days.	Between 10-20% of Council's annual revenue (excluding capital revenue) = $2m - $4million.
Moderate	**3**	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service interruption for a week.	Moderate impact on the environment; no long term or irreversible damage. May incur cautionary notice or infringement notice.	Short to medium term loss of key IT network/hardware.	Significant statewide concern/exposure and short to mid-term loss of support from Douglas Shire residents. Adverse impact and intervention by another local government & LGAQ.	Staff issues cause failure to deliver minor strategic objectives and temporary and recoverable failure of day-to-day service delivery.	Short to medium term loss of key assets and infrastructure.	Medical treatment. Lost time of up to 4 working days.	Between 6-10% of Council's annual revenue (excluding capital revenue) = $1.2m - $2million.
Minor	**2**	Temporary and recoverable failure of Council causing intermittent service interruption for several days.	Minor environmental damage such as remote temporary pollution.	Minor loss/damage. Repairs required.	Minor local community concern manageable through good public relations. Adverse impact by another local government.	Staff issues cause several days interruption of day-to-day service delivery.	Minor loss/damage. Repairs required.	First aid treatment. No lost time.	Between 2-6% of Council's annual revenue (excluding capital revenue) = $400,000 - $1.2million.
Insignificant	**1**	Negligible impact of Council, brief service interruption for several hours to a day.	Brief, non-hazardous, transient pollution or damage.	Damage where repairs are required however equipment still operational.	Transient matter, e.g. Customer complaint, resolved in day-to-day management. Negligible impact from another local government.	Staff issues cause negligible impact of day-to-day service delivery.	Damage where repairs are required however facility or infrastructure is still operational.	No injury.	Less than 2 % of Council's annual revenue (excluding capital revenue) = $400,000.

Risk Matrix

		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
5	Almost Certain (5)	Moderate (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
4	Likely (4)	Moderate (4)	Moderate (8)	High (12)	High (16)	Extreme (20)
3	Possible (3)	Low (3)	Moderate (6)	High (9)	High (12)	High (15)
2	Unlikely (2)	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
1	Rare (1)	Low (1)	Low (2)	Moderate (3)	Moderate (4)	High (5)

DOUGLAS SHIRE COUNCIL

Risk Appetite Statement

1. Purpose

Douglas Shire Council (Council) is committed to delivering high-quality services, protecting the region's unique natural environment, and supporting the wellbeing and resilience of its communities. Effective risk management enables Council to make informed decisions, respond to uncertainty, and take opportunities that support sustainable development, climate resilience, economic vitality, and cultural heritage.

This Risk Appetite Statement establishes the level and types of risk Council is willing to accept in pursuit of its strategic objectives. It supports transparent governance, responsible stewardship of resources, and alignment with AS ISO 31000:2018 principles.

The purpose of this Risk Appetite Statement is to:

- Provide clear guidance for decision-making at all levels of Council.
- Ensure risks are managed consistently, proactively, and proportionately.
- Support innovation, community value, and prudent financial management.
- Balance opportunity with protection of community, environment, and assets.
- Embed risk thinking into planning, projects, operations, and service delivery.

2. Overall Risk Appetite

Council maintains a **balanced and cautious overall risk appetite**.

Council seeks to maximise benefits for the community while ensuring risks to people, natural environment, cultural heritage, financial sustainability and reputation are carefully managed.

Council is **open to taking reasonable risks** in areas that enable innovation, service improvement, economic diversification, and community wellbeing—provided controls are in place and risks remain within acceptable thresholds.

3. Risk Appetite Level Descriptions

DEFINITION	TYPICAL CHARACTERISTICS	USE CASES
1. Averse Appetite	***Avoid risk entirely***	***Strict compliance, zero tolerance***
Council is **not willing to accept any meaningful level of risk**, except in situations where eliminating the risk is impossible. Decisions prioritise full compliance, strict controls, and avoidance actions.	• Zero tolerance for breaches, misconduct, or illegal activity. • Preference for highly reliable, proven methods. • Focus on preventing loss or harm over pursuing opportunity.	Governance, integrity, fraud, and compliance-related controls.
2. Minimal Appetite	***Very low risk acceptance***	***Strong controls, high caution***
Council is willing to accept **very low levels of risk**, and only where the potential benefits clearly outweigh the exposure. Controls must be strong and consistently applied.	• High emphasis on safety, wellbeing, and quality. • Preference for predictable, low-variance processes. • Limited experimentation or innovation.	Community safety, workplace health and safety, public health obligations.
3. Cautious Appetite	***Low–moderate risk acceptance***	***Evidence-based decisions, controlled innovation***
Council is willing to accept **small to moderate levels of risk**, provided risks are well understood, managed, and monitored. Some innovation is supported, but within a structured framework.	• Decisions supported by evidence and robust analysis. • Moderate tolerance for delays, cost variations, or uncertainty. • Innovation allowed if risks are controlled.	Environmental programs, infrastructure projects, reputation management.
4. Open Appetite	***Moderate–high acceptance***	***Encourages innovation, accepts uncertainty***
Council is willing to accept **higher levels of risk** where potential benefits are significant. Innovation, pilot programs, and new ways of working are encouraged, if risk controls are reasonable.	• Flexibility and experimentation. • Acceptance of potential setbacks; provided learnings are captured. • Balanced pursuit of opportunity and service improvement.	Digital transformation, service innovation, workforce initiatives

4. Risk Appetite by Category

RISK APPETITE BY CATEGORY	EXPLANATION
4.1. Community Safety and Public Health	
Minimal Appetite.	Council has a ***minimal*** appetite for risks that could impact public safety, community wellbeing, or essential health standards. Council prioritises: • Safe public spaces. • Resilient infrastructure. • Effective disaster management. • Strong compliance with public health regulation. Council will not knowingly accept risks that may result in harm to residents, visitors, or employees.
4.2. Environment & Climate Risk	
Cautious to Open Appetite	As steward of the Daintree Rainforest, Great Barrier Reef coastline, and other sensitive ecosystems, Council adopts a **cautious** appetite regarding environmental harm. However, Council is **open** to risks associated with: • Climate adaptation initiatives. • Innovative sustainability projects. • Environmental partnerships and eco-tourism opportunities. Council recognises that pursuing climate resilience may involve trialling new methods or technologies.
4.3. Financial Sustainability	
Cautious Appetite	Council has a **conservative** appetite for financial risk to ensure long-term stability and prudent use of ratepayer funds. Council will accept limited financial risk where: • Value for money is demonstrated. • Investments support long-term community benefit. • Opportunities align with strategic objectives. Significant borrowing, unplanned expenditure, or uncertain financial returns must be carefully justified and transparently governed.

4.4. Governance, Compliance & Integrity	
Averse Appetite	Council is **averse** to risks involving: • Fraud, corruption, misconduct. • Breaches of legislation or policy. • Failures in transparency, ethics, or accountability. Council fosters a culture of integrity, strong internal controls, and responsible decision-making.
4.5. Reputation & Stakeholder Confidence	
Cautious Appetite	Council maintains a **cautious** appetite for reputational risk. While open engagement and honest communication may involve risk of public criticism, Council seeks to: • Promote trust through transparency. • Maintain constructive relationships with community and partners. • Manage issues proactively to safeguard confidence. Council may accept short-term reputational risk where long-term benefits justify the approach.
4.6. Service Delivery & Customer Experience	
Open Appetite	Council is **open** to risks that support improved service delivery, innovation, digital transformation, and efficiency gains. Council encourages: • New technologies that improve customer experience. • Creative approaches to community engagement. • Partnerships that enhance service outcomes. Projects must include suitable planning, engagement, and mitigation strategies.
4.7. Projects & Infrastructure	
Cautious Appetite	Council is **cautious** toward risks inherent in capital works and complex projects, such as: • Schedule delays. • Cost overruns. • Construction risks. Council supports measured risk-taking where: • Projects align with strategic priorities. • Risks are actively managed. • Strong project governance exists.

4.8. People, Workforce & Culture	
Minimal to Open Appetite (depending on context)	Council has a ***minimal*** appetite for unsafe work practices or poor staff wellbeing and an ***open*** appetite for: • New workforce initiatives. • Leadership development. • Flexible work innovation. Council values a positive, high performing culture and supports initiatives that strengthen capability and resilience.
4.9. Disaster Management	
Averse Appetite	Council is **averse** to risks involving: • Business Continuity and Critical Service Disruption. • Emergency and Incident Response Capability. • Community Resilience and Preparedness.

5. Risk Scales, Consequence Definitions and Matrix

DESCRIPTION	FREQUENCY	PRESUMPTIONS
Almost Certain (5)	Event may occur within one year	The event is expected to occur in most circumstances
Likely (4)	Event may occur every 1 - 2 years	The event will probably occur in most circumstances
Possible (3)	Event may occur once every 2 - 5 years	The event should occur at some time
Unlikely (2)	Event may occur every 5 - 10 years	The event could occur at some time
Rare (1)	Event may occur once every 10+ years	The event may only occur in exceptional circumstances

Consequence Definitions

Consequence	Rating	Operational – Business Continuity	Environmental	Information Technology	Strategic/Corporate Governance – Reputation - Political	Human Resources	Infrastructure, Asset & Property	Workplace Health & Safety	Financial and Economic
Catastrophic	**5**	The continuing failure of Council to deliver essential services. The removal of key revenue generation.	Widespread and irreversible environmental damage attributed by the courts to be negligent or incompetent actions of Council.	Widespread, long-term loss of IT network/hardware.	Loss of State Government support with scathing criticism and removal of Council. National media exposure. Loss of power and influence restricting decision making and capabilities.	Staff issues cause continuing failure to deliver essential services.	Widespread, long-term loss of substantial key assets and infrastructure.	Fatality or significant irreversible disability.	Above 20% of Council's annual revenue (excluding capital revenue) = $4million.
Major	**4**	Widespread failure to deliver several major strategic objectives and service plans. Long-term failure of Council causing lengthy service interruption.	Severe environmental impact requiring significant remedial action. Penalties and/or direction or compliance order incurred.	Widespread, short to medium term loss of IT network/hardware.	State media and public concern/exposure with adverse attention and long-term loss of support from Douglas Shire residents. Adverse impact and intervention by State Government.	Staff issues cause widespread failure to deliver several major strategic objectives and long-term failure of day-to-day service delivery.	Widespread, short to medium term loss of key assets and infrastructure.	Extensive injuries. Lost time of more than 4 working days.	Between 10-20% of Council's annual revenue (excluding capital revenue) = $2m - $4million.
Moderate	**3**	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service interruption for a week.	Moderate impact on the environment; no long term or irreversible damage. May incur cautionary notice or infringement notice.	Short to medium term loss of key IT network/hardware.	Significant statewide concern/exposure and short to mid-term loss of support from Douglas Shire residents. Adverse impact and intervention by another local government & LGAQ.	Staff issues cause failure to deliver minor strategic objectives and temporary and recoverable failure of day-to-day service delivery.	Short to medium term loss of key assets and infrastructure.	Medical treatment. Lost time of up to 4 working days.	Between 6-10% of Council's annual revenue (excluding capital revenue) = $1.2m - $2million.
Minor	**2**	Temporary and recoverable failure of Council causing intermittent service interruption for several days.	Minor environmental damage such as remote temporary pollution.	Minor loss/damage. Repairs required.	Minor local community concern manageable through good public relations. Adverse impact by another local government.	Staff issues cause several days interruption of day-to-day service delivery.	Minor loss/damage. Repairs required.	First aid treatment. No lost time.	Between 2-6% of Council's annual revenue (excluding capital revenue) = $400,000 - $1.2million.
Insignificant	**1**	Negligible impact of Council, brief service interruption for several hours to a day.	Brief, non-hazardous, transient pollution or damage.	Damage where repairs are required however equipment still operational.	Transient matter, e.g. Customer complaint, resolved in day-to-day management. Negligible impact from another local government.	Staff issues cause negligible impact of day-to-day service delivery.	Damage where repairs are required however facility or infrastructure is still operational.	No injury.	Less than 2 % of Council's annual revenue (excluding capital revenue) = $400,000.

Risk Matrix

		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
5	Almost Certain (5)	Moderate (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
4	Likely (4)	Moderate (4)	Moderate (8)	High (12)	High (16)	Extreme (20)
3	Possible (3)	Low (3)	Moderate (6)	High (9)	High (12)	High (15)
2	Unlikely (2)	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
1	Rare (1)	Low (1)	Low (2)	Moderate (3)	Moderate (4)	High (5)

Douglas Shire Council Risk Register

No.	Risk	Risk Category	Source of Risk	Consequences description	Likelihood (Inherent)	Consequence (Inherent)	Inherent Risk Rating	Risk Appetite	Risk Treatment Decision	Risk Treatment / Actions	Likelihood Residual	Consequences Residual	Residual Risk Rating	Responsibility: Position
	Financial Sustainability	Strategic	- Lack of strategic planning - Inappropriate staffing/management - Failure to monitor forward estimates / life-cycle costs / long-term financial sustainability - Poor Budget control - Councillor decision-making - Poor internal controls - Poorly managed financial delegations - Under insurance - Lack of asset management strategies/systems - Delays in budget adoption due to Council elections	- Modified audit - Budget overspend - Reputation and community backlash - Fraud - Loss of significant investment income (contract work) - Loss of confidence by Government Departments and regulatory bodies - Additional scrutiny from regulatory bodies.	Possible (3)	Catastrophic (5)	High (15)	Cautious	Control the risk	- Maintain effective internal and external audit functions - Maintain accurate long term financial forecast that informs budget decisions - Regular budget monitoring and reviews - Mature monthly performance reporting processes - Developed 10 year financial modelling capability - Suitably qualified professional staff - Adopted fit-for-purpose asset management plans - Documented internal controls and reconciliation processes - Allocate sufficient funding to allow expert consultancy as required - Reporting intergrated to Audit and Risk Committee activities	Unlikely (2)	Major (4)	Moderate (8)	GM Corporate and Communities
	Failure to deliver essential services (water, transport, sewerage, waste)	Strategic	- Major equipment failure - Weather event - cyclone, flood - Failure of external service provider (e.g. Ergon, Telstra) - Poor operational control - Lack of qualified and experienced staff (e.g. transition of aging workforce) - Insufficient qualified personnel to maintain delivery of these essential services - Changes to legislation and standards - Lack of planning - Asset management (maintenance and renewal) insufficient planning, preventative maintenance and lack of funds available. - Terrorist attack - Not understanding the customer's expectations regarding service standards - changes in legislative requirements with insufficient time to plan for the change - Council expands service provision into 'non traditional' areas or forced to take on management through higher government responsibility shifting - Disruption of services due to maintenance activities	- Penalties, fines - Adverse publicity - Reputational damage - Health impact on residents - Financial loss - Political fallout - Environmental damage - Loss of asset	Possible (3)	Major (4)	High (12)	Cautious	Control the risk	- Suitably qualified and trained staff - Business continuity plans - Back-up power supply at critical installations - Counter disaster sub plans - Asset management plans linked to long-term financial plans - Asset Management Plans reflect the service standards expected by the customer - Review core business obligations - Communication and collaboration with external providers - Agreed service standards and maintenance intervals - Regional agreements and alliances - Implement appropriate security measures to protect essential assets	Unlikely (2)	Major (4)	Moderate (8)	GM Infrastructure
	Culture, Conduct, Leadership and Maturity	Strategic	Leadership failure to maintain a positive and productive culture within the organisation.	Low productivity and service delivery.	Possible (3)	Major (4)	High (12)	Minimal	Control the risk	- Develop a Leadership Behaviour Framework endorsed and modelled by ELT and SLT. - Introduce management accountability measures based on behaviour KPIs and subject to 360 degree feedback. - Tone from the top communication plan — regular ELT and SLT messaging reinforcing values, conduct, and ethical expectations. - Assign a formal ELT member to sponsor organisation culture uplift initiatives. - Deliver mandatory ethics and conduct training. - Invest in Leadership Development Programs, coaching, mentoring, emotional intelligence, conflict management. - Structured Change Management Framework — Ensures people impacts and cultural risks are managed in transformation programs.	Unlikely (2)	Moderate (3)	Moderate (3)	Chief Executive Officer
	Disaster Management	Strategic	Failure to plan for, prevent, prepare for, respond to and recover from disaster events in accordance with statutory obligations under the *Disaster Management Act 2003* and community expectations.	- Potential Loss of life and injury - Financial/economic loss - Delay in recovery across human and social, economic, roads and transport, infrastructure and environmental spheres - Loss of reputation - incursion of significant costs that can't be claimed - Lack of communication - Reduced Financial Stability	Possible (3)	Major (4)	High (12)	Averse	Control the risk	- Appointment of dedicated and permanent Disaster Management Manager. - Local Disaster Management Group meetings and relevant sub-groups activated per event - MOU updated and renewed with other NQ Region Councils: currently valid for 2021 to 2026 - Actively maintaining an afterhours/availability roster for Easter/Christmas periods. - Annual review and moving to user-friendly checklists (paper light system) of Disaster Management Plan and sub-plans. - Improved communication to community and within Council via engagement sessions and establishment of the Douglas Disaster Facebook page. - Investment in Disaster incident management software (Guardian IMS), Disaster Dashboard development - Opt in alert messaging - Increased community engagement such as awareness raising with PDNC, Douglas Shire Aged Care and stall holders at markets. - Damage to Disaster Recovery Centre (IT infrastructure), addressed by the procurement of a Pelicase and radio comms audit. - Increased training (QDMA, masterclass, DRFA, Dashboard and teambuilding) with the IMT - Concept design drawings and construction estimate completed for a multi-purpose training and disaster coordination centre. - Providing regular reporting to relevant stakeholders.	Unlikely (2)	Major (4)	Moderate (8)	Manager Disaster Management
	Strategic Workforce and Capability	Strategic	- Lack of corporate knowledge due to turnover of staff - Ageing workforce - higher retirement rate - Lack of training and development - Inappropriate staff culture - Lack of succession planning - Uncompetitive remuneration - Shortage of skills within region - Inability to attract appropriately skilled and experienced staff - Staff fatigue during critical timeframes - Loss of confidence by Council staff in the Vision	- Failure to deliver operational requirements - Inability to meet service needs - Ineffective planning - Missed opportunities - Community backlash - Financial implications - Increased use of consultants - A greater pressure on capable people	Possible (3)	Moderate (3)	High (9)	Minimal	Control the risk	- Commitment to training/professional development of staff - Competitive remuneration packages - Dedicated Human Resources and Training team - Opportunities for secondments within organisation - Opportunities for trainees and graduates -Transition to retirement program - Participation in networking groups e.g. FNQROC / Peak Services - Partner with LGAQ & LGMA	Unlikely (2)	Moderate (3)	Moderate (3)	GM Corporate and Communities

No.	Risk	Risk Category	Source of Risk	Consequences description	Likelihood (Inherent)	Consequence (Inherent)	Inherent Risk Rating	Risk Appetite	Risk Treatment Decision	Risk Treatment / Actions	Likelihood Residual	Consequences Residual	Residual Risk Rating	Responsibility: Position
	ICT Disruption Cyber Security Digital Resilience	Strategic	Failure or disruption of Council's ICT systems, digital platforms or cyber security controls.	- Inability to maintain service delivery to the community. - Compromise of sensitive or confidential information including privacy breaches. - Reputational harm and erosion of community trust.	Possible (3)	Major (4)	High (12)	Averse	Control the risk	- Develop, implement and maintain a ICT strategy. '- Maintenance of system backups (on & off site) - Standby generator - Budgeting for routine maintenance, disaster recovery testing & upgrades - Maintain high levels of System Security and access approval procedures. - Document and test business continuity processes - Up skilling of all staff in IT. - Establish IT Steering group to monitor risks - Offsite remote connectivity for use in emergency/pandemic - Extensive Cyber Risk training for all staff	Unlikely (2)	Major (4)	Moderate (8)	GM Corporate and Communities
	Reputational / Political	Strategic	- Perceived conflicts of interest (Councillors or senior officers) - Poor transparency or inadequate community engagement - Inconsistent application of policies or local laws - High-profile service failures or safety incidents - Procurement, development, or planning decisions seen as biased - Inappropriate use of public funds or resources - Weak complaints handling or delayed responses - Inaccurate, late, or unclear public communications - Social media misinformation or Council responses perceived as defensive - Political tensions between Councillors, Mayor, Chief Executive Officer, and Executive Leadership	- Erosion of trust in Council leadership and decision-making - Long-term reputational damage across election cycles - Reduced ability to deliver strategic priorities - Increased State Government oversight or intervention - Investigations by the Crime and Corruption Commission (CCC) - Ombudsman complaints or public interest disclosures - Project delays or cancellations - Reduced staff morale and retention	Possible (3)	Major (4)	High (12)	Averse	Control the risk	- Councillor Code of Conduct - Employee Code of Conduct - Conflicts of Interest policy and registers - Delegations register framework and decision-making protocols - Public council meetings and published agendas/minutes - Media and communications policy - Complaints management system - Records management and information governance - Internal audit and risk management framework - Audit and Risk Committee - Internal audit function - Mandatory training for Councillors and officers	Possible (3)	Major (4)	High (12)	Chief Executive Officer
	Financial Management	Corporate	Failure to manage operating result.	Negative impact on financial sustainability.	Possible (3)	Major (4)	High (12)	Cautious	Control the risk	Maintain proper financial management and reporting systems and practices '- Regular budget monitoring and reviews as required - Develop mature monthly Budget v Actual reporting - Oversight by qualified professional staff - Financial system in place - Documented internal controls and reconciliation processes - Ongoing refinement of business processes	Unlikely (2)	Moderate (3)	Moderate (3)	Chief Financial Officer
	Asset and Infrastructure Management	Corporate	Failure to systematically manage the condition, performance, and lifecycle of its physical and digital assets.	Inability to maintain service delivery to the community. Financial impact of unexpected asset failure.	Likely (4)	Major (4)	High (16)	Cautious	Control the risk	- Develop, implement and maintain a Long Term Asset Management Plan. - Asset Management Policy and Strategy aligned to Council objectives- Asset lifecycle planning covering acquisition, maintenance, renewal, and disposal - Asset criticality assessments to prioritise resources - Workforce training and capability development in asset management	Likely (4)	Moderate (3)	High (12)	Manager Infrastructure Planning and Delivery
	Procurement, Contract and Vendor Management	Corporate	- Failure to provide adequate training and development to 'procurement officers' - Inadequate procurement policies and procedures and/or untimely review processes - Immature procurement analytics processes - Lack of or ineffective consequences where non-compliance is identifed - Techology system/application doesn't support Council's procurement objectives	- Failure to demonstrate value-for-money and compliance with Procurement Policy, procedures, legislative obligations and other prescribed requirements - Ineffective contract management—including absence of monitoring, unclear responsibilities, leading to service failures, financial liabilities, legal disputes, and reputational damage.	Likely (4)	Moderate (3)	High (12)	Cautious	Control the risk	- Futher maturation of compliance process, policies and procedures through benchmarking an adoption of better practice - Introduce timely and regular training regime on better practice for procurement officers and senior staff - Secure greater capability and capacity into the existing procurement team	Likely (4)	Moderate (3)	High (12)	Chief Financial Officer
	Cyber Security	Corporate	Cyber security control bypass or controls that are insufficient to detect, prevent or respond to malicious cyber activity.	Council operations are impacted by malicious cyberattack, malware or ransomware.	Possible (3)	Major (4)	High (12)	Averse	Control the risk	- Develop, implement and maintain a ICT strategy. - Address security & usability of the SCADA environment . - Build an annual Cyber improvments program of works using feedback and input from: -Aust Cyber Security Centre & QLD Cyber Security unit. -Results from Penatration and Security Assessments -Cyber Security Insurance / LGMA Review & Assessment -Industry best practise - Assess AI usage and related apps with caution. Evaluate each AI app / use for compliance with government guidelines and the risk of data breach by the AI provider.	Possible (3)	Major (4)	High (12)	Team Leader ICT
	Information Management, Privacy and Records Governance	Corporate	Information management system failure.	Data loss, unauthorised disclosure of records, privacy breaches, inability to meet statutory obligations, reduced organisational efficiency and reputational damage.	Possible (3)	Moderate (3)	High (9)	Averse	Control the risk	- Ensure control policies and procedures are adequate and reviewed annually - Staff are adequately trained - Council regularly tests internal controls	Unlikely (2)	Moderate (3)	Moderate (3)	Coordinator Governance and Risk

No.	Risk	Risk Category	Source of Risk	Consequences description	Likelihood (Inherent)	Consequence (Inherent)	Inherent Risk Rating	Risk Appetite	Risk Treatment Decision	Risk Treatment / Actions	Likelihood Residual	Consequences Residual	Residual Risk Rating	Responsibility: Position
	Digital Systems Reliability and Business Continuity	Corporate	Failure of Council's digital systems, infrastructure or technology platforms and/or extended outage.	Business continuity compromise, critical service interruption and the inability of Council to operate effectively, particularly during emergencies.	Possible (3)	Catastrophic (5)	High (15)	Averse	Control the risk	- Develop, implement and maintain a ICT strategy including business continuity plans. - Redundant network links estabilshed at all key Council buildings. - Maintain a cloud based DR enviroment which syncronises with the On-premise systems 3 times per day. - Fully redundant server and network hardware, able to tolerate equipment failures. - Core Applications are all within vendor supported versions & usually at the current release level. - Core Application patching is done either monthly, bi-annually or annually - in line with current releases. Hotfixes are applied as needed.	Possible (3)	Moderate (3)	High (9)	Team Leader ICT
	Environmental Compliance Climate and Sustainability	Corporate	Failure to ensure environmental compliance in the undertaking of Council's day to day operations and project delivery.	This may result in environmental harm, regulatory action, increased remediation costs, loss of accreditation, reputational damage, diminished community confidence in Councils environmental stewardship and reduced influence as an environmental regulator in the area.	Likely (4)	Moderate (3)	High (12)	Cautious	Control the risk	Effective management of operations to ensure environmental compliance obligations are met. - Review Council's "Environmental (Council Operations) General Policy", consider ISO14001 as a guiding standard - Embed environmental compliance within each business unit's risk assessments - Formalise internal reporting and escalation mechanism for environmental compliance breaches - Include enhanced environmental controls into Council's permits, approvals and licences	Unlikely (2)	Moderate (3)	Moderate (3)	Manager Environment and Planning
	Climate Adaptation Integration in Operations	Corporate	Failure to appropriately prepare for, or respond to, climate change impacts on Council's service delivery and assets.	Council infrastructure may be exposed to environmental hazards and increasing insurance premiums, disruption to the delivery of services and reputational damage.	Possible (3)	Moderate (3)	High (9)	Open	Control the risk	Conduct operations in line with the Climate Change (Council Operations) general policy. - Conduct a Climate Risk Gap Analysis identifying vulnerabilities, adaptation requirements, and priority mitigation actions for integration into strategic and operational planning and budget review cycle. - Progress through to phase 3 of QCRC Framework - Identify quick wins for solar and renewable sources of energy for Council infrastructure - Identify appropriate software for emissions and climate related reporting - Review relevant policies	Unlikely (2)	Minor (2)	Low (4)	Manager Environment and Planning
	Business Continuity and Critical Service Disruption	Corporate	Failure to maintain effective disaster governance arrangements, contemporary disaster management plans, and compliance with statutory obligations.	Ineffective disaster coordination, increased harm to the community, regulatory non-compliance, and reputational damage.	Likely (4)	Catastrophic (5)	Extreme (20)	Averse	Control the risk	Maintain the LDMP and support the LDMG. - Undertake a comprehensive review, restucture and endorsement of the Local Disaster Management Plan by Q3 2026. - Implement an annual disaster governance assurance program by Q3 2026 including comliance checks, plan currency, and reporting to ELT and Audit and Risk Committee - Deliver targeted disaster governance training focused on statutory roles, decision making and accountability during disasters including QDMA training - Undertake a review of responsible departments and roles for DRFA accountability by Q4 2026/27	Unlikely (2)	Major (4)	Moderate (8)	Manager Disaster Management
	Emergency and Incident Response Capability	Corporate	Failure to plan for, prevent, prepare for, respond to and recover from disaster events in accordance with statutory obligations under the Disaster Management Act 2003 (QLD) and community expectations.	Delayed response, inefficient use of resources, increased harm to community and prolonged service disruption.	Possible (3)	Major (4)	High (12)	Averse	Control the risk	Maintain the LDMP and support the LDMG. - Ensure that 80% of identified incident management roles are filled by trained personnel by Q2 2026 - Conduct at least two disaster response exercises and one recovery exercise annually from Q1 2026 onward, with documented outcomes and tracked improvement actions -Complete updated flood hazard and vulnerability mapping for all urban and high-risk rural areas by Q4 2026. - Audit of all Council owned buildings used in disaster management activities/provision of essential services completed by Q4 2026 and prority replacement/upgrade plan developed by Q2 2027 for identified asset improvements	Unlikely (2)	Major (4)	Moderate (8)	Manager Disaster Management
	Community Resilience and Preparedness	Corporate	Failure to effectively plan for and coordinate disaster recovery and resilience activities.	Community recovery may be delayed or fragmented, resulting in long-term social, economic, environmental and infrastructure impacts and reduced community resilience to future disasters	Possible (3)	Major (4)	High (12)	Averse	Control the risk	Maintain and implement disaster management plan and activities. - Update and endorse the Douglas Recovery Resilience Sub Plan by Q4 2027-28 - Establish a formal recovery monitoring and reporting framework by Q1 2026 - Deliver recovery and resilience training to senior leaders by Q2 2026. Focus on governance, funding compliance and community centred recovery - Local Resilience Action Plans (LRAPs) are reviewed on a six month timeline, commencing Q1 2026 and identified changes endorsed by Council before submission to Queensland Reconstruction Agency	Unlikely (2)	Major (4)	Moderate (8)	Manager Disaster Management
	Work Health and Safety	Corporate	Failure to maintain systems, resources and practices to ensure a safe and healthy workplace.	Injury, illness, death, legal exposure, financial impacts and loss of community confidence in Council's safety and capability.	Likely (4)	Catastrophic (5)	Extreme (20)	Averse	Retain the risk	Develop, implement and maintain a safety management system. - Fully implement an ISO45001 aligned Safety Management System by Q4 2027/28 - Implement a Psychosocial Hazard Prevention Framework (from OVWG work) including early-intervention pathways -Develop a WHS training and competency framework - Conduct inspections and safety culture audits across high risk work groups - Improve incident investigation quality and cause analysis - Improve safety and emergency hazard management drills - Introduce manual handling training	Unlikely (2)	Major (4)	Moderate (8)	Manager People Safety and Culture
	Organisational Workforce and Resource Planning	Corporate	Failure to effectively plan, secure and allocate the workforce, capability and financial resources required to deliver its strategic objectives and operational commitments.	Service delivery, project outcomes and organisational performance being compromised.	Likely (4)	Moderate (3)	High (12)	Open	Control the risk	Maintain effective planning and reporting systems. - Develop an integrated Workforce Plan aligned to strategic priorities, service demand and capital program requirements by Q2 2026-27. - Establish a corporate project management framework and capability uplift program for all project leads. - Implement workforce analytics and FTE modelling to identify gaps and resource needs by Q3 2026-27. - Strengthen attraction and retention initiatives including EVP, benefits, pathways and recruitment strategies by Q2 2026-27. - Build succession planning for critical roles across the organisation by investing in training, mentoring and leadership development. - Embed workforce impacts and OPEX requirement into all CAPEX business cases - Improve internal reporting on workforce capacity, utilisation and vacancy inputs	Unlikely (2)	Moderate (3)	Moderate (3)	Manager People Safety and Culture

No.	Risk	Risk Category	Source of Risk	Consequences description	Likelihood (Inherent)	Consequence (Inherent)	Inherent Risk Rating	Risk Appetite	Risk Treatment Decision	Risk Treatment / Actions	Likelihood Residual	Consequences Residual	Residual Risk Rating	Responsibility: Position
	Legislation and Regulatory Compliance	Corporate	Failure to maintain legislative compliance.	Legal breaches, enforcement actions, loss of accreditation, QAO findings, performance audits, funding risks and erosion of trust in Council's governance capability.	Likely (4)	Moderate (3)	High (12)	Averse	Control the risk	Maintain and effective governance framework. - Q1 2026/27 establish and maintain a consolidated legislative and regulatory obligations register - Implement a structured compliance reporting framework for presentation to Audit and Risk Committee by Q2 2026/27 - Embed compliance checkpoints into procurement, disaster and project workflows by Q2 2026/27 - Deliver targeted compliance training for exectutives, managers and project leads	Unlikely (2)	Moderate (3)	Moderate (3)	Chief Executive Officer
	Customer Experience	Corporate	Failure to maintain effective, consistent and customer focused service delivery and partnership arrangements.	Device dissatisfaction, strained partnerships, reputational harm and reduced trust, and diminished capacity to meet strategic outcomes.	Possible (3)	Moderate (3)	High (9)	Open	Control the risk	Maintain and report on customer service charter KPIs. - Review, consolidate and standardise Council's customer service response standards across all service areas by Q4 2026/27 - Strengthen customer request tracking and reporting processes to enable consistent capture, monitoring and closure of CRMs across all categories with reporting to SLT and ELT by Q2 2026/27 - Develop a Service Catalogue, Service Standards including performance indicators by Q4 2026/27	Unlikely (2)	Moderate (3)	Moderate (3)	Manager Community Services
	Partnerships, Stakeholder Engagement and Reputation	Corporate	Failure to proactively manage stakeholder relationships, communications and reputation.	Reputational harm, increased scrutiny, reduced stakeholder cooperation, and diminished ability to deliver strategic, operational and recovery outcomes.	Possible (3)	Moderate (3)	High (9)	Cautious	Control the risk	Develop, implement and maintain a Stakeholder Engagement and Reputation Management Strategy. - Communications and media management protocols - Disaster communications arrangements - Corporate governance and transparency	Unlikely (2)	Moderate (3)	Moderate (3)	Chief Executive Officer
	Fraud & Corruption Control	Corporate	Failure to prevent, detect and respond to fraud, corruption and improper influence	Financial loss, regulatory action and loss of public trust.	Possible (3)	Major (4)	High (12)	Averse	Control the risk	Maintain a fraud and risk management framework. - Monitor and report on assurance activities. - Strong commitment demonstrated by the Management Team - Councillors promoting ethical behaviour to set the tone - Develop strong internal controls and documented procedures - Appropriate segregation of duties and delegations - Internal audit program with initial focus on high risk areas - External audit program - Mandatory Staff training and regular awareness sessions - Investigation of allegations undertaken by competent staff and/or industry professionals as required & followed through to disciplinary proceedings if required - Robust corporate induction program - Implement actions from Fraud and Corruption Control Plan - Maintain an effective Audit and Rick Committee - Conflict of Interest (Staff) Policy adopted	Unlikely (2)	Moderate (3)	Moderate (3)	Coordinator Governance and Risk
	First Nations Cultural Heritage Compliance (duty of care)	Corporate	Council activities cause unlawful harm to Aboriginal cultural heritage due to inadequate early assessment and engagement.	Project delays, penalties and reputational harm.	Possible (3)	Major (4)	High (12)	Cautious	Control the risk	Cultural Heritage Management Plans (where triggered), early Traditional Owner engagement, work-area clearances, staff training, incident stop-work protocols.	Rare (1)	Major (4)	Moderate (4)	Manager Community Services