Risk Management and Compliance Framework

Version 2 – June 2023

logan.qld.gov.au

CITY OF LOGAN

This Framework relates to:	Risk management and compliance procedures to be developed
Target audience:	All Staff
Description:	The Risk Management and Compliance Framework is designed to support Councillors, employees and contractors of Logan City Council (Council) to effectively manage risks and maintain compliance with statutory obligations, as we deliver against our strategic and operational goals and objectives

Related legislation, standards, and policies:

- *Local Government Act 2009*
- *Local Government Regulation 2012*
- ISO 31000:2018 Risk Management Guidelines
- ISO 37301:2021 Compliance Management Guidelines
- Logan City Council Governance Framework
- Logan City Council Audit and Risk Committee Policy
- Logan City Council Code of Conduct for Staff
- Logan City Council Risk Appetite Statements

Director responsible for Framework:	Director, Organisational Services
Manager responsible for Framework implementation:	Corporate Governance Manager
Framework Contact Person:	Risk and Compliance Program Leader

Framework review due date: 2 years from date of adoption or date of last review.

Document Control			
File:	**1336292-1**	**Document Id:**	**14119488**
Version Number	**Description of change**	**Author/Branch**	**Date Adopted**
1.0	Creation	Corporate Governance	28 October 2020
2.0	2023 Review	Corporate Governance	21 June 2023

Table of Contents

1 Introduction

The Risk Management and Compliance Framework is a strategic policy adopted by Council. It supports Council's commitment in the Corporate Plan 2021-2026 to be a high performing organisation. This framework provides Councillors, employees, and contractors with guidance on how to:

- apply consistent and comprehensive risk management
- manage statutory obligations.

This framework identifies key activities needed for an effective enterprise risk management approach. It provides information on how to identify, analyse, assess, and treat risks (threats and opportunities). The risk management process contained in this framework aligns with ISO31000:2018 Risk Management. Council's enterprise risk management practices are outlined below in Section 4.

The compliance elements of this framework outline Council's approach to managing its compliance obligations in accordance with the requirements of ISO 37301:2021 Compliance Management Systems. Council's enterprise compliance management practices are outlined below in Section 5.

This framework supports Council's Governance Framework. It outlines good risk management and compliance practices that, when applied, will help Council appropriately manage identified risks and statutory obligations. Adopting these practices will also help Council better understand the risks and compliance requirements when considering new initiatives and making key operational and strategic decisions.

2 Objectives

Risk management and compliance is the responsibility of all Councillors, employees, and contractors.

Good risk management and compliance practices support Council in meeting its corporate values. They also deliver on strategic and business objectives, through consistent and comprehensive processes. In adopting this framework, Council aims to:

- provide for a consistent organisational approach to both enterprise risk management and enterprise compliance management
- provide for centralised operational risk registers and a separate strategic risk register for Council to capture identified risks, with ongoing monitoring and oversight of appropriate actions to manage risks within Council's risk appetite (defined in section 4.7.1)
- provide for a centralised Statutory Obligations Register and greater clarity over statutory obligations by applying a risk-based approach to monitoring compliance, with oversight of actions taken to address non-compliances
- encourage a high standard of integrity and accountability at all levels of the organisation
- support more effective decision making through better understanding of risk exposure
- create an environment that enables Council to deliver its services and meet performance objectives in an efficient and cost-effective manner by incorporating risk and compliance management in decision-making processes
- monitor and review risk appetite and compliance levels to ensure that risk exposure remains acceptable and within Council's risk appetite
- make available accurate and concise risk information that informs decision making, including business direction
- safeguard Council assets – human, property, and reputation.

3 Roles and responsibilities

Council's risk management and compliance roles and responsibilities are outlined below. This illustrates that risk management and compliance are not the sole responsibility of one individual but is supported at all levels in the organisation.

Responsibility	Risk management	Compliance
Council	• Adopt this framework. • Provide strategic oversight and review.	• Adopt this framework. • Provide strategic oversight and review.
Audit and Risk Committee (ARC)	• Advisory committee of Council, that satisfies the requirement of the *Local Government Act 2009* that each large local government must have an audit committee. Legislatively, the ARC is responsible for monitoring and reviewing: o the integrity of financial documents o the internal audit function o the effectiveness and objectivity of Council's internal auditors. • Monitor and review the risk management function and internal control systems. • Provide an independent and objective forum to promote transparency, accountability and ethical behaviour and culture. • Monitor whether Council has in place a current and comprehensive enterprise risk management framework and associated procedures to ensure effective identification, assessment, management, and reporting of strategic and operational risks and provide oversight of this framework's review.	• Monitor and review the compliance management function. • Provide an independent and objective forum to promote transparency, accountability and ethical behaviour and culture. • Monitor whether Council has in place a current and comprehensive enterprise compliance management framework and associated procedures to ensure statutory obligations are effectively identified, assessed, managed, and reported and provide oversight of this framework's review.

Responsibility	Risk management	Compliance
Chief Executive Officer (CEO)	• Actively promote a positive risk culture. • Oversee implementation and embedding of risk management practices outlined in this framework. • Effectively manage Council's risks. • Own identified strategic risks. • Approve and accept operational risks in line with the escalation thresholds outlined in Appendix 1E. • Ensure that risk exposures are maintained within risk appetite; consider approval for risks that are outside of risk appetite; and oversee completion of treatment actions for these risks. • Review, assess and endorse Council's risk appetite statements.	• Actively promote a positive compliance culture. • Oversee implementation and management of compliance obligations.
Directors / Executive Leadership Team (ELT)	• Responsible to the CEO for effective risk management in their directorate. • Lead by example and demonstrate support and promote a positive risk management culture. • Identify, assess, and manage risks and controls. • Endorse this framework. • Oversee implementation of this framework. • Own relevant identified strategic risks. • Approve and accept operational risks in line with the escalation thresholds outlined in Appendix 1E. • Ensure, where possible, that risk exposures are maintained within risk appetite. • As required, consider approval for risks that are outside of risk appetite, including treatment actions. • Review, assess and endorse Council's risk appetite statements.	• Responsible to the CEO to oversee compliance with key statutory obligations in their directorate. • Lead by example and demonstrate active commitment to, and support for, a positive compliance culture. • Endorse this framework. • Oversee implementation of this Framework.

Responsibility	Risk management	Compliance
Corporate Governance Branch Risk and Compliance Program	• Regular review of this framework. • Provide operational and administrative oversight, guidance, expert advice and advisory support over risk management activities in the organisation in line with this framework. • Promote a positive risk culture, along with the benefits of good risk management practices. • Develop and maintain operational risk registers for each branch, in consultation with managers and risk owners. • Develop and maintain Council's strategic risk register in consultation with the ELT. • Facilitate risk workshops. • Report key risks to managers, risk owners, the ELT and ARC, including Council's risk profile. • Provide risk management training to Council staff as required. • Provide oversight over control self-assessments and any resultant updates to the relevant risk rating and control effectiveness. • Develop and progress a controls and assurance testing regime. • Provide oversight over the internal audit function.	• Regularly review this framework. • Provide operational and administrative oversight, guidance, expert advice and advisory support over compliance activities in the organisation in line with this framework. • Promote a positive compliance culture, along with the benefits of good compliance management practices. • Develop and maintain a statutory obligations register for each branch, in consultation with managers and obligation owners. • Advise obligation owners of changes to statutory obligations as they occur. • Facilitate compliance workshops. • Report key compliance matters to managers obligation owners, the ELT and ARC, including non-compliances and reportable breaches. • Provide compliance management training to Council staff as required. • Perform root cause analysis over identified non-compliances by applying a risk-based approach. • Provide oversight over the internal audit function.

Responsibility	Risk management	Compliance
Managers	• Responsible to their director to manage risk in their branch and adhere to this framework. • Demonstrate support for the risk management culture and actively promote a positive risk culture. • Identify, assess, and manage risks and controls relevant to their branch in line with this framework and in consultation with the Risk and Compliance Program. • Own, approve and accept identified operational risks relevant to their branch, in line with the escalation thresholds outlined in Appendix 1E. • Oversee treatment actions to improve controls over identified risks and reduce them to be within Council's risk appetite where appropriate. • Participate in risk assessments when required.	• Own and maintain compliance with key statutory obligations relevant to their branch and rectify identified non-compliances where required. • Ensure policies and other documents reflect current compliance obligations and are updated in a timely manner as requirements change. • Lead by example and demonstrate active commitment to, and support for, the compliance culture and actively promote a positive compliance culture. • Advise the Risk and Compliance Program of non-compliance with statutory obligations and escalate as required. • Participate in compliance assessments when required.
Program Leaders	• Identify, assess, and manage operational risks and controls relevant to their program in line with this framework and in consultation with the Risk and Compliance Program. • Oversee treatment actions to improve controls over identified risks and reduce these to be within Council's risk appetite where appropriate. • Participate in risk assessments when required.	• Own and maintain compliance with key statutory obligations relevant to their program and rectify identified non-compliances where required. • Advise the Risk and Compliance Program of non-compliance with statutory obligations and escalate as required. • Participate in compliance assessments when required.
Employees and contractors	• Ensure risks are appropriately identified, assessed, and controlled. • Comply with this framework. • Participate in risk assessments when required.	• Conscientiously seek to comply with relevant obligations in the course of their duties. • Comply with this framework. • Participate in compliance assessments when required.

4 Risk management

4.1 Overview of risk framework

A risk is a possibility that an event will occur that will adversely affect the achievement of objectives. Risk management is defined in the ISO 31000:2018 Risk Management Guidelines as 'coordinated activities to direct and control an organisation with regard to risk'. By applying the enterprise risk management approach outlined in this framework, Council will be able to identify and manage risks effectively and in turn, embed good risk management practices throughout the organisation. These practices support an enterprise risk management approach that will assist managers, risk owners and staff in their decision-making considerations. These practices have a foundation of documenting key risks in a centralised organisational risk register, along with regular review and reporting of those risks. Key risks are considered those that present the highest risk to Council.

4.2 Scope of the risk framework

This framework covers strategic risks and operational risks. These risks will be maintained in the organisational risk registers.

Strategic risk is a risk that impacts Council's strategic direction, as outlined in the corporate plan. ELT own Council's strategic risks.

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people or systems or from external events. Operational risks at Council are owned by a manager.

Across Council, there are other risk management practices in use, and these are managed in their own risk systems. These include:

- project risks
- health, safety and environment risks.

4.3 Risk culture

Risk culture can be described as the values, beliefs, knowledge, attitudes and understanding of risk throughout an organisation. The foundations to building Council's risk culture is supported by:

- Council's Risk Appetite Statements
- the requirements and activities outlined in this framework
- the Logan City Council Code of Conduct for Staff.

4.4 How Council manages risk

Council's approach to risk management is aligned with the ISO 31000:2018 Risk Management Guideline, which outlines the risk management process from risk identification through to risk treatment, recording and monitoring. The ISO 31000:2018 risk management process is illustrated in Figure 1, and further explained in clauses 4.5 to 4.10.

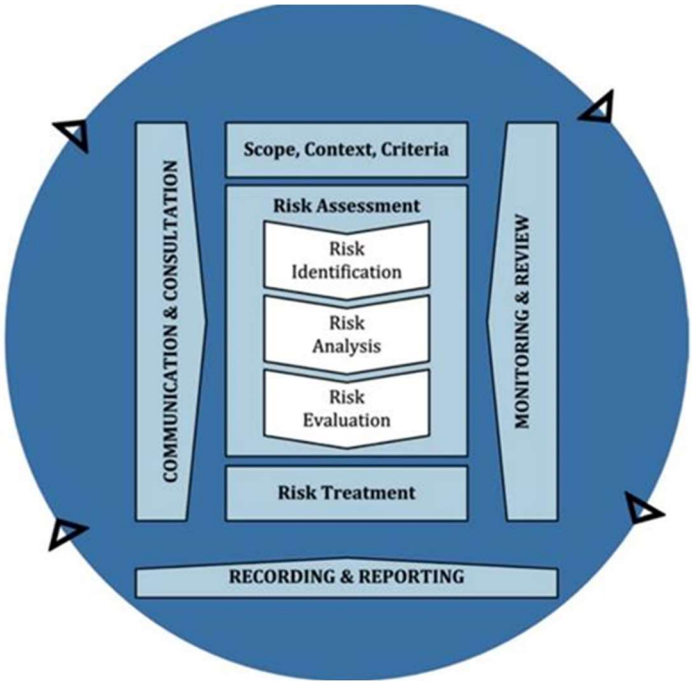

Figure 1: Risk management process

4.5 Risk identification

Risks are identified by detecting, recognising and cataloguing them. When a risk has been detected, 3 elements need to be identified:

- event (what could happen)
- cause/s (possible event triggers)
- consequence/s (result of the event).

Council catalogues strategic and operational risks in centralised risk registers. It does this in a consistent manner to ensure the 3 risk elements are adequately recognised when captured:

> *'There is a risk that [an event may happen] due to [these cause/s] resulting in [these consequence/s].'*

4.6 Risk analysis

Risk analysis involves:

- identifying the existing controls
- determining the likelihood of the risk occurring
- determining the consequence/s of the risk occurring
- calculating the risk rating (applying the likelihood and consequence ratings to Council's risk matrix).

Once risks have been identified, clearly defined and documented, they must be assessed to understand the implications of each risk. The Risk Tools in Appendix 1 provide the criteria to evaluate the significance of risk at Council. These include:

- Consequence/Impact Table (Appendix 1A) - confirm which risk category is most relevant and then consider the potential impact that could result should the risk be realised
- Likelihood Table (Appendix 1B) - consider the likelihood of the risk event
- Risk Matrix (Appendix 1C) – confirm the risk rating, having regard to the consequence/impact and likelihood.

Council determines and records both an inherent risk rating and a residual risk rating.

Inherent risk is the potential risk exposure with no effective controls in place – due to the absence, failure or removal of controls. This rating should not change during the life of the risk.

Residual risk rating (current risk rating) is the remaining risk exposure after the effectiveness of existing controls has been considered. The residual risk is a dynamic assessment, as it may change over time as treatment actions are implemented, controls are removed, or their effectiveness changes.

When considering how effective the existing controls are at managing the risk, refer to the Effectiveness of Controls table (Appendix 1D).

4.7 Risk evaluation

Risk evaluation is performed to support Council to make decisions based on the outcomes of risk assessments. It considers which risks are acceptable and prioritises risk treatments.

Risk evaluation involves determining:

- the risk target (preferred level of risk, based on Council's risk appetite)
- the treatment decision.

Risk appetite is the amount of risk Council is willing to pursue, retain, take, or turn away from to achieve its strategic vision and objectives, and deliver its services and projects. Council's Risk Appetite Statements are adopted by ELT and are outlined in an internally published document.

Once the residual risk has been determined, it should be assessed against Council's risk appetite to confirm if the risk is at an acceptable level, or if further treatment is required to reduce the risk to be within an acceptable level. Acceptable parameters have been determined for each risk category. If the risk is outside of the risk appetite, it will require approval by the ELT (refer to Risk Approval and Acceptance table at Appendix 1E).

4.8 Risk treatment

For risks that are outside of Council's risk appetite, the following risk treatment options should be considered:

- avoid – do not proceed with the activity
- accept – proceed with the activity and obtain approval at the appropriate level to operate outside of Council's risk appetite
- mitigate – implement risk treatments / additional controls to reduce the risk
- transfer – some, or all, of the risk to reduce the overall risk impact, by obtaining insurance or adopting a partnership with a third party.

Risk treatments are developed to reduce risk to an acceptable level and should be documented and tracked to completion. They should be regularly reviewed and monitored. When implementing risk treatment plans, they should be integrated into relevant processes and activities. Risk treatment plans should outline:

- those who are accountable for approving the plan and those responsible for implementing the plan
- proposed actions
- resource requirements including contingencies
- performance measures and constraints
- reporting and monitoring requirements
- timing and schedule for completion.

4.9 Accountability

Council's corporate value of excellence highlights that the organisation is committed to achieving excellent outcomes. By adopting the good risk management practices outlined in this framework, Council will ensure there is accountability, authority, and appropriate competence for managing risks. The framework also ensures there are adequate and effective controls by:

- documenting, assessing and tracking key risks across Council
- allocating risk owners, who have the accountability and authority to manage risks
- including responsibility for risk management at all levels in the organisation and ensuring Councillors, employees and contractors understand their responsibility for risk management
- establishing appropriate risk approval and escalation processes
- establishing regular reporting of key risks and their ratings – for risk owners, the ELT and the Audit and Risk Committee.

4.10 Monitoring, review and reporting

Continuously monitoring and reviewing risks is essential to ensure Council's identified risk assessments remain current and emerging risks are understood.

Council will establish regular reporting of key risks and their ratings – for risk owners, the ELT and the Audit and Risk Committee.

Council will review key risks with risk owners and key stakeholders every 6 months. This review process will be coordinated and overseen by the Risk and Compliance Program.

Based on this 6-month review, Council's risk profile will be produced and reported, at a directorate level and at a consolidated Council-wide level. The risk profile reporting will include heat maps to illustrate key risks that are of the greatest concern for Council.

5 Compliance management

5.1 Overview of Compliance Management

Compliance is defined by the ISO 37301:2021 Compliance Management Guidelines as being 'an ongoing process and the outcome of an organisation meeting its obligation'. Compliance management enables Council to demonstrate its commitment to comply with legislative and regulatory requirements, industry codes and organisational standards. It also demonstrates Council's commitment to standards of good governance, generally accepted best practices, and ethics, and to meeting community expectations.

By applying the enterprise compliance management processes outlined in this framework, Council will be able to identify and manage its statutory obligations effectively. In turn, it can embed good compliance management practices throughout the organisation. These practices include developing and maintaining a Statutory Obligations Register and assessing the level of compliance of key obligations. Council applies a risk-based approach to managing compliance, with assessments focused on obligations that present the greatest risk to Council. These practices support an enterprise compliance management approach that will help managers, obligation owners and staff understand their key compliance obligations.

5.2 Scope of the compliance management framework

This framework covers statutory (legislative and regulatory) compliance obligations. These obligations will be maintained in a centralised Statutory Obligations Register and have identified owners.

5.3 Compliance culture

Compliance culture can be described as the values, ethics, beliefs, knowledge, attitudes and understanding of compliance throughout an organisation. The foundations to building Council's compliance culture is supported by:

- Council's risk appetite statements
- requirements and activities outlined in this framework
- Logan City Council Code of Conduct for Staff.

5.4 How Council manages compliance

Council's approach to compliance management is aligned with the ISO 37301:2021 Compliance Management Systems. It outlines the compliance management process from gaining an understanding of the organisational context, through to assessing levels of compliance and managing instances of non-compliance. The ISO 37301:2021 compliance management process is illustrated in Figure 2.

Figure 2 Elements of a Compliance Management System

5.5 Statutory Obligations Register

Developing a centralised statutory obligations register will help Council progress and embed the key elements outlined in the ISO 37301:2021 standard. It will capture:

- key information that will ensure Council has a better understanding of its organisational context, from a compliance perspective
- performance evaluation results
- actions planned to address non-compliances
- improvement opportunities.

The register will provide all employees and contractors with an awareness and understanding of legislation relevant to their functions. It also allocates accountability for legislative compliance. The Risk and Compliance Program will develop and maintain this register in consultation with managers and obligation owners. The register will include updates to statutory requirements as necessary.

Details to be recorded in the statutory obligations register include:

- name of the relevant act or regulation
- directorate(s) and branch(es) impacted by the legislation
- the obligation owner and manager responsible for overseeing compliance with the requirement
- details of relevant policy and procedures to assist Council in maintaining compliance
- an assessment of level of compliance

- if non-compliant, the actions to be progressed to be compliant and regulatory reporting requirements, if applicable.

5.6 Accountability

Council's corporate value of excellence highlights the organisation's accountability for achieving excellent outcomes. Council is required to comply with requirements set out in legislation, regulations, and standards. These requirements are enforced by a regulator or standards board. A number of these requirements are also subject to reporting to the relevant regulator. For example, if there has been significant non-compliance with a legislative requirement, the breach will be reported to the relevant regulator. This may result in a financial or criminal penalty being applied.

5.6.1 Internal reporting and investigation

- Non-compliance with legislation, or standards, must be disclosed to the Risk and Compliance Program. The program will assist the branch manager with root cause analysis to determine actions required to remediate the non-compliance.
- A non-compliance may be identified by a finding in a review or audit.
- A non-compliance may be disclosed anonymously.
- A reported non-compliance will be risk assessed for importance and consequence to Council.
- Where a non-compliance results in a reportable breach to a regulator, the relevant branch manager, in consultation with the Risk and Compliance Program, will recommend treatment for restoring compliance.
- Taking a risk-based approach, non-compliances will have a compliance treatment plan developed in consultation with the Risk and Compliance Program.
- Consultation will occur to mitigate negative effects in other areas of Council.

5.6.2 External notification of reportable and notifiable breaches

Reportable and notifiable breaches are to be reported to the relevant regulatory authority as required.

5.7 Monitoring, review and reporting

Ongoing monitoring and review of the statutory obligations register and identified non-compliances is essential for Council to maintain compliance with statutory obligations.

Once the statutory obligations register is established, regular reporting to the ELT and the Audit and Risk Committee will also be established. This will include:

- compliance breaches that are reportable to a regulator
- significant changes to legislation or regulation and their effect to Council
- compliance improvement activities and recommendations
- key performance indicators for compliance management.

Appendix 1: Risk tools

A. Consequence/impact table

Risk category	Negligible	Minor	Moderate	Major	Catastrophic
Service delivery Risks associated with: • communication, data, technology • software, hardware, records • infrastructure, assets, property, buildings, equipment, plant, fleet, supplies • project management: scope quality, risk management, stakeholder consultation and communication, procurement, governance.	• Minor issue with communication, information systems, technology, records, assets, facilities, or infrastructure. • Service interrupted briefly. • No impact on external customers. • Minor, localised workforce issues. • Completion/success of the project could be impacted by time or cost increases less than 5%. • All requirements of effective project management in place. • Insignificant / minor damage to assets or property / facilities (incident report only submitted).	• Temporary restriction of access or disruption to essential services or critical business functions for less than one day. • Localised workforce issues. • Business Continuity Directorate Recovery Plan is reviewed. • Completion/success of the project could be impacted by time or cost increases 5% to 10%. • Effective project management is in place, with additional internal and external stakeholder consultation required. • Slight or minor damage to assets or property/facilities.	• Restriction of access or disruption to essential services or critical business functions less than 2 days • Multiple sites impacted by workforce issues. • Business Continuity Directorate Recovery Plan is referenced. • Completion/success of the project could be impacted by time or cost increases 10% to 15%. • Inadequate scoping may lead to partial completion of project or achievement of outcomes. • Significant but temporary damage to assets or property/facilities.	• Restriction of access or disruption to essential services or critical business functions for 2 to 5 days. • Multiple sites impacted by significant workforce issues. • Master business continuity plan may be enacted. • Completion / success of the project could be impacted by time or cost increases 15% to 25%. • Sustained damage to assets or property/facilities lasting many months.	• Loss of access or disruption to essential services or critical business functions for more than 5 days. • Ongoing, significant workforce issues at multiple sites. • Master business continuity plan enacted. • Completion/success of the project *adversely* impacted by time or cost increases of more than 25%. • Long term or permanent loss of critical assets or property/facilities.
Finance and legal Risks associated with fraud, corruption, litigation, claims, contract management, intellectual property, operational budgets, procurement, contracts management, public liability, professional indemnity, insurance, cashflow and debt management.	• Loss of less than 1% of branch operational budget. • Loss of less than $50,000. • Budget variation manageable in the short term. • Temporary disruptions to delivery of products, services, or systems. • Low level legal issues managed internally, including civil claims. • Health and Safety Representative (HSR) issued Provisional Improvement Notice (PIN).	• Loss of 1% to 5% of branch operational budget. • Loss of $50,000 to $250,000. • Budget variation manageable, absorbed over current financial year. • Minor disruptions to delivery of products, services, or systems. • Minor legal issues including civil claims, non-compliance issues, breach of legislation which may lead to prosecution in the Magistrates Court. • Cease Work Notice/ Workplace, Health & Safety Queensland Improvement Notice.	• Loss of 5% to 10% of branch operational budget. • Loss of $250,000 to $750,000. • Impact on budget beyond current financial year, but manageable within the next financial year. • Restriction or disruptions to delivery of products, services, or systems over a short period. • Moderate breach of legislation. Escalated civil claims. Litigation in the District Court. • Workplace, Health & Safety Queensland Prohibition Notice.	• Loss of 10% to 20% of branch operational budget. • Loss of $750,000 to $2.5m. • Impact on budget with recovery over proceeding 2 or 3 financial years. • Severe delays or restriction to key products, services, or systems over a sustained period. • Major breach of legislation with consequences including large financial penalties and/or sanctions. Escalated civil claims. • Workplace, Health & Safety Queensland prosecution.	• Loss of more than 20% of branch operational budget. • Loss of more than $2.5m. • Impact on budget with recovery over proceeding 3 or more financial years. • Non delivery or loss of critical products, services, or systems over a sustained period. • Major litigation including class actions in the Supreme Court. • Significant fraud/corruption.

Risk category	Negligible	Minor	Moderate	Major	Catastrophic
Workforce, health and safety Risks associated with human resource management, organisational culture and change management. This includes risks that impact on the ability of employees to attend work and perform their duties (i.e. industrial action etc.). Includes injuries and illness to staff, contractors, and the public such as exposure to chemicals, vehicles, falls, and other workplace hazards.	• Lack of suitable candidates to fill key operational roles in a reasonable timeframe. • Isolated incidents of short-term decline in staff confidence/morale. • Isolated incidents individual staff unaware of their roles and responsibilities in relation to code of conduct. • Report only – minor incidents where no injury was sustained.	• Difficulty attracting and retaining key personnel. • Short term decline in staff confidence/morale. • Some understanding by staff of their obligation to work within specific legislative frameworks. • Limited understanding of several staff in relation to code of conduct. • Injury or illness where first aid treatment is required (can be administered by a GP, first aider or co-worker).	• Inability to attract and retain key personnel. • Frequent/medium term decline in staff confidence/morale. • Limited understanding by staff of their obligation to work within specific legislative frameworks. • Limited understanding of several staff in relation to code of conduct. • Injury or illness requiring treatment by a medical practitioner.	• Low retention of key personnel. • Long term decline in staff confidence/morale. • Lack of understanding by staff of their obligation to work within specific legislative frameworks. • Lack of understanding of several staff in relation to code of conduct. • Injury or illness requiring treatment by a medical practitioner or hospitalisation, and where a full work shift or more is lost. • Any notifiable event to Workplace, Health & Safety Queensland or the Electrical Safety Office regulator	• Significant loss of several key personnel. • Significant ongoing lack of staff confidence and low staff morale across the organisation. • Severe lack of understanding by staff of their obligation to work within specific legislative frameworks. • Significant lack of understanding of several staff in relation to code of conduct. • Permanent disability. • Long term hospitalisation. • Life threatening event/death.
Politics, leadership and governance Risks associated with political influence, governance, management, complaints, auditing, performance, resource accountability, service level agreements, strategic and operational planning, compliance with statutory obligations (i.e. legislation, regulation), codes of practice, directives, delegations, policies, local laws, code of conduct – staff and Councillors.	• Internal political/leadership issues. • Community is unconcerned. • Effective governance and decision making. • Positive working relationships with other levels of government. • Non-compliance with legislation, regulations, directives, policies, code of conduct, procedures, etc requiring limited internal rectification.	• Political or leadership issues result in community concern. • Challenges identified with leadership and governance. • Decision making has potential to disrupt service delivery in one branch. • Introduction of new legislation impacts service delivery in one branch. • A 'working' relationship exists between Council and other levels of government. • Non-compliance is managed internally without penalties or prosecution.	• Political or leadership/management issues result in ongoing community concern. • Ongoing challenges with leadership/management. • Decision making has potential to disrupt service delivery in multiple branches. • Introduction of new legislation impacts service delivery of multiple branches. • Disagreement between Council and other levels of government. • Non-compliance or policy failure is investigated (internally/externally) and is resolved without financial penalties or prosecution. • Decision made re individual consequences.	• Political or leadership/management issues result in escalation of community concerns. • Instability recognised in leadership/management. • Decision making causes disruption to service delivery of one branch. • Introduction of new legislation impacts service delivery across Council. • Ongoing disagreement between Council and other levels of government. • Non-compliance requires formal, external investigation. High possibility of financial penalties and/or prosecution (individual/corporate). • Decision made re individual suspension or termination.	• Ongoing political or leadership/management issues result in escalation of community concern for a sustained period. • Ongoing instability in leadership/management. • Decision making causes disruption to service delivery across Council. • Introduction of new legislation significantly impacts service delivery and capacity to ensure compliance across Council. • Ongoing disagreement results in irreparable damage between Council and other levels of government. • Formal, external investigation of non-compliance results in financial penalties and prosecution (individual or corporate), including imprisonment. • Termination of individual.

Risk category	Negligible	Minor	Moderate	Major	Catastrophic
Reputation and community expectation Risks associated with Council's perceived or actual reputation with the community, media exposure, social media, feedback from community and stakeholder engagement.	• Predominantly local publicity. • Positive reputation maintained. • Positive relationships with media stakeholders. • Isolated social media communications. • Some attention from minor stakeholders with little to no publicity, but able to be resolved by routine management processes without impact to Council's reputation. • Stakeholder engagement occurs. • Community expectations known. • Minimal local feedback.	• Periodic, local, adverse publicity. • Identified that service delivery may be impacted by media scrutiny. • Limited damage to Council's reputation; minor one-off negative local publicity or visible dissatisfaction with Council by local stakeholder groups. • Positive relationships with media stakeholders maintained. • May cause some social media or formal complaints (justified or unjustified). • Active stakeholder engagement. • Community expectations not fully known or understood. • Divergence between policy and public opinion identified.	• Some negative publicity or short-term damage to Council's reputation at state-wide level. • Disruption to some core Council services resulting in the potential loss of public confidence in Council's processes. • Sustained reputation variances in the community. • Relationships with media stakeholders may be strained. • Significant social media and/or formal complaints. • Unsuccessful stakeholder engagement. • Community expectations are not fully known or understood. • Clear divergence between policy and public opinion.	• Negative publicity or short-term damage to Council's reputation at state-wide level resulting in CEO involvement and potential state Premier/Minister inquiry. • Disruption to major Council services resulting in the loss of public confidence in Council's processes. • Damage to reputation in the community. • Publicity may lead to an audit, inquiry, or other legal proceedings. • Impact of strained relationships with media stakeholders known. • Mass and extended adverse social media coverage. • Stakeholder engagement fails. • Community expectations are not known or understood. • Escalating community concerns or complaints. • Community campaigning may occur. • Major divergence between policy and public opinion.	• Significant and sustained negative publicity or damage to Council's reputation at national level resulting in senior staff resignation, public inquiry or sustained long tern loss of public confidence in Council's processes. • Media scrutiny adversely impacts service delivery. • Sustained damage to reputation in the community. • Ongoing exposure may lead to audit, inquiry, or legal proceedings. • Irreparable damage to relationships with media stakeholders. • 'Viral' adverse social media coverage (e.g. hashtag on Twitter). • No stakeholder engagement. • Escalating, ongoing community concerns or complaints. • Active community campaigning. • Loss of community support. • Total divergence between policy and public opinion.
Emergency and disaster response Risks associated with pandemic, terrorism, environmental spills, hazardous substances, evacuations, fire, flood, storms, threats, toxic releases, chemical spills.	• No emergency or disaster response required by Council. • No interruption to service. • Inconvenience to localised operations.	• Emergency or disaster response required by Council results in disruption to service delivery of one branch for up to one day. • Review of business continuity plan recommended. • Some disruption manageable by altered operational routine. • Reduction in operational routine.	• Emergency or disaster response required by Council resulting in disruption to service delivery for multiple branches for up to one day. • Reference to Master Business Continuity Plan required.	• Emergency or disaster response required by Council resulting in disruption to service delivery for multiple branches for one to 5 days. • Master Business Continuity Plan may be enacted.	• Emergency or disaster response required by Council resulting in disruption to service delivery for multiple branches for more than 5 days. • Master Business Continuity Plan enacted.

Risk category	Negligible	Minor	Moderate	Major	Catastrophic
Environment Risks associated with Council's operations that have potential or actual negative environmental or ecological impacts, regardless of whether these are reversible or irreversible in nature.	• Minor breach of policy or procedures. • Minimal environmental damage is immediately remediated with minimal resources.	• Minor localised impact: one-off situation easily remedied. • Minor environmental damage is immediately remediated with minimal resources.	• Long term impact on the environment and/or culture. • Able to be contained with specialist assistance. • Investigation by Department of Environment and Science and/or warning letters. • Increased supervision of environmental authorities for key business activities • Moderate impact on the environment; no long term or irreversible damage. • May incur cautionary notice or infringement notice.	• Severe long-term impact on the environment and/or culture. • Investigation by Department of Environment and Science and/or penalties. • Strict supervision of environmental authorities for key business activities. • Severe impact requiring remedial action and review of processes to prevent reoccurrence. • Penalties and/or direction or compliance order incurred.	• Long-term, large-scale damage to habitat or environment. • Serious/repeated breach of legislation/licence conditions. • Cancellation of licence and/or prosecution.

B. Likelihood table

LIKELIHOOD	DESCRIPTION/EXAMPLES ** Select one column that is most appropriate for the assessment – it is not necessary to meet the criteria of all 3 columns		
Almost certain	The risk event will occur in at least 95% of occasions.	The risk event will occur multiple times a year.	The risk event will occur on most occasions.
Likely	The risk event will occur in 75% to 95% of occasions.	The risk event will occur once every year.	The risk event will probably occur on most occasions.
Possible	The risk event will occur in 30% to 75% of occasions.	The risk event will occur once every one to 5 years.	The risk event will likely occur at some time.
Unlikely	The risk event will occur in 10% to 30% of occasions.	The risk event will occur once every 5 to 10 years.	The risk event may occur at some time.
Rare	The risk event will occur in less than 10% of occasions.	The risk event may occur greater than every 10 years.	The risk event would only occur in exceptional circumstances.

C. Risk matrix

CONSEQUENCE / IMPACT RATINGS						
LIKELIHOOD		Negligible	Minor	Moderate	Major	Catastrophic
	Almost certain	Medium	Medium	High	Extreme	Extreme
	Likely	Medium	Medium	High	High	Extreme
	Possible	Low	Medium	High	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	High

D. Effectiveness of controls

Rating	Description
Effective	A high degree of reliance can be placed on the internal controls. The controls are operating effectively to mitigate, detect or prevent risk in all circumstances. High level of control monitoring in place. Control will mitigate the inherent risk to an acceptable level of residual risk.
Partially effective	A limited degree of reliance can be placed on the internal controls. The controls are operating effectively to mitigate, detect or prevent risk in most circumstances. Limited control monitoring in place. Control may mitigate the inherent risk to an acceptable level of residual risk.
Ineffective	No reliance can be placed on the internal controls. The controls are not operating effectively and do not prevent the risk from being realised. No control monitoring in place. Control will not mitigate the inherent risk to an acceptable level of residual risk.

E. Risk approval and acceptance

RISK RATING	ACTION REQUIRED	RISK AND ACTION APPROVER
Low	Risk is managed by existing controls, routine operations and procedures, with ongoing monitoring.	Branch manager.
Medium	Risk is managed by existing controls, routine operations and procedures, with ongoing monitoring. Treatment actions to reduce the risk and / or prevent the risk from increasing, may be identified and tracked to completion.	Branch manager.
High (within Council's Risk Appetite)	Risk is managed by existing controls, routine operations and procedures, with ongoing monitoring. Treatment actions to reduce the risk and / or prevent the risk from increasing, may be identified and tracked to completion. Escalation is required to the relevant director, through the relevant manager for further review and approval.	Approval from relevant director required before commencing task (branch manager > director).
High (outside of Council's Risk Appetite)	Risk may be managed by existing controls, routine operations and procedures, with ongoing monitoring. Treatment actions to reduce the risk and / or prevent the risk from increasing, must be identified and tracked to completion. Escalation is required to the CEO/ELT (Manager > Director > CEO/ELT) for further review and approval.	Escalation is required to the CEO/ELT (branch manager > director > CEO/ELT) for approval.
Extreme	Avoid the related activities that relate to this risk. If, however, activities related to this risk are required for Council, there must be existing controls, routine operations and procedures, with ongoing monitoring. Treatment actions to reduce the risk must be identified and tracked to completion. Escalation is required to the CEO/ELT (Manager > Director > CEO/ELT) for further review and approval. CEO/ELT may escalate to Council if required.	Avoid the related activities if possible. Do not commence activities. Escalation is required to the CEO/ELT (branch manager > director > CEO/ELT) for approval.