BYRON
SHIRE
COUNCIL

DRAFT - Strategy

Risk Management 2023

INFORMATION ABOUT THIS DOCUMENT
(INTERNAL USE ONLY)

Date Adopted by Council		**Resolution No.**	
Document Owner	Director Corporate and Community Services		
Document Development Officer	Manager Corporate Services		
Review Timeframe	Annually		
Last Review Date:	March 2023	**Next Scheduled Review Date**	March 2024

Document History

Doc No.	Date Amended	Comments
E2023/14734		New Document

Further Document Information and Relationships

Related Legislation/Regulation	NSW Local Government Act 1993 Civil Liability Act 2002 Work Health and Safety Act 2011 Australia/New Zealand Standard for Risk Management (AS/NZS ISO 31000:2018) OLG - Guidelines for Risk Management and Internal Audit for Local Government NSW NSW Treasury Guidelines for Risk Management (TPP 015)
Related Policies	Risk Management Policy 2023
Related documents	Enterprise Risk Management Framework – as outlined in Risk Management Policy 2023

Contents

Introduction 4
Objectives 5
Scope 5
Roles and Responsibilities 6
Risk Appetite Statement 7
Cautious 8
Moderate 8
Council's Risk Profile 9
Climate Change 9
Risk Management Process 10
Communication and Consultation 10
Establishing Context 10
Risk Assessment 11
Risk Identification 11
Risk Analysis 12
Likelihood Descriptors 12
Consequence Table 13
Risk Evaluation 15
Risk Treatment 15
Controls 16
Mitigating Actions 16
Residual Risk Rating vs Target Risk Rating 16
Risk Registers 16
Monitoring and Review 17
Key Risk Activities 18
Training 19
Future Actions 19
Legislative and Strategic Context 19

Introduction

Byron Shire Council (Council) is committed to embedding an integrated, consistent, and sustainable approach to risk management. Effective risk management supports the achievement of objectives set out in the *Community Strategic Plan 2032*, improves service delivery, supports well-informed decision making and contributes to the success of the Council and the community.

Council has adopted an enterprise-wide approach to risk management which is supported by an Enterprise Risk Management Framework (ERMF). Where traditional risk management tends to focus on risk avoidance, enterprise risk management takes stock of potential risks and identifies which ones are worth taking, allowing a focus on opportunity. The ERMF integrates the processes for managing risk into Council's overall governance, strategic objectives, and planning.

Council's approach to risk management is consistent with the guidelines outlined in *AS ISO 31000:2018* and recognises the need to apply the following principles:

- ✓ Risk management is integrated into Council's processes.
- ✓ Risk management is structured and comprehensive.
- ✓ Risk management is customised to Byron Shire Council's needs.
- ✓ Risk management is inclusive and transparent.
- ✓ Risk management is dynamic and responsive to change.
- ✓ Risk management takes into consideration the best available information.
- ✓ Risk management considers human and cultural factors where practicable.
- ✓ Risk management encourages and drives continuous improvement.

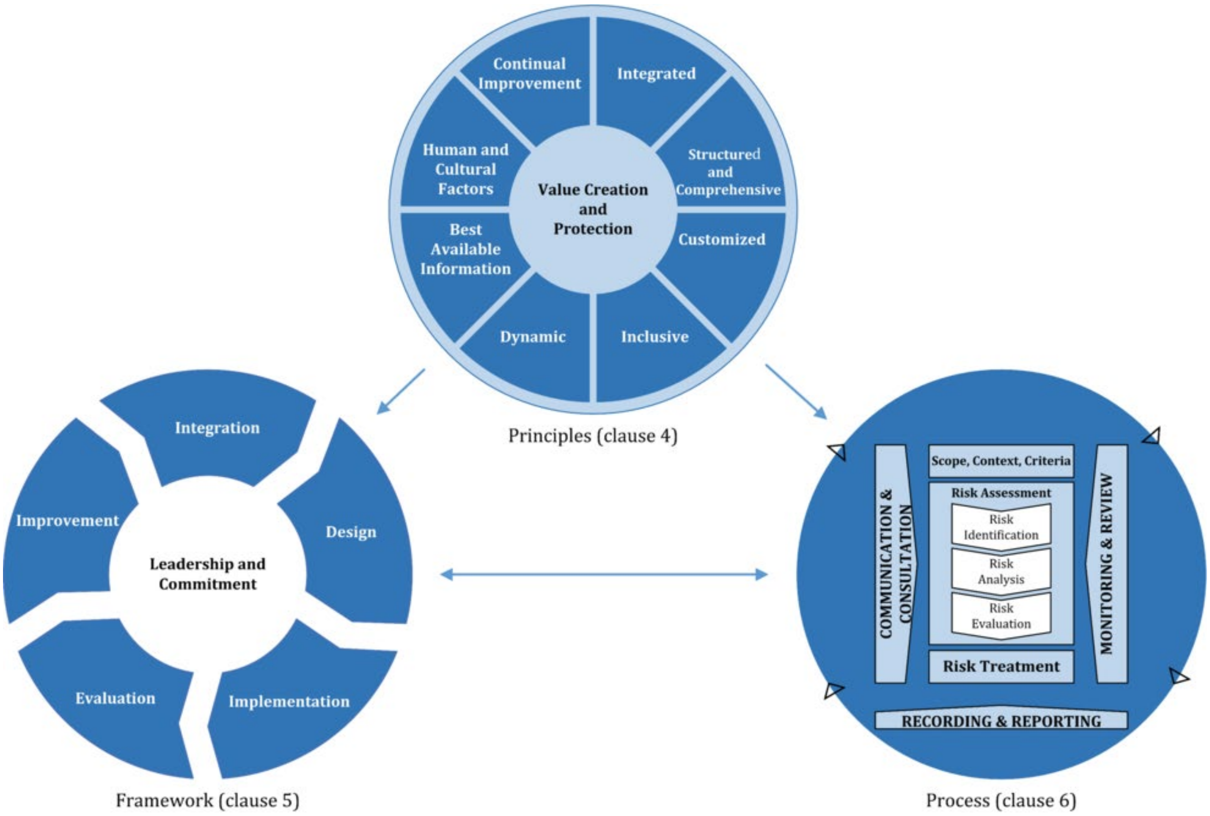

Figure 1 — Principles, framework and process (AS ISO 31000:2018)

Objectives

AS ISO 31000:2018 defines risk as “the effect of uncertainty on objectives”; which can be both positive or negative. Risk can create opportunities or result in an unwanted outcome. Risk management is defined as the “coordinated activities to direct and control an organisation with regard to risk”.

Council’s Risk Management Strategy aims to provide an overview of Council’s risk management approach, including systems and processes to assist all staff, stakeholders, and Councillors to effectively manage enterprise risk. The strategy outlines the requirements and responsibilities of staff to ensure that the management of risk is a shared responsibility throughout the organisation.

The Risk Management Strategy supports Council to:

- safeguard Council’s assets; including people, property, information and financial resources through effective decision-making;
- identify and prepare for uncertain events to reduce their impact should they arise;
- ensure all Council employees assume responsibility for managing risk by embedding a positive risk culture;
- provide consistent terminology to aid, promote and improve understanding of risk;
- outline the tools, resources and training required to effectively identify and manage risk;
- identify and implement monitoring and reporting processes and methods of feedback;
- seek continuous improvement

Council activities where risk management practices can be utilised to improve outcomes include, but may not be limited to:

- strategic and operational planning
- projects management
- organisational culture
- decision making processes
- events
- disaster management
- fraud and corruption controls
- disclosure
- service provision
- business and financial processes
- policy formulation
- asset management
- procurement
- insurance
- business continuity
- health and safety
- environmental management
- information technology
- community and stakeholder engagement
- land use planning

Scope

This Strategy applies to all Councillors, employees, contractors and to any person or organisation that acts for or represents Council, including volunteers.

Roles and Responsibilities

Byron Shire Council supports a top-down approach to risk management and is committed to making the necessary resources available.

Role	**Responsibility**
Council	In accordance with the principle of good governance, Council has the responsibility to prudently manage risk in the exercise of policy setting and decision-making powers and considers risk management contained in Council reports. Adoption of the Risk Management Policy, including the Enterprise Risk Management Framework.
Audit, Risk and Improvement Committee	Comply with obligations outlined in OLG - Guidelines for Risk Management and Internal Audit. Provide independent assurance and assistance to Council on risk management, ensuring risks and exposures inherent to Council's activities and objectives are identified and managed. Periodic review of Risk Registers to advise on the adequacy of control measures.
Internal Auditors	Provide an independent review function to Council. In accordance with an agreed internal audit strategy and plan, the internal audit conducts regular reviews across Council's activities and identifies areas of risk and scope for improvement.
General Manager, Directors	Responsible for leading and maintaining an enterprise-wide risk management culture across the organisation and ensuring that the risk management policy and strategy are effectively implemented and embedded within Council's day-to-day business. The Executive Team are responsible for the management of Strategic Risks.
Managers, Team Leaders	Responsible to their Director for the risk management function within their area of responsibility. Strongly advocate and support a risk management culture. Continually identify, assess and manage risks relevant to their area of responsibility. Ensure all risk reviews and subsequent reporting is undertaken in a timely manner. Managers are responsible for the management of Operational Risks.

Strategic Risk Coordinator	Responsible for the day-to-day tasks required to implement Council's ERMF and to support all staff in the identification and management of risk. Oversight of Council's Strategic and Operational Risk Registers and relevant reporting to the Executive Team and Audit Risk and Improvement Committee. Coordination of risk awareness and risk training at staff induction and as required.
All Staff	Develop and maintain a sufficient understanding of Council's policies and supporting procedures and processes in relation to risk. Maintain an awareness of risks (current and potential) that relate to their area of responsibility. Raise additional risks for consideration by their supervisor/manager. Positively contribute to Council's risk management culture.

Risk Appetite Statement

ISO 31000 defines risk appetite as "the amount and type of risk that an organisation is prepared to pursue, retain or take". Risk is an inherent part of Council's activities and objectives. The Risk Appetite Statement considers the most significant categories of potential risks to Council and provides an outline as to how much risk Council is willing to accept in this area.

Council, its subcommittees, management, and staff (including contractors and volunteers) should consult Council's Risk Appetite in both strategic and operational decision making.

Risk Appetite

Minimal Risk Approach

Risk Positive Approach

	Cautious Preference for options that avoid risk or have low inherent risk	Moderate Preference for safe options with a low degree of residual risk for potential reward	Open Willing to consider all potential options, with a preference for innovation, leading to higher rewards
Financial	Conservative approach to avoid exposure to corrupt financial transactions or activities that contravene legislated or policy requirements.	📍	
People			Open to a diverse recruitment strategy that considers other sectors, experiences and innovation that would benefit Council and the community. 📍
Legal & Compliance	Minimal appetite for breaches of legal obligations or contractual agreements that result in fines, penalties, or reputational damage. 📍		
Environmental	Cautious appetite for environmental impacts arising from normal business activities, however open to innovative practices and services for the betterment of the environment and Byron Shire.	📍	
Workplace & Public Safety	Minimal appetite for work practices, actions, or inactions that compromise the wellbeing and safety of people, including staff and members of the public. 📍		
Business Systems & Technology	Adverse to exposure to cyber security threats and extended outages, while being open to the implementation of new technologies creating opportunity for business improvement.	📍	
Service Delivery			Focused on continuous improvement and opportunity to enhance service delivery and efficiencies for the community. 📍
Assets			Willing to trial new methods and technologies for asset maintenance, management, and renewals, even where long term outcomes may be unknown. 📍
Reputation	Unwilling to accept decisions or behaviour that may result in prolonged, adverse scrutiny from the media and/or community. 📍		

Council's Risk Profile

Council has identified Strategic Risk, Operational Risk and Project Risk as the three key groups of risks to be assessed.

Level	**Description**	**Risk Ownership**
Strategic Risks	Affect the sustainability of the organisation or its ability to deliver on the objectives of the Community Strategic Plan. Are significant risks that affect the longer-term interests of Council and the community. Are those impacted in the most part by external events.	Executive Team
Operational Risks	Relate to risks that may impact delivery of services and daily operations of each business unit. Can have short-term or long-term impact or be ongoing. Are those impacted by internal or external events.	Managers
Project Risks	Relate to the delivery of specific projects and are the risk of an uncertain event or condition on project outcomes. Impact the project itself, where the life of the risk is limited to project delivery. Are those impacted by internal or external events.	Project Manager in consultation with project sponsor

Climate Change

Building the preparedness of Council to respond to climate change risks is an emerging area of risk management. In 2020, Council engaged Statewide Mutual to facilitate Climate Change Risk Assessment workshops, making use of the projected impacts of climate variation that are specifically related to this region.

The outcome of these workshops is the Climate Change Adaptation Plan (The Plan) which aims to:

- Reduce the risk of projected climate impacts by delivering specific actions and planning measures within Council's operational control;
- Enhance community resilience and adaptive capacity before, during, and after climate events.

Integrating the actions from "The Plan" into Council's IP&R framework has been an essential step forward in our response to climate risks. Further integration into the enterprise risk framework will ensure Council's core functions are protected through better understanding of the impacts.

Risk Management Process

AS ISO 31000:2018 states “The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organisation”.

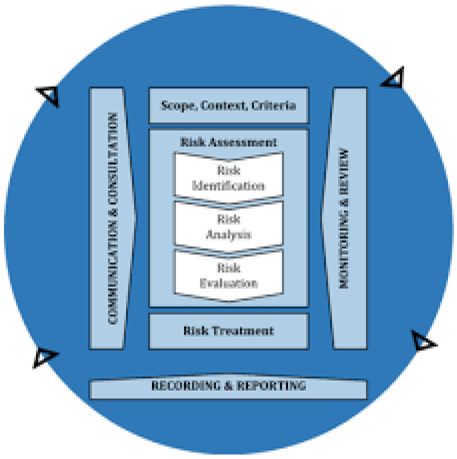

Figure 2 — Process (AS ISO 31000:2018)

<u>Communication and Consultation</u>

Council will effectively communicate and engage with all stakeholders to build a positive risk aware culture that encourages staff to proactively manage risks. This will assist to;

- improve the understanding of risk and risk management processes within the context of Council;
- ensure the timely identification of risks and the support required for treatment plans;
- ensure the interests of stakeholders are understood and considered;
- ensure that everyone is clear on their roles and responsibilities.

Council communicates its approach to risk management through its policy and strategy, on induction, in meetings and through regular reporting.

<u>Establishing Context</u>

Risk Management Context defines the goals and objectives of the risk management activity and requires an examination of the external and internal environments in which the risk identification, analysis and treatment options will be considered.

The external context relates to the environment in which Council operates and seeks to achieve its objectives including policy, operational, cultural, political, people, environmental, legal, regulatory, financial, technological and economic factors. Other things to be considered include key drivers and trends that impact upon the objectives, and the relationship with, and expectations of, the community.

The internal context includes those factors within Council that are relevant to the risk assessment. This is important as risk assessments will be most effective when they are linked to the objectives of Council or the activity under assessment. Factors typically considered in the internal context include the entity’s strategic objectives, organisational capabilities and culture.

Risk Assessment

Risk Identification

Risk identification is the process of identifying risks that may prevent Council or a business unit from achieving its objectives, and should consider:

- what might happen or what can go wrong?
- what would cause it to happen?
- what would the effect on Council's objectives be?

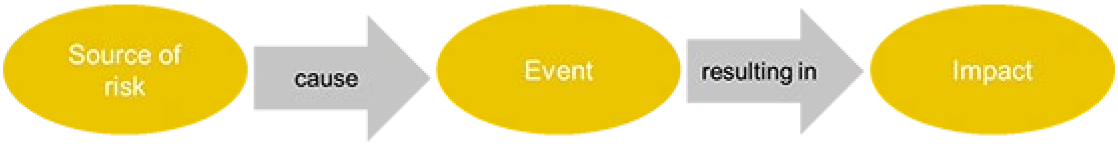

Figure 3 Adapted from TPP12-03: Risk Management Toolkit for NSW Public Sector Agencies

An example of an operational risk is:

"*Council processes a fraudulent request for payment by a third party due to inadequate payment verification processes, resulting in financial loss and reputational harm*".

The *JLT Public Sector Report for 2021* outlines the top 5 risks identified by NSW Local Government as follows:

Financial Stability	Ability to increase revenue to deliver operational requirements in line with community expectations Inadequate government funding programs and grants for local government
Cyber Security	Proactive management of cyber security Reliability and integrity of critical IT
Disaster / Catastrophic Events	Unpredictability, uncertainty and severity of extreme events Cost of natural disasters
Assets and Infrastructure	Financial capacity to manage and maintain assets and infrastructure Ageing property, assets and infrastructure
Reputation	Failure to meet increasing public demands and expectations Ability to administer council governance effectively

Risk Analysis

Effective risk analysis allows Council to understand the nature of the risk, including the cause or source, the likelihood of it happening and the consequence of it happening. Council's Risk Rating Matrix (as seen below) combines the likelihood and consequences to produce an estimate level of inherent risk (the amount of risk that exists in the absence of controls) which assists in determining appropriate controls to reduce or mitigate the risk.

Risk Rating Matrix	**Consequence Level**				
Likelihood Level	Very low	Minor	Medium	High	Extreme
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	High	Extreme
Possible	Low	Medium	High	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium	High

Likelihood Descriptors

The following table is used during the risk assessment process to provide guidance on assessing the likelihood of a risk occurring.

Likelihood Category	**Event Frequency**	**Historical**	**Project**
Almost Certain	More than once per year	Expected to occur, occurs regularly in the industry.	Likely to occur in more than 1 in 2 projects of this kind
Likely	Once per year	Will probably occur, has occurred many times in the industry.	Likely to occur in between 1 in 2 and 1 in 4 projects of this kind
Possible	Once every 10 years	Might occur, has occurred several times in the industry.	Likely to occur in between 1 in 4 and 1 in 10 projects of this kind
Unlikely	Once every 50 years	Not likely to occur, has occurred once or twice in the industry.	Likely to occur in less than 1 in 10 projects of this kind
Rare	Less than once every 50 years	May only occur in exceptional circumstances, unheard of in the industry.	Will not happen

Consequence Table

The following table is used during the risk assessment process to provide guidance on assessing the consequence level.

Category	**Consequence Level**				
	Very Low	**Minor**	**Medium**	**High**	**Extreme**
Financial	Negligible financial loss; <$10,000	Minor financial loss; $10,000 - $100,000	Significant financial loss; $100,000 - $500,000	Major financial loss; $500,000 - $1M	Extensive financial loss; >$1M
People	Minimal HR issues easily remedied. Employer of choice. High level of staff productivity despite risk.	Some HR issues within organisation, staff turnover considered appropriate. Employer of choice. Appropriate level of productivity remains despite identified risk.	Elements of poor HR culture, above average staff turnover and reduced long term productivity due to HR issues.	Poor internal culture within various departments hampering innovation and achievement, high staff turnover and ongoing loss of valued employees. Not perceived as an employer of choice resulting in attracting poor prospective employee candidates. High level reduced productivity due to HR issues.	Organisational wide poor internal culture hampering innovation and achievement, high staff turnover and ongoing loss of valued employees. Not perceived as an employer of choice resulting in attracting poor prospective employee candidates. Severe reduced long term productivity issues resulting from HR issues.
Legal and Compliance	Isolated non-compliance or breach, one off minor legal matters. Minimal failure of internal controls. Negligible financial impact.	Contained non-compliance or breach with short term significance. Low statutory penalty or minor financial impact.	Significant breach involving statutory authorities or investigation; significant failure in internal controls; prosecution possible with significant fine.	Major breach with fines and litigation; critical failure of internal controls.	Extensive breach involving multiple individuals. Extensive fines and litigation with potential class action.
Environmental	Negligible effect on environment. Examples include: • Very minor, no real effect, reversible. No impact or potential impact off site. • Environmental nuisance.	Short term effect on built or natural environment easily remedied. Examples include: • Minor short-term impact, almost no effect, potentially cumulative if not cleaned up, reversible. • Environmental nuisance.	Medium term effects on environment. Examples include: • Material environmental harm (significant effect and extent, causes $100,000 - $500,000 damage. • Immediate containment required, medium clean-up, some remediation required.	Significant medium to long term impact on natural or built environment. Examples include: • Material environmental harm (significant effect and extent, causes $500,000 - $1M damage). • Immediate containment required, large clean up, significant remediation required. • Serious impact to a protected species or habitat significantly	Significant environmental impact with long term effects. Examples include: • Serious environmental harm (irreversible, high impact, widespread, cases > $1M damage). • Immediate containment required, extensive clean-up, extensive or ongoing remediation needed.

	• Minor clean up required, no remediation required. • Insignificant impact to a protected specifies or habitat, no recovery efforts required.	• Containment required, minor clean-up, no remediation required. • Minor impacts on protected species or habitat, no recovery efforts required.	• Impact to a protected species or habitat, requiring short term recovery efforts (in the immediate area). (<5% loss of an ecosystem type, <5% loss of a species, locally).	contributing to localised extinction pressures in the Byron Shire area, requiring medium to long term recovery efforts (5-40% loss of an ecosystem type, 5-40% loss of a species, locally).	• Major impact to a protected species or habitat greatly contributing to or causing localised extinction risk in the Byron Shire area, requiring long term recovery efforts (>40% loss of an ecosystem type, >40% loss of a species, locally).
Business Systems and Technology	No loss/theft of corporate and/or personal data IT systems availability >99.9%	Short outage of core business systems resulting in minor disruption to administrative functions. Data breach resulting in exposure of confidential information.	Failure of several core business systems resulting in impacts to essential services. Cyber incident resulting in temporary unavailability of core business systems at multiple locations	Extended outage of core business systems resulting in major ongoing impacts to the delivery of council services. Significant loss/theft of corporate and/or personal data resulting in non-compliance with privacy legislation.	Catastrophic loss of IT systems due to cyber attack with no means for restoration from backups
Workplace and Public Safety	None or very minimal injuries; no treatment or first aid treatment only.	Minor injuries resulting in first aid or medical treatment. Some days lost.	Moderate injuries where medical treatment or hospitalisation is required. Numerous days lost.	Long term illness/ disability or multiple serious injuries. Loss of multiple key staff at once	Fatality/ multiple fatalities or permanent disability. Sustained and serious industrial action.
Service Delivery	Isolated, internal or minimal impact on service delivery. Disruption < 48 hours, usual scheduled interruptions.	Contained impact on service delivery of short term significance. Disruption between 2 and 20 days.	Moderate to significant impact on service delivery with potential investigation involved. Disruption between 20 and 60 days.	Major impact on service delivery with long term significance. Investigation required. Disruption between 60 and 90 days.	Extensive impact/disruption to service delivery; threat to viability of critical program or whole of organisation. Disruption > 90 days.
Asset	None or minimal impact on assets, which can be dealt with through routine maintenance.	Minor impact on assets managed with minimal efforts. Some restrictions in capability.	Some impact on assets managed with programmed response. Isolated loss of capability.	Major impact on assets requiring a programmed repair/replacement response. Limited capability.	Extensive impact on assets requiring a significant replacement or reconstruction effort. Total loss of capability.
Reputation	Isolated, internal or minimal attention or complaint.	Heightened concerns from a small group of residents; one off negative local media coverage.	Concerns from cross section of residents, with or without ongoing negative local media coverage.	Significant outcry from residents, significant negative state level media coverage.	Significant and widespread public outcry, sustained negative state or national media coverage.

Risk Evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation compares the results of the risk analysis with established risk criteria to determine whether a risk needs further treatment and the priority for that treatment.

Council uses the following risk matrix to provide guidance on the priority of treatment.

Escalation Table	**Assessed Risk Level**	**Required Action**
Unacceptable	Extreme	Immediate action required
	High	Prioritised action required
Acceptable	Medium	Planned action required
	Low	Action by routine procedure

Risk Treatment

The purpose of risk treatment is to select and implement options for addressing and mitigating risk. Approaches to risk treatment include:

- ceasing the activity that created the risk;
- formulating and selecting risk treatment options;
- planning and implementing risk treatment actions;
- assessing the effectiveness of the treatment;
- deciding whether the remaining (residual) risk is acceptable; and
- if not acceptable, taking further treatment to achieve the target risk rating.

The below table summarises Council’s key treatment options:

Mitigation Strategy	**Description**
Avoid	Not to proceed with the activity or choosing an alternative approach to achieve the same outcome. Aim is risk management, not aversion.
Mitigate	Reduce the likelihood by improving management controls and procedures or reduce the consequence by putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts.
Transfer	Shifting responsibility for a risk to another party by contract or insurance. Can be transferred as a whole or shared.
Accept	Controls are deemed appropriate in line with Council’s risk appetite. These must be monitored and contingency plans developed where appropriate.

Controls

A control is any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk. Following the identification of existing controls, it is necessary to evaluate them for effectiveness.

Council uses the following guidelines to assist in rating control effectiveness and deciding whether further treatment is required.

Good	A high degree of reliance can be placed on the system of internal control. Compensating controls are in place such that even if part of the system breaks down, the control criteria will probably still be met.
Satisfactory	The system of control can generally be relied upon however, some improvements to controls can be made to reduce the risk.
Marginal	There are several weaknesses in the system of control. There are some circumstances where control criteria may not be met.
Weak	The system of internal control cannot be relied upon to meet the control criteria. If there has not already been a significant breakdown, it is only a matter of time before this occurs.

Mitigating Actions

Where the effectiveness of a control is marginal or weak, or additional controls are required to aid in mitigating a specific risk, “mitigating actions” or tasks are developed and documented. Mitigating actions can be delegated to any staff member and will have a start and completion due date to ensure accountability is maintained.

Residual Risk Rating vs Target Risk Rating

Residual Risk Rating can be defined as the amount of risk that remains after controls are accounted for. Council’s risk assessment process also includes a Target Risk Rating, which is used to determine whether a risk falls within acceptable tolerance levels.

If the Target Risk Rating is lower than the Residual Risk Rating, further treatment is usually required. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk Registers

Byron Shire Council uses the Enterprise Risk Management (ERM) Module in Pulse, an online platform, to help identify, record and manage risk across the organisation. The ERM module captures Strategic and Operational risks, risk owners, existing controls and owners and staff assigned responsibility for implementing mitigating action plans when further treatment is required.

Project Risks and Technical Risks (IT) are also recorded and managed through the ERM module by respective managers.

Monitoring and Review

In addition to being an important continuous improvement activity, monitoring and review of the risk registers ensures that risk assessments and risk treatments are current for the objectives of Council. With the implementation of the ERM Module in Pulse in August 2022, Council saw an opportunity to commence a review of the existing registers, where through communication and collaboration Council ensures currency of information and the identification of emerging risks.

Council has also adopted the Three Lines of Defence Model to ensure appropriate oversight of organisational risk management.

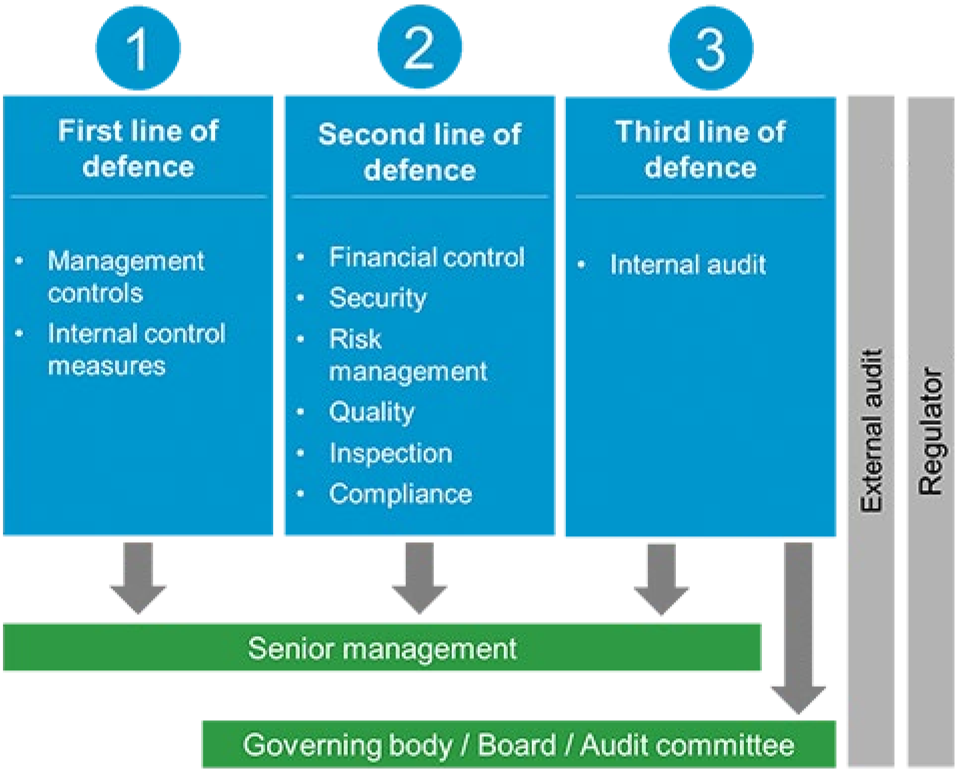

Figure 4: Adapted from Audit Committees: A guide to good practice, Third Edition. Australian Institute of Company Directors.

First line of defence:

- ❖ Primary responsibility for risk management rests with the business units undertaking day-to-day operations (own and manage risks);

Second line of defence:

- ❖ Risk management is delivered through financial controls, risk management processes, quality controls, security (such as delegations), inspection and compliance (oversee risks).

Third line of defence:

- ❖ Gives independent assurance that the first and second lines are working effectively. This is typically supplied by an internal audit function, overseen by the Audit Risk and Improvement Committee).

Key Risk Activities

Council commits to the following key risk activities outlined below:

Action	Description	Responsibility	Timeframe
Risk Management Policy	Review the currency and effectiveness of Council's Risk Management Policy	Strategic Risk Coordinator Council to adopt following review by the Audit, Risk and Improvement Committee	Every four years (or within 12 months of new Council being elected)
Risk Management Strategy	Review the currency and effectiveness of Council's Risk Management Strategy, including Council's risk appetite statement and consequence/likelihood tables	Strategic Risk Coordinator Executive Team to adopt following review by the Audit, Risk and Improvement Committee	Annually
Strategic Risk Register	Review risks and controls contained in Council's Strategic Risk Register and identify new or emerging risks to the organisation	Executive Team and Audit, Risk and Improvement Committee	Quarterly in February, May, August and November
Operational Risk Register	Review risks and controls contained in the Operational Risk Register	Managers	Quarterly in February, May, August and November
Develop Operational Risk Assessments and Treatment Plans	Identify key risks that may impact on Operational Plan activities as well as strategies and controls in place (or proposed) to manage those risks	Managers/Risk Owners (overseen by Strategic Risk Coordinator)	As identified
Quarterly Report	Provide the Executive Team and Audit, Risk and Improvement Committee an update on the risk	Strategic Risk Coordinator	Quarterly in February, May, August and November

	registers and risk activities planned or underway		
Communication/ Training	Ensure all staff are aware of the risk management framework and their obligations	Executive Team/ Managers/ Strategic Risk Coordinator	On-going

Training

To ensure the successful implementation of risk management throughout Council, appropriate training in risk management will be provided to management and employees through the induction process and at regular intervals.

Future Actions

The organisation's risk management goals for the period 2023-2025 are to:

- continue to consolidate an enterprise risk management framework in accordance with *AS/NZS ISO 31000, Risk Management – Principles and guidelines*;
- continue to review and update Strategic and Operational risks to ensure currency of information and identification of emerging risks;
- development of A Quick Guide to Risk Assessment;
- identify training opportunities across Council, on a priority basis, to facilitate improved understanding of risk management;
- consider reporting possibilities for project risks;
- investigate the implementation of an Enterprise Risk Management Committee.

Legislative and Strategic Context

The *Local Government Act (1993) NSW* section 8B(c)(iv) requires sound policies and procedures over risk management practices.

The management of risk across the business is linked to Council's objectives contained in its *Community Strategic Plan 2032*, particularly community objective 1: *'We have community led decision making which is open and inclusive'.*

Compliance with the Risk Management Strategy will be periodically monitored and assessed by the Audit, Risk and Improvement Committee.