

Shire of Halls Creek Risk Management Policy

V1 9 March 2026

Shire of Halls Creek Risk Management Policy
Adapted from [Strathbogie Council Risk Management Policy May 2024](#)
V1, 9 March 2026

Table of Contents

Table of Contents.....	3
1. Purpose	1
2. Policy Statement.....	1
Application of this Policy	2
3. Accountability and Responsibilities	2
4. Enterprise Risk Profile Structure.....	3
5. Our Risk Management Approach	4
6. Risk Analysis and Escalation Criteria	4
7. Risk Register	12
8. Definitions	13
9. Related Policies and Legislation.....	15
10. Policy Review	15

1. Purpose

Through integration with the approved Risk Management Framework, the purpose of this policy is to:

1. establish the principles upon which our organisational risks are managed in accordance with the risk management standard, ISO 31000:2018 Risk Management Guidelines.
2. guide the integration of risk management driving continuous improvement into our organisational culture, daily business practices and strategic planning processes.
3. implement an approach to risk management that is fit for purpose at all levels throughout Council.
4. integrate risk-based decision-making across the elected Council and organisation for the benefit our community and stakeholders.
5. develop a culture of risk awareness, accountability and shared attitudes that promote a willingness and capability to manage risk at all levels across the organisation and elected Council.
6. create an effective risk management framework so that all staff understand the business risks in their area and actively manage those risks as part of their day-to-day activities.
7. clearly identify roles and responsibilities in creating and maintaining a robust risk management framework.

2. Policy Statement

This policy is a core component of Council's corporate policy framework and Risk Management Framework. Through this policy and associated documents, the Shire of Halls Creek Council confirms its commitment to establishing a system of risk oversight, management and internal control to identify, assess, monitor and manage material risks related to the conduct of its activities. Its aim is to:

- continually improve the management of risk;
- better understand the reward-to-risk balance; and
- reduce the risks to acceptable levels.

Wherever we operate we will develop, implement and maintain a system for all material risks that enable us to:

- identify, assess and manage risks in an effective and efficient manner;
- make decisions based on a comprehensive view of the reward-to-risk balance;
- provide greater certainty of the delivery of objectives; and
- satisfy our corporate governance requirements.

We will do this by:

- implementing a comprehensive and systematic risk assessment and reporting process across the organisation; and
- embedding risk management across all program areas, with an awareness instilled in all employees.

Council's approach to risk management will be:

1. proportionate to the size of the organisation, recognising the limitations on the resources of a remote shire, targeting effort and resources to the areas of highest priority.
2. integrated into all our activities and functions, therefore forming an integral part of all that we do and the way we deliver services.
3. agile, forward thinking and flexible in its design and application so that quick responses can be made to unexpected changes and events outside of Council's control.
4. focused on continuous learning and improvement.
5. compliant with our legislated obligations.
6. adding value through each step of the risk management process.
7. efficient to operate and maintain, avoiding administrative burden wherever possible.

Council accepts that, on occasion, even with sound risk management practices, things may go wrong. On such occasions, we will take the opportunity to review the reasons for the occurrence and endeavour to further strengthen controls to reduce the likelihood of a recurrence.

Application of this Policy

This policy applies to all areas of Council operations and is to be understood and implemented by all Councillors, staff, contractors and volunteers undertaking any function for or on behalf of Council.

3. Accountability and Responsibilities

Role	Responsibilities and accountabilities
Elected members	• Oversight of risk management at Council (including setting the Risk Appetite). • Oversight of the Audit, Risk and Improvement Committee.
Chief Executive Officer	• Overall accountability for risk. • Setting the tone, culture and expectations for risk management and governance activities. • Ensuring resources for risk management activities are adequate for Council purposes. • Setting appropriate delegations for the risk management function.
Audit, Risk and Improvement Committee	• The ARIC is a statutory committee established under the <i>Local Government Act 1995</i> and the <i>Local Government (Audit) Regulations 1996</i>, with expanded responsibilities following recent legislative reform, including the <i>Local Government Amendment Act 2024</i>. • Provides independent oversight of audit, risk management, internal controls, legislative compliance,

	financial reporting, performance and improvement activities across the organisation.
Internal audit	• Risk assurance to the Audit, Risk and Improvement Committee and CEO through execution of the internal audit, risk and improvement plan.
Executive Leadership Team	• Accountable for ownership and management of risks in their respective areas of responsibility. • Role modelling the tone, culture and expectations for risk management and governance activities. • Oversight of risk management across Council.
Risk Officer- Director Governance and Sustainability)	• Coordinating the risk management function. • Developing, implementing and maintaining a Risk Management Framework that is fit for purpose. • Risk reporting to the CEO and Audit, Risk and Improvement Committee. • Supporting the organisation to manage its risks through the provision of risk management advice and guidance to staff.
All Staff And Contractors	• Applying sound risk management practices in accordance with Council policies and frameworks.

4. Enterprise Risk Profile Structure

There are three levels of risk:

Level 1 Strategic and organisational risks

Strategic risks are forward looking and linked to the strategic objectives. The time horizon for these risks is typically the time horizon of the strategic community plan (i.e. ten-years). Strategic risks are few and externally focused. Organisational risks are linked to the strategic risk and are the risks that impede the delivery of strategic objectives.

A control not well designed or managed may be the source of a risk.

Organisational risks are internally focused and identify the critical controls required to enable the delivery of the strategic community plan.

Level 2 Operational risks

Operational risks are the risks focused on delivering business objectives, compliance objectives and are function based. The time horizon for these risks is aligned to the corporate business plan (i.e. four years). Operational risks are linked to strategic risks.

Level 3 Project risks

Project and event risks are risks linked to the delivery of a project and focus on changes to scope, budget, schedule and the project quality.

5. Our Risk Management Approach

Our approach to risk management involves the following four steps:



Throughout this process, communication and consultation with relevant stakeholders, staff and where appropriate the Audit, Risk and Improvement Committee and Elected Members through Council meetings, will be key to ensuring a comprehensive approach to managing and mitigating risk.

Risk assessments and their management must be living documents and at all times we will:

- Plan:** plan what departments and services should do to work safely. Review the strategic register and operational risk assessments.
- Implement:** put into practice the control measures to minimise the risk across the organisation. Controls can be in many forms including policies, procedures, technology, reporting or skill development/training.
- Monitor:** keep checking to see how well the control measures are working.
- Improve:** address any issues and find ways to make what the business does more effective.

6. Risk Analysis and Escalation Criteria

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including where appropriate, the level of risk.

The main objective of risk analysis is to separate the minor acceptable risks from the major ones and to provide data to assist in the evaluation and treatment of risk.

Risk analysis involves a detailed consideration of risk uncertainties, risk sources, consequence, likelihood, event, scenarios, controls and their effectiveness.

When determining the likelihood or consequence of a risk occurring, it is important to take into consideration existing controls.

6.1 Risk rating

A risk analysis will result in an overall risk rating.

A full, accurate and objective assessment of any identified risk must be undertaken to:

- evaluate the effectiveness of existing controls.
- determine the consequences of the risk.
- determine the likelihood of consequences occurring because of a specific risk.
- determine the level of risk to judge its importance or acceptance to the organisation.

- prioritise risks based on their assessed level and the organisation's tolerance of the risk.
- identify remedial actions and allocate appropriate resources for risk treatment.

There are two main factors applied when analysing risks – consequences and likelihood.

6.2 Determining consequences

The consequence of a risk can usually be expressed as a measure of financial loss, impact upon achieving business or project initiatives, reputational damage or safety.

Consequences are usually determined on the basis of “most credible worst-case scenario” recognising that “worst case scenario” is not usually what is experienced.

The estimation of consequence needs to be done in full consideration of the effectiveness of the risk controls already in place. Criteria for assessing the consequences of a risk are summarised in Table 1

.

Table 1: Determining risk consequences

Risk category	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Assets, infrastructure, and Projects	Isolated, insignificant damage and impact on assets and infrastructure including heritage listed	Minor damage and impact on assets and infrastructure including heritage listed buildings. Minor inconvenience, dissatisfaction in community.	Moderate damage and impact on assets and infrastructure. Moderate inconvenience, increased	Considerable damage to assets and infrastructure Significant inconvenience and high-level dissatisfaction.	Total loss of critical assets and infrastructure including heritage listed buildings for an extended period of time. Severe impact to staff.
Climate/Natural Environment	Minor release of pollutants which does not require notification to third parties – brief nonhazardous temporary pollution	Required to inform EPA – Contained temporary pollution	Significant release of pollutants – residual pollution requiring clean-up work	Major release of toxins/water resulting in high compensation or reconstruction costs Likelihood of legal prosecution by EPA	Major release of toxic waste resulting in long term damage to the environment
Compliance and regulatory	Negligible legal issues, No Non-Compliance or breaches.	Minor legal issues, Non-Compliance. Minor losses or damages incurred	Breach of legislation. Possible prosecution or fine.	Major breach of legislation. Probable fine and litigation.	Significant prosecution resulting in fines and/or possible incarceration.
Financial sustainability	Cost to Council- < \$50,000	Cost to Council- < \$50,000	Cost to Council- \$200,000 to \$1M Fines to Council personnel	Cost to Council- \$1M to \$5M Council officer or Councillor convicted	Cost to Council- > \$5M Curbing of programs required due to significant shortfall in revenue or blow out in expenditure. Intervention by relevant Minister

Governance	Inefficient operations, wasted resources Delayed detection of financial distress No breach; negligible legal impact No public impact; minimal internal concern Negligible financial impact; handled within routine processes	High staff turnover and inability to attract talent due to a toxic or ineffective corporate culture. Minor adverse publicity; manageable stakeholder concern Minor breach Low level financial impact; manageable budget variance	Non-compliance with penalties; breach of contract Increase in accident and injuries Local media coverage, noticeable community and stakeholder dissatisfaction 5-10% EBIT loss; significant cost overruns Organisation vulnerable to fraudulent behaviour	Significant breach, litigation or regulatory action. Serious damage to reputation Long term stakeholder and community concern 10-15% EBIT loss; severe budget impact Organisation open to allegations of fraudulent behaviour	Greater than 15% EBIT loss; Organisation placed into administration Potential for directors and officers to face personal fines or jail time for breaching their duties. Major breach, prosecution, public scandal, permanent loss of stakeholder and community trust National media coverage Fraud confirmed; CCC and WAPOL intervention
Land Tenure	Negligible impact on land use Minor delay in land registration; no operational disruption	Low level impact; manageable Short term restriction on land access; minor breach of lease conditions with no fines	Medium level impact; requires intervention Delay in project approval due to native title issues, minor reduction in agricultural productivity	High level impact; significant damage/loss Long term suspension of land use; legal action; significant financial penalties; Breach of environmental regulations	Permanent or irreversible damage; Permanent forfeiture of tenure; permanent loss of access; catastrophic environmental damage; major social/community conflict
People, Health and Safety	Medical treatment injury Temporary, minor health impact on staff or public	Multiple medical treatments or lost time	Health impact on member of the public or staff member- more than 10 days rehabilitation required	Loss of key member of management team- serious health impact on multiple members of staff or public	Multiple or single fatalities- public or staff. Loss of a significant number of employees
Political, reputation and trust	Marginal impact on Council operations	Inadequate probity being exercised.	Public/media negative attention	Public/media concern	Public/media outrage

	Minimal to no effect on reputation- Resolved in day-to-day management	Minor/isolated concerns raised by members of public, customers, suppliers	Local community concern Customer or supplier concern	Damage to Council's reputation Council subject to formal inquiry/sanction	Public pressure to curtail operations of Council
Service Delivery	Business disruption or loss of a critical service for up to 4 hours Low impact to Service Delivery, minimal disruption and inconvenience to customers, buildings. Minimal impact to staff, stakeholders and the community.	Multiple medical treatments of lost time Business disruption or less of a critical service for between 4-24 hours. Minor disruption to non-critical services	Business disruption or loss of critical service for between 1-3 days. Disruption to non-critical services. Moderate inconvenience to customers.	Disruption or loss of critical service for > 3 days. Significant disruption to delivery on non-critical services for several weeks. Significant impact to customers and elevated levels of dissatisfaction.	Business disruption for > 1 week. Complete disruption to Council services for several months. Critical inconvenience to customers and Community.
Technology and Cyber Security	Minor disruption to system with no downtime Negligible impact on service provision	Disruption to system with some downtime Insignificant impact on generation of information Brief service interruption (1 day)	Temporary loss of key data Impact on generation of management information Temporary recoverable service failure Interruption of service (2 days)	Serious disruption to system leads to more than 3days downtime (loss of key data and customer support) Service or provider needs to be replaced. Cyber Attacks	Sustained Cyber Attacks leads to collapse of major system leading to unrecoverable loss of core data. Service removed or unable to function for over one week.

6.3 Determining likelihood

The “likelihood” of a risk happening is the likelihood of an event occurring with a particular consequence as determined above. An estimation of likelihood is based on a consideration of the effectiveness of the controls known to be in place. As with determining consequence, it is the likelihood of an event occurring with the predetermined “most credible worst-case scenario.

The following table outlines how, in the current control environment, the likelihood that a risk will occur is to be estimated.

Table 2: Evaluating likelihood

Likelihood	Recurrent Risks	Single Event
1. Rare	Only occur as a “100-year event”	May only occur in exceptional circumstances – probability very small, close to zero
2. Unlikely	Could occur in “years to decades”	May occur but not anticipated – probability low but noticeably greater than zero
3. Possible	Could occur within “months to years”	Might occur at some time – less than 50% chance but still quite high
4. Likely	Could occur within “weeks to months” or may arise about once per year	Will probably occur in most circumstances – at least 50/50 chance or greater
5. Almost certain	Risk is occurring now, or could occur within “days to weeks”, or could occur several times per year	Is expected to occur in most circumstances – probability high (e.g., greater than 90%)

6.4 Calculating Overall Risk Rating

Evaluating risks involves determining what risks can be tolerated and those that cannot.

The overall risk rating (RR) is a product of the likelihood (L) multiplied by the consequence (Severity) of the risk as outlined in Table 3.

Table 3: Overall Risk Rating Matrix

		Consequence				
		Insignificant (rating 1)	Minimal (rating 2)	Moderate (rating 3)	Major (rating 4)	Catastrophic (rating 5)
Likelihood	Almost certain (rating 5)	Medium (5)	Medium (5)	High (15)	High (20)	High (25)
	Probable (rating 4)	Low (4)	Medium (8)	Medium (12)	High (16)	High (20)
	Possible (rating 3)	Low (3)	Medium (6)	Medium (9)	Medium (12)	High (15)
	Unlikely (rating 2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium (10)
	Rare (rating 1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
	Opportunity (best practice/ improvement)	Opportunity (0)	Opportunity (0)	Opportunity (0)	Opportunity (0)	Opportunity (0)

6.5 Risk Appetite

The risk appetite is the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives. It is best described as an organisation's pursuit of risk or its willingness to take risks rather than avoiding them. This is because it is extremely difficult to introduce control measures to eliminate risks altogether.

The Risk Management Framework provides guidance on our risk appetite through stating that Council will take measured risk, informed by a robust risk management framework to inform decision making.

The table below identifies the definitions for our risk appetite and the levels of intervention required for each.

Table 4: Risk tolerance and intervention levels

HIGH risk: 15- 25	Issue represents a control weakness, which could cause or is causing major disruption of the process or major adverse effect on the ability of the process to achieve its objectives. Requires significant senior management intervention and should be reported to Executive Team Leadership immediately. Potential for resource diversion and may require possible external assistance. Requires high priority to be actioned within 0 – 3 months.
MEDIUM risk: 5- 12	Issue represents a control weakness, which could cause or is causing moderate adverse effect on the ability of the process to achieve its objectives. Requires prompt escalation to responsible Management Group as may require possible external assistance. Requires prompt action. Response required within 0 – 6 months.
LOW risk: 1- 4	Issue represents a minor control weakness, which is minimal but reportable impact on the ability of the process to achieve its objectives. Requires management attention and possible use of external resources. Requires action commensurate with the process objectives. Response required as soon as practicable.
Opportunity: 0	Issue represents a best practice improvement, which is not addressing an identified risk but looking to improve efficiencies and business practices. Requires review by management with a view to implement if considered practical and beneficial.

6.6 Risk Treatment

Once the overall risk rating and the intervention level have been identified, attention then moves to risk treatment options.

Strategic risks are managed through the Strategic Risk Register, which is reviewed by the Executive Leadership Team and the Audit, Risk and Improvement Committee on a quarterly basis, and then submitted to Council for review and consideration.

The Operational Risk Register and the risk profile are managed by the Risk Officer, who records and monitors treatment activities. The key elements of this system are recording:

- Risk – What could happen and how serious could it be?
- Causes – Why/how could the risk event happen?
- Controls in place- What is in place to mitigate/manage the risk?
- Control effectiveness rating – When was the control last reviewed and how effective was it at managing the risk?
- Current risk rating – Given the effectiveness of risk controls, how significant is the risk now?
- Treatment- What more needs to be done to manage the risk? Depending on the materiality of the current risk exposure there are several risk treatment options available.

Risk treatment options, as defined by the Risk Management Framework, are detailed in the below table.

Table 5: Risk Treatment Options

Decision	Indicators
Remove/avoid the risk	Removing the risk by not proceeding with the policy, program or activity or choose an alternate means of action.
Retain/accept the risk	Council has made an informed decision not to treat the risk, because: a) the cost of controlling outweighs the benefits from controlling the risk, or b) there are no effective controls available to reduce or eliminate the risk. Where any risk ranked low or above are accepted, justification of acceptance is required, and a record included in the risk register system.
Treat the risk	Decide to apply controls or other mitigating activities designed to reduce the likelihood and/or consequences of the risk event occurring.
Transfer/share the risk	Share the responsibility with another party such as an insurer/contractor who shares the loss if the risk event were to occur.
Increase the risk	Consciously taking on risk to pursue an opportunity and achieve desired outcomes of a strategy, project or initiative.

7. Risk Register

Project Risks are recorded for each project from the inception stage.

Operational risks are identified by staff teams and documented with the assistance of the Risk Officer. The system is used by teams at the operational level to record risks, record and monitor treatment activities, assign responsibility for treatments, monitor treatments, record control effectiveness assessments and generate risk reporting. Internal Audit uses the Operational Risk Register to help develop the Internal Audit Program.

Strategic and whole of Council risks are currently recorded in an excel spreadsheet but will be transitioned to a digital platform as part of the Shire's ICT upgrade. Reports generated will be used as the basis for reporting risks to the Audit, Risk and Improvement Committee and to Council Meetings.

Key fields in the risk register are:

- **Risk** – What could happen and how serious could it be?
- **Causes** – Why/how could the risk event happen?
- **Controls in place** - What is in place to mitigate/manage the risk?
- **Control effectiveness rating** – When was the control last reviewed and how effective was it at managing the risk?

- **Current risk rating** – Given the effectiveness of risk controls, how significant is the risk now?
- **Actions** - What more needs to be done to manage the risk? Depending on the materiality.

Please note that the Shire will move from this manual way of doing things to a digital platform that will allow us to assess, manage, monitor and report in a more efficient and timely manner. Digitalisation is expected to be completed late 2026.

8. Definitions

Term	Meaning
Audit, Risk and Improvement Committee	means the committee established under the <i>Local Government Amendment Act 2024</i> .
Audit, Risk and Improvement Committee terms of reference	means the Audit, Risk and Improvement Committee (ARIC) Terms of Reference that sets out the purpose, authority, responsibilities, membership and operating procedures of the Committee. The ARIC provides the governance framework that guides how the Committee carries out its role in supporting Council and the Chief Executive Officer with independent oversight of audit, risk management, internal controls, legislative compliance and organisational improvement. The Terms of Reference define the Committee's scope of responsibilities, reporting arrangements and meeting protocols to ensure the Committee operates effectively and in accordance with the <i>Local Government Act 1995</i> and the <i>Local Government (Audit) Regulations 1996</i>.
Administrative Procedures Handbook	means the document developed to provide clear internal guidance for all staff on how the Audit, Risk and Improvement Committee is to be supported, coordinated and administered.
Control	means a measure that maintains or modifies risk. It can take many forms, for example a control may be policies and procedures (providing instruction), technology (systems), reporting, or people (capability) controls that reduce the consequence and or rectify a failure after it has been discovered, such as continuous improvement actions, crisis management, business continuity and or disaster recovery plans and insurance.
Council	means the Shire of Halls Creek Council
Risk Management Framework	means the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. It includes procedures for the day-to-day implementation of risk management.
Executive Leadership Team	means the direct reports to the Chief Executive Officer

Level of Risk	means the magnitude of a risk or combination of risks expressed in terms of the combination of severity/consequences and their likelihood of occurring.
Likelihood	means the chances of something happening.
Severity/Consequence	means the outcome of an event affecting Council objectives – it can be certain or uncertain and have either a positive or negative direct or indirect affect.
Management Group	means the group comprised of managers and coordinators
Monitoring	means continual checking; supervising, critically observing or determining the status to identify change from the performance level required or expected.
Operational Risk	means a risk which occurs in or hampers or effects an individual team or function within Council in achieving its plans
Residual Risk Rating (RRR)	means the risk remaining after risk management treatments and controls have been applied.
Risk	means how uncertain future events could influence the achievement of Council's strategic and operational objectives.
Risk Analysis	means the process to comprehend the nature of the risk and to determine the level of risk.
Risk Appetite	means the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives. It is best described as an organisation's pursuit of risk or its willingness to take risks rather than avoiding them.
Risk Management	means coordinated activities to direct and control an organisation in relation to risk.
Risk Management Plan	means the scheme within the risk management Framework specifying the approach, components and resources to be applied to the management of risk
Risk Owner	means the person or entity with the accountability and authority to manage a risk and implement controls to mitigate the risk.
Risk Tolerance	means the level of risk that Council is prepared to accept before action is considered necessary to reduce it and represents a balance between the potential benefits of a calculated risk and the threats that inevitably brings
Strategic Risk	means a risk that will affect or hamper the organisation in its ability to operate or deliver its services.

9. Related Policies and Legislation

Related policies and legislation include but are not limited to the following:

- *Local Government Act 1995 (WA)* and subsidiary legislation including local government regulations
- *Local Government Amendment Act (WA) 2024*
- ISO 31000:2018 Risk Management – Guidelines
- Shire of Halls Creek Risk Management Framework
- 2026 – 2036 Shire of Halls Creek Strategic Community Plan
- Shire of Halls Creek Business Continuity Plan (2026 – 2030)
- Audit, Risk and Improvement Committee terms of reference
- Administrative Procedures Handbook
- Shire of Halls Creek Delegations Policy
- Shire of Halls Creek Employee Code of Conduct
- Code of Conduct for Elected Members
- Code of Conduct – Behavioural Management (Council Members, Committee Members and Candidates)
- Separation of Duties Policy (*Local Government Amendment Act 2024*)
- Fraud and Corruption Policy

10. Policy Review

Council may review this policy at any time and at least annually from the date of adoption or the completion of the last review.

Minor amendments to the policy may be authorised by the CEO at any time where such changes do not alter the substance of the policy (e.g., a change to the name of a related document, or a change in legislation).