RISK MANAGEMENT POLICY

AUTHORISATION

POLICY TYPE: *(Council or Operational)*	Council
POLICY LOCATION: *(eg. Corporate, Engineering, etc.)*	Governance and Risk
RESPONSIBLE OFFICER: *(by position title)*	Director Corporate and Community Services
AUTHORISED BY: *(GM or Director Title)*	Manex
DATE ADOPTED:	21 July 2021
ADOPTED BY: *(Manex or Council)*	Council
MINUTE NO: *(If required)*	
REVIEW DUE DATE: *(Four years unless statutorily required sooner)*	July 2023
REVISION NUMBER:	1

DOCUMENT HISTORY

VERSION NO.	**DATE**	**DESCRIPTION OF AMENDMENTS** *Include names of former policies that this policy will replace if applicable*	**AMENDED BY** *(Where required)*

REVIEW OF THIS POLICY

This Policy will be reviewed within two (2) years from the date of adoption or as required in the event of legislative changes. The Policy may also be changed as a result of other amendment that are to the advantage that Council and in the spirit of this Policy. Any amendment to the Policy must be by way of a Council Resolution for all policies categorised as “Council” policies or the approval of the General Manager for all policies categorised as “Operational” policies.

1. Purpose:

Key to the ERM framework is a policy statement that communicates Council's commitment to managing enterprise wide risks and establishes clear expectations regarding staff responsibilities for identifying and managing risk.

Risk management thinking, principles and practices will support the achievement of objectives, helping Council deliver quality services, improve decision-making, establish priorities, promote safety, minimise the impact of loss, and ensure regulatory compliance.

The ERM framework is supported by Council's policies and procedures that support Council's approach for the management of the total risk exposure. Refer to Council's Policy Framework for further details.

2. Scope:

This policy will apply to:

- both Council staff and Councillors
- permanent employees, whether full-time or part-time
- temporary or casual employees
- consultants
- individual contractors working for the Council.
- employees of contractors providing services to Bland Shire Council
- other people who perform Council official functions whose conduct and activities could be investigated by an investigating authority, including volunteers.

3. Outcomes:

Council is committed to effectively and systematically managing risks in order to maximise opportunities and limit adverse effects in accordance with AS/NZS ISO 31000 2018 Risk Management Guidelines.

To minimise the effect of negative risk and optimise opportunities, mangers and risk owners are expected to act in accordance with Council's policies, procedures, and guidelines and delegated authority.

Assessment of strategic operational and project risks must be completed in accordance with Bland Shire Council's policies and procedures.

Employees are expected to implement Council's Policies and Procedures which identify requirements for responding to assessed risks, including:

- Identification of risk treatments
- Analysis of residual risk
- Management involvement in decision making
- Nominating a risk owner

It is the responsibility of all Council staff to have knowledge of, and to ensure compliance with, the Policy and Procedures.

4. Roles and Responsibilities:

Role	Responsibilities
All Councillors	• Are responsible for the adoption and commitment to Enterprise Risk Management and its policies as well as oversight of Council's risk management framework through the normal course of good governance. • Act at all times in a manner consistent with Council values and Council policies, including the requirements of the ERM framework.

Role	Responsibilities
	• Take relevant steps to manage Council's risk exposure.
All staff	• Act at all times in a manner consistent with Council values and Council policies, including the requirements of the ERM framework • Take practical steps to manage Council's risk exposure with their area of activity and responsibility, including the identification of emerging risks and opportunities • Notify or escalate information about risks and opportunities to ensure an effective and timely response • Identify emerging risks requiring attention • As risk owners take responsibility for the effective management of specific risks as nominated in Council's risk data base
Senior Management Team (MANEX)	• Lead the development of ERM culture across Council • Set priorities for the implementation of ERM framework to maximise value to Council • Ensure the effective implementation and operation of Council's ERM framework • Define and communicate Council's risk appetite and tolerance • Assess and manage strategic risks, including the assessment of emerging risks within Council and the local Government sector to ensure that appropriate action is being taken by Council • Monitor the management of operational risks and direct risk responses as required • Nominate risk owners for all high-ranked-operational risk • Provide direction regarding responses to strategic, operational and project risks, as required • Identify strategic projects having potential to significantly impact on the achievement of Council's strategic objectives • Monitor risks associated with strategic projects • Provide direction to the Risk and Insurance Officer • Provide direction in response to reports and recommendations provided • Resolve urgent sensitive, complex or Council wide management issues that cannot be resolved by staff
General Managers Office	• Develop and document Council's corporate strategy (including plans, reports and other documents) in accordance with the IP&R framework that includes Council objectives, and provides a basis for strategic and operational risk assessment • Implement a risk-based assurance strategy (including Council's internal audit program) • Implement or delegate actions in response to advice provided by the Audit Committee
Directors	• Ensure the ERM framework is being effectively implemented and operated within their areas of responsibility • Participate in strategic, operational and project risk assessments • Manage operational risks within their directorate • Promote a culture that encourages the open and transparent discussions of risk • Escalate high-ranked risks to MANEX (as appropriate) • Approve Service Unit Business Plans, Business Cases and Project Plans – defining planned strategies for managing service and project risks • Plan and facilitate the progressive implementation of the ERM framework and the development of a risk-aware culture • Establish and monitor key performance indicators for the implementation and operation of the ERM framework • Ensure resources to support the implementation of the ERM framework • Support the formal review and update of the ERM framework

Role	Responsibilities
	• Promote the ERM framework across Council
Managers	• Ensure that the ERM framework is being effectively implemented and operated within their areas of responsibilities • Participate in operational and project risk assessments • Manage risks within the Business Unit • Develop strategies for the management of applicable operational risks and document these strategies in the Business Unit • Report operational risks monthly to the Director • Escalate risks to a Director for resolution (as appropriate)
Coordinators and Team Leaders	• Manage risks within functional areas • Contribute to the development of Service Unit Business Plans (where required) • Escalate risks to Managers and/or Directors to support the achievement of operational objectives (where required)
Project Managers	• Develop strategies for the management of project risks and document these strategies • Assess and manage project risks • Include project specific risk management requirements and methodology in the project plan • Ensure the effective management of risks within the project team to support the achievement of project objectives • Escalate risks to the Project Control Group, the project sponsor or MANEX (where required)
Risk & Insurance Officer	• Provide specialist risk management support and training to staff to ensure a consistent risk management approach across Council • Facilitate the progressive implementation of the ERM framework and the development of a risk-aware culture • Promote the communication of risks within and between Council's various Business Units and Directorates • Provide information to the Audit Committee regarding Council's risk exposure and the operation of the ERM framework • Coordinate day-to-day risk management activities across Council • Identify opportunities for improvement of the ERM framework • Report quarterly to MANEX regarding the performance of the ERM framework including recommendations to achieve performance targets • Identify training and development needs to achieve the required risk management competencies across Council • Coordinate resources to support the implementation of the ERM framework • Facilitate the formal review and update of the ERM framework • Promote the ERM framework across Council
Audit, Risk and Improvement Committee	• Provide independent assurance, advice and assistance to Council on risk management control, governance and external accountability responsibilities as defined in the Audit Committee Constitution

5. Definitions:

Term	Definition/Comment	Source
Council	Bland Shire Council	
Risk	Risk is defined as "the effect of uncertainly on objectives" where an effect is a deviation from the expected – either	ISO 31000-2018

Term	Definition/Comment	Source
	positive (an opportunity) or negative (a threat) ISO 3100 2018 The definition emphasises the need to establish objectives as the basis for risk assessment. Council's objectives may be expressed in term of: • Strategic and operational objectives and key performance indicators defined in Council's Integrated Planning and Reporting Framework. • Objectives defined within service unit Business Plans • Project specific objectives defined within business cases and project plans • Objectives implicit within Council's policies An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories, and can be applied at different levels.	
Risk Management	Risk management is defined as the "coordinated activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives". Risk management is a common sense, yet highly evolved discipline. The tools and training supporting this ERM Framework will support a change from an ad-hoc management approach to a structured approach that provides consistent, timely and valuable information about risk as a basis for effective decision-making.	ISO 31000-2018
Enterprise risk management	Enterprise risk management involves embedding risk thinking into Council's everyday activities. A risk management framework is formally defined as the "set of components that provide the foundations and organisational arrangements for designing, implementing monitoring, reviewing and continually improving risk management throughout the organisation. Enterprise risk management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall	Wikipedia
Potential exposure	The total plausible maximum impact on an organisation arising from a risk without regard to controls **Comment:** Sometimes the term "inherent risk" is used as an alternate to risk exposure.	HB 158 – 2010 Delivering assurance based on ISO 31000-2009 Risk management

Term	Definition/Comment	Source
		Principles and Guidelines
Risk appetite	The amount and type of risk an organisation is prepared to pursue or take. Council's risk appetite describes the amount and type of risk that Council is prepared to take in pursuit of it objectives. Risk appetite is about defining what Council does (and does not) want to do, and how it goes about it. It is an important foundation for the ERM framework. While mindful that reputation risk is inherent in our business activities, we will take a cautious approach and not be constrained by reputation related risk in pursuing innovation. Council has considerable appetite for improvements and innovation in service delivery, technology and the efficiency of our operations. Risk appetite is an articulation of an organisations willingness to take reign or accept risk and because it operates at strategic and operational levels. It is an integral part of any risk management capability in order to influence strategies and objectives it should be considered and reviewed during Strategic Planning. Additionally, risk appetite is a key influence in concert with cost/benefit of mitigation considerations, when determining the Target Risk Ratings of specific tasks. Understanding and applying effective considerations is highly beneficial in managing risk. Comment: Risk appetite is not about the pursuit of risk. It is about what the organisation does (or does not) want to do, and how it goes about it.	ISO Guide 73=2009 Risk Management vocabulary
Risk processes	*Risk assessment* is a process that is made up of three separate processes: risk identification, risk analysis, and risk evaluation. *Risk identification* is a process that is used to find, recognize, and describe the risks that could affect the achievement of objectives. *Risk analysis* is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and on sequences and to examine the controls that exist. *Risk evaluation* is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable	ISO 31000-2018
Risk category	A class or group of risk events based on their risk consequence **Risk categories** are used by Council to classify risk events as a basis for risk management including risk reporting and risk management decision making	
Risk owner	A *risk owner* is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.	ISO 31000-2018
Risk tolerance	A series of limits which, depending on the organisation may either be:	IRM Risk Appetite and Tolerance Guidance paper

Term	Definition/Comment	Source
	• In the nature of absolute limits, beyond which the organisation does not wish to proceed (i.e. The organisation cannot deal with risks beyond these limits): or • In the nature of alarms that alert the organisation to an impending breach of tolerance risks. Risk tolerance can be expressed in terms of absolutes, for example "we will not expose more than x% of our capital to losses in a certain line of business" or "we will not deal with certain types of customer".	
Risk Treatment	*Risk treatment* is a risk modification process. It involves selecting and implementing one or more treatment options. Once a treatment has been implemented, it becomes a control or it modifies existing controls. You have many treatment options. You can avoid the risk, you can reduce the risk, you can remove the source of the risk, you can modify the consequences, you can change the probabilities, you can share the risk with others, you can simply retain the risk, or you can even increase the risk in order to pursue an opportunity.	ISO 31000-2018
Residual Risk	Risk remaining after risk treatment.	ISO 27001

6. Legislation and Supporting Documents:

The Integrated Planning and Reporting Framework
Bland Shire Council has a tiered structure of external focused and internally focused strategies that align with the NSW Office of Local Government Integrated Planning and Reporting (IP&R) framework.

These documents identify strategic objectives and community outcomes, operational objectives, and key performance indicators that establish the primary basis for strategic and operational risk assessment across Council.

- Bland Shire Council Community Strategy Plan 2012-2027
- Combined Delivery Program & Operational Plan 2018 – 2022
- Resourcing Strategy 2018 – 2028
- Revenue Policy 2018 – 2019
- Office of Local Government Internal Audit Guidelines
- Audit, Risk & Improvement Committee Charter
- Business Continuity
- Internal Audit and Risk Management Policy for NSW Public Sector 2009
- ISO 31000:2018 Risk management - Guidelines
- Work Health and Safety Act 2011
- Risk Appetite Statement
- Risk Management Policy
- Risk Management Plan
- Work Health and Safety Policy
- Investment Policy
- Incident Reporting & Investigation Policy.

7. Relationship to Community Strategic Plan:

Under the theme of *Our Leadership - A well run Council acting as the voice of the community,* this policy fits within the Delivery Program Objective 12: Lead the Community, specifically Strategy 12.4 – Review and implement Council policies and comply with WHS and Risk Management requirements.

8. Attachments:

Risk Management Procedure

RISK MANAGEMENT PROCEDURE

AUTHORISATION

POLICY TYPE: *(Council or Operational)*	Council
POLICY LOCATION: *(eg. Corporate, Engineering, etc.)*	Governance and Risk
RESPONSIBLE OFFICER: *(by position title)*	Director Corporate and Community Services
AUTHORISED BY: *(GM or Director Title)*	Manex
DATE ADOPTED:	21 July 2021
ADOPTED BY: *(Manex or Council)*	Council
MINUTE NO: *(If required)*	
REVIEW DUE DATE: *(Four years unless statutorily required sooner)*	July 2023
REVISION NUMBER:	1

DOCUMENT HISTORY

VERSION NO.	**DATE**	**DESCRIPTION OF AMENDMENTS** *Include names of former policies that this policy will replace if applicable*	**AMENDED BY** *(Where required)*

REVIEW OF THIS PROCEDURE

This Procedure will be reviewed within two (2) years from the date of adoption or as required in the event of legislative changes. The Procedure may also be changed as a result of other amendment that are to the advantage that Council and in the spirit of this Procedure. Any amendment to the Procedure must be by way of a Council Resolution for all policies categorised as “Council” policies or the approval of the General Manager for all policies categorised as “Operational” policies.

1. Purpose:

Council has determined that, to effectively manage risk, it must foster a positive, risk aware culture across the organisation. Communication and consultation are crucial at every step of the risk management process to ensure all participants understand, are involved in and contribute to the process. Issues relating to the risk itself, its causes, its consequences and the measures being taken to treat it should be communicated to staff.

This ensures that all staff understands the basis on which decisions are made and the reasons why particular actions are required. Where appropriate, consulting stakeholders with different experiences, beliefs, assumptions, needs and concerns about the risk ensures through comprehensive consideration of the risk being taken.

Embedding risk management into the organisation culture is fundamental to achieving integrated risk management. This will be accomplished by:

- Directors and Managers championing risk management behaviours and actions
- Promoting the view that all staff are managers of risk
- Encourage staff to develop knowledge and skills in risk management
- Including risk management in Council's induction program, and ongoing training program
- Providing targeted training and support to staff so that risk management practices are effectively incorporated into their everyday roles and responsibilities.

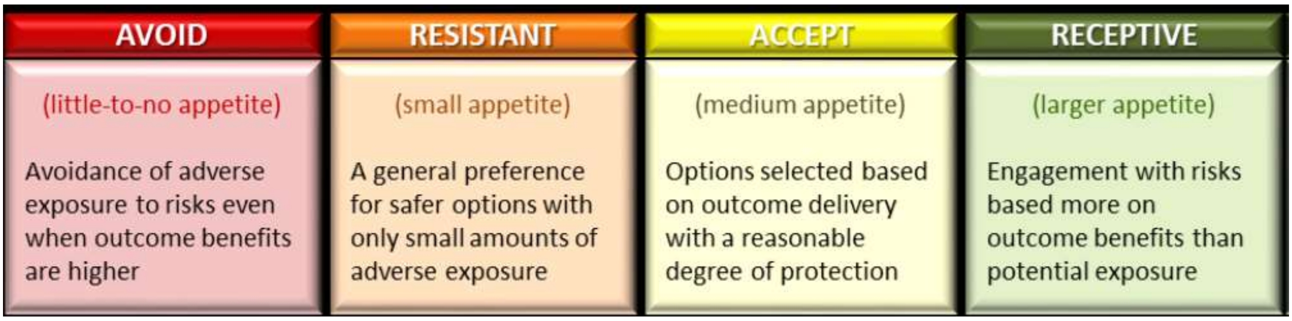
Council's risk appetite describes the amount and type of risk that Council is prepared to take in pursuit of it objectives. Risk appetite is about defining what Council does (and does not) want to do, and how it goes about it. It is an important foundation for the ERM framework. While mindful that reputation risk is inherent in our business activities, we will take a cautious approach and not be constrained by reputation related risk in pursuing innovation. Council has considerable appetite for improvements and innovation in service delivery, technology and the efficiency of our operations.

Risk appetite is an articulation of an organisations willingness to take reign or accept risk and because it operates at strategic and operational levels. It is an integral part of any risk management capability in order to influence strategies and objectives it should be considered and reviewed during Strategic Planning. Additionally, risk appetite is a key influence in concert with cost/benefit of mitigation considerations, when determining the Target Risk Ratings of specific tasks. Understanding and applying effective considerations is highly beneficial in managing risk.

2. Risk Appetite Summary:

The Risk Appetite Statements for Bland Shire Council are based on the amount of risk that the Council is willing to take or retain in pursuit of its objectives over the life of the current Operational Plan. The Council has a strategic focus on multiple areas, and many different and varied operations are carried out to support the Shire. As such, appetites for taking risk can vary across these different operations and strategic foci. Therefore, Council's Risk Appetite Statements have been developed against each of Council's risk categories. These Statements use a four-level ordinal scale to indicate the amount of risk Council is willing to take or retain for each category. Table 1 on the following page illustrates the four-level ordinal scale, with a definition for each.

Table 1: Risk Appetite Levels and Definitions



AVOID	RESISTANT	ACCEPT	RECEPTIVE
(little-to-no appetite)	(small appetite)	(medium appetite)	(larger appetite)
Avoidance of adverse exposure to risks even when outcome benefits are higher	A general preference for safer options with only small amounts of adverse exposure	Options selected based on outcome delivery with a reasonable degree of protection	Engagement with risks based more on outcome benefits than potential exposure

Risk tolerance
Risk tolerance provides more detail about Council's risk appetite. Risk tolerance defines the absolute limits (expressed as metrics for specific performance indicators) that Council will not exceed. Risk tolerance implies that Council cannot effectively deal with risks beyond those limits.

Risk categories
Council has established a number of risk categories. The risk categories reflect the types of risk consequences to which Council is exposed. The risks identified are:

- Community
- Compliance
- Natural Environment
- Finance
- Governance
- Human Resources
- Infrastructure
- Information Technology (IT)
- Legal/Regulatory
- Service Delivery
- Reputation
- Project Delivery
- Workplace Health and Safety.

Council define risk appetite and tolerance
MANEX has defined Council's risk appetite and tolerance at a strategic level for a number of risk categories Council has no appetite for risks, which may compromise the safety and wellbeing of staff. The community, contractors and volunteers. Council has no appetite for risks that cause significant and irreparable damage to the environment and seeks to preserve and enhance it for future generations.

Risk evaluation
Risk evaluation involves comparing the level of risk found during the analysis process against the risk criteria to determine whether the risk is acceptable. It involves making decisions based on the risk rating about which risk is acceptable. It involves making decisions based on the risk rating about which risks are going to be treated and the priorities of those treatments. Treatment strategies will vary depending on the level of risk. It is important to strike a balance between the cost of eliminating or reducing a risk and any potential benefits or loss reduction.

The higher the overall level of risk the greater level of management attention is required to reduce it probability and/or impact or manage the risk.

Table 2, provides a summary of Bland Shire Council's risk appetite position across its identified risk categories. Each category has one coloured cell, which represents the Primary Appetite position and one 'greyed' cell, which represents the Secondary Appetite position. These positions are defined as follows:

Primary Appetite: indicates a general appetite for taking or retaining risk for the given risk category.

Secondary Appetite: indicates an appetite-by-exception position for taking or retaining risk in specific circumstances. It is not necessary for all risk categories to have a Secondary Appetite position.

Table 2: Summary of Council's Risk Appetite position as of October 2020

Risk Category	Avoid	Resistant	Accept	Receptive
Community			PRIMARY	
Compliance	Secondary	PRIMARY		
Natural Environment		Secondary	PRIMARY	
Finance				
Governance	Secondary	PRIMARY		
Human Resources		Secondary	PRIMARY	
Infrastructure			PRIMARY	Secondary
Information Technology (IT)	Secondary	PRIMARY		
Legal/Regulatory	Secondary	PRIMARY		
Service Delivery		Secondary	PRIMARY	
Reputation		PRIMARY	Secondary	
Project Delivery			PRIMARY	Secondary
Workplace Health & Safety	PRIMARY			

Note: The Community risk category did not have designated secondary appetite. This indicates that in the current environment, Council does not perceive of circumstances that would encourage it to alter its appetite for taking risk with this risk category. To ensure the primary and secondary distributions are comparative, the secondary for Community is at the same level as its primary.

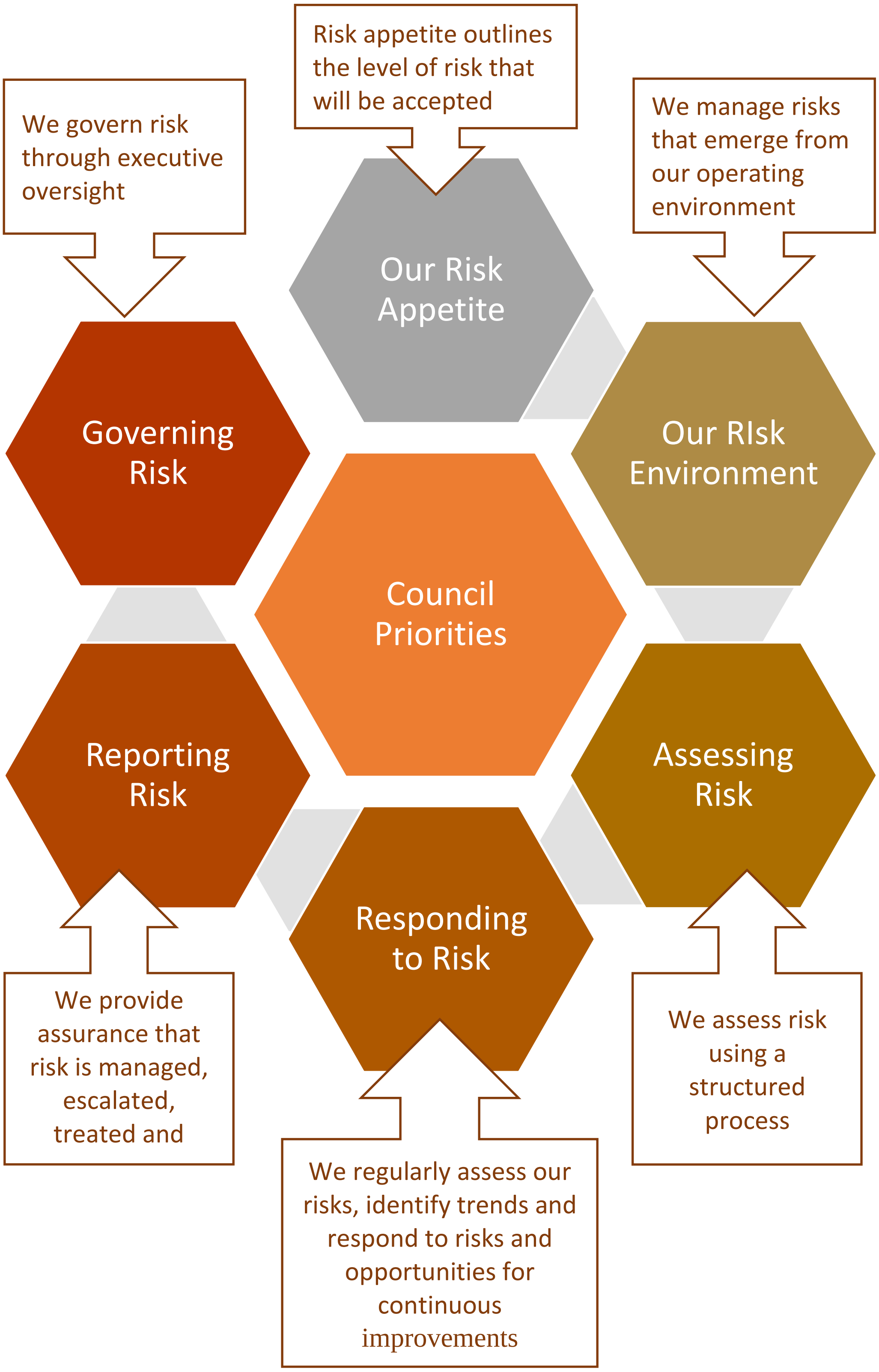
This report is from a comprehensive Risk Appetite Planning Session conducted by Craig Huntley Senior Consultant, Marsh Consulting Services Solutions Pacific and Damien Connell Regional Risk Manager Statewide Mutual.

3. Overview:

The process map following defines Council's process, responsibilities for the management of strategic, operational, and project risks.

Elements of the Enterprise Risk Management (ERM) Framework

The ERM identifies the key elements of Council's approach of managing risks.


Risk appetite outlines the level of risk that will be accepted
We govern risk through executive oversight
We manage risks that emerge from our operating environment
Our Risk Appetite
Governing Risk
Our RIsk Environment
Council Priorities
Reporting Risk
Assessing Risk
Responding to Risk
We provide assurance that risk is managed, escalated, treated and
We assess risk using a structured process
We regularly assess our risks, identify trends and respond to risks and opportunities for continuous improvements

Work health and safety risks
Council is committed to a robust Work Health and Safety (WHS) risk management system to support Council's commitment to zero harm for all its workers. The Work Health and Safety Act 2011 (NSW) came into effect on 1 January 2012 and provides for a balanced and nationally consistent framework to ensure the health and safety of workers and workplaces.

Council has developed its WHS system to manage WHS risks and includes separate policy, procedures and reporting mechanisms to those outlined in this document.

The WHS system, with supporting documentation is available on Council's internet.

http://www.blandshire.nsw.gov.au/sites/default/files/Work%20Health%20Safety%20Policy.pdf

Business continuity risks
An element of Council's risk management strategy is the maintenance of an effective Recovery and Business Continuity Plan Council's plan has been developed to:

- identify critical aspects of Council services exposed to risk from business interruption
- define preparatory actions which will minimise loss or damage should an interruption occur
- adopt strategies to maintain critical Council services through periods of disruption
- minimise adverse effects on the public, employees and Council.

Council intends to review the plan on a regular basis.

Council insurance program
Integral to Council's management of risk is the impact and value of Council's insurance program. Council has a comprehensive suite of insurances in place to mitigate direct pecuniary loss. The program's purpose is to reduce Council's business exposure against risk, which cannot otherwise be effectively mitigated and are normally accidental in nature or an unexpected calamity or incident.

Council has an obligation under section 382 of the Local Government Act 1993 (NSW) to hold adequate public liability and professional indemnity coverage. Council's insurance program is reviewed annually.

4. Risk-based decision making:

The following sections identify requirements for risk management that will support key Council decision-making activities.

Strategic planning
A review of high-ranked strategic, operational and project risks will be used to inform decisions regarding Council's Strategic planning activities.
Business cases
Organisational change is a major source of risk within Council. Business cases are used to define proposed changes to business operations and include:

- change in strategic direction or focus
- organisational change/restructure
- introduction of new technologies or work practices
- initiatives to improve service delivery
- Workforce changes (e.g. Roles. Employment type, skill requirements)

Business cases must be prepared and submitted for review and approval to MANEX.

All business cases must include a risk assessment based on the defined objectives of the business case and associated tangible benefits to be delivered by the business case.

Project risk management

Strategic projects

MANEX will identify strategic projects having potential to significantly impact on the achievement of Council's strategic objectives.

Project plan

A project plan will be prepared for every project or program. Project plans will include an assessment of project risks having the potential to effect the achievement of project objectives, and will include action plans to manage high-ranked risks.

Risk reporting

Consistent, comprehensive and timely risk reporting is critical to provide management with the opportunity to monitor risks, and to inform decision-making. The following table summarises the key ERM framework actions, reports required for strategic operational and project risks.

Action	Description	Responsibility	Timing
Review of strategic risks	Regular reviews of strategic risks to maintain the currency of the risk register and to monitor the status of risk treatments	MANEX	As determined by MANEX
Operation risk assessment	Comprehensive risk assessment based on Council's current operational and Business Unit objectives	MANEX	Annual
Operation risk reviews	Review of the status of selected actions in response to the operational risk assessment	MANEX	Monthly
Review of strategic projects	Review of risks and the status of risk treatments for strategic projects	MANEX	Monthly
Review Council's Internal audit program	Review outcomes of strategic operational and project risk assessments as an input to Council's internal audit program	General Managers office and MANEX	Annual
Review of risks and actions nominated within Business Units Business Plans	Review of the status of actions (including risk responses) identified in each Business Unit and Business Plan Reporting of the status of actions (including the responses) identified in each Business Unit and Business Plan	Managers and Directors Managers and Directors	Monthly Quarterly

Reports to Council

Reports to Council are prepared using a standard template and must include a risk assessment and the identification of any required risk mitigation measures – providing a basis for the risk informed decision-making.

Risk assessments use the approved Bland Shire Council risk matrix and follow the Council's risk management policies and procedures.

MANEX will review reports to Council and determine whether risk treatments identified in reports to Council should be subject to further analysis and/or included in Council's risk database.

5. Risk Information Systems:

Risk Records
Risk management activities will be recorded to provide:

- a record of risk assessment and risk ownership for ongoing monitoring
- a record of completed risk treatments
- an audit trail demonstrating the basis for decision making
- evidence of good corporate governance
- records that can be used as a point of reference for future risk management activities.

Records will be maintained for all activities and follow Bland Shire Council's records management procedures.

Risk Register
Records of risk assessment will be maintained in Council's Risk Register. The Register will be developed to also include records of:

- objects used as a basis for risk assessment
- risk assessments (including, analysis and evaluation)
- nominated risk owners
- risk treatments (including existing controls, actions, target timeframe and responsibilities)
- projected residual risk (post treatment)
- the status of risk monitoring and risk treatments.

The Risk Register will be used:
- To record all risks across Council – strategic, operation and project – with the ability to select, filter and sort.
- To monitor and manage the status of risk treatments
- A resource to be used for risk assessments, assurance activities and for continuous improvement across Council.

The Risk & Insurance Officer will review and update Council's Risk Register on a regular basis.

Risk owners are to monitor the accuracy and status of the risks that have been allocated to them and report on them in accordance with the requirements of the risk assessment.

The risk register will be formally reviewed on a nominated basis. One of the reviews should coincide with the annual integrated planning and budgeting process. This helps determine work priorities and ensures appropriate resources are assigned to manage and control risks.

Council's risk management framework, policies and procedures will be reviewed on a regular basis. The review will cover:

- The adequacy of risk management policies and procedures
- Compliance with risk management policies and procedures
- The effectiveness of policies, procedures and controls in mitigating risk.

6. Assurance and improvement process:

Council's control framework

Council’s risk database will identify risk controls in response to identified risks and will evolve to provide a consolidated reference for governance, risk and compliance controls across Council, representing Council’s control framework.

Monitoring the ERM Framework

MANEX will be responsible for regularly monitoring the performance of the ERM framework. The MANEX will report to Council and the Audit Committee on the performance of the ERM framework.

Council's Internal Audit function will be responsible for conducting independent reviews of the performance of the ERM framework as instructed by the MANEX and the Audit Committee on the performance of the ERM framework.

Council's internal audit program

Strategic, operational and project risk based assurance strategy (including an internal audit program) consistent with;

- Internal Audit Guidelines (2010), Division of Local Government, NSW Department of Premier and Cabinet
- HB 158:2010 Delivering assurance based on ISO 31000 2009 Risk Management principles and guidelines.

Internal audit and self-assessment findings will be reviewed by MANEX and where appropriate, risk treatments for identified high ranked risks will be identified in the risk database and/or designated as actions.

The Audit Risk and Improvement Committee

The Audit Risk and Improvement Committee will provide information regarding Council's risk exposure and the operation of the ERM framework for review. The Audit Committee will provide an annual report to the General Manager, providing independent assurance, advice and assistance to Council on risk management, control, governance, and external accountabilities.

Continual improvement

MANEX will be responsible for continual improvement in risk management through the setting of organisational performance goals, measurement, review and the subsequent modification of process, systems, resources, capabilities and skills.

Improvement will be achieved:

- By establishing explicit performance goals and key performance indicators as a base for reviewing and improving performance of the ERM framework.
- In response to internal and external audit findings and recommendations, and in response to advice from the Audit Risk and Improvement Committee
- In response to opportunities for improvement identified as a result of risk maturity assessments
- Through an ongoing process of identification examples of success and failure as a basis to analysis and knowledge sharing

Attachment A: Definitions

Term	Definition/Comment	Source
Council	Bland Shire Council	
Risk	Risk is defined as "the effect of uncertainly on objectives" where an effect is a deviation from the expected – either positive (an opportunity) or negative (a threat) ISO 3100 2018 The definition emphasises the need to establish objectives as the basis for risk assessment. Council's objectives may be expressed in term of: • Strategic and operational objectives and key performance indicators defined in Council's Integrated Planning and Reporting Framework. • Objectives defined within service unit Business Plans • Project specific objectives defined within business cases and project plans • Objectives implicit within Council's policies An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories, and can be applied at different levels.	ISO 31000-2018
Risk Management	Risk management is defined as the "coordinated activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives". Risk management is a common sense, yet highly evolved discipline. The tools and training supporting this ERM Framework will support a change from an ad-hoc management approach to a structured approach that provides consistent, timely and valuable information about risk as a basis for effective decision-making.	ISO 31000-2018
Enterprise risk management	Enterprise risk management involves embedding risk thinking into Council's everyday activities. A risk management framework is formally defined as the "set of components that provide the foundations and organisational arrangements for designing, implementing monitoring, reviewing and continually improving risk management throughout the organisation. Enterprise risk management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular	Wikipedia

	events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall	
Potential exposure	The total plausible maximum impact on an organisation arising from a risk without regard to controls **Comment:** Sometimes the term "inherent risk" is used as an alternate to risk exposure.	HB 158 – 2010 Delivering assurance based on ISO 31000-2009 Risk management Principles and Guidelines
Risk appetite	The amount and type of risk an organisation is prepared to pursue or take. Council's risk appetite describes the amount and type of risk that Council is prepared to take in pursuit of it objectives. Risk appetite is about defining what Council does (and does not) want to do, and how it goes about it. It is an important foundation for the ERM framework. While mindful that reputation risk is inherent in our business activities, we will take a cautious approach and not be constrained by reputation related risk in pursuing innovation. Council has considerable appetite for improvements and innovation in service delivery, technology and the efficiency of our operations. Risk appetite is an articulation of an organisations willingness to take reign or accept risk and because it operates at strategic and operational levels. It is an integral part of any risk management capability in order to influence strategies and objectives it should be considered and reviewed during Strategic Planning. Additionally, risk appetite is a key influence in concert with cost/benefit of mitigation considerations, when determining the Target Risk Ratings of specific tasks. Understanding and applying effective considerations is highly beneficial in managing risk. Comment: Risk appetite is not about the pursuit of risk. It is about what the organisation does (or does not) want to do, and how it goes about it.	ISO Guide 73=2009 Risk Management vocabulary
Risk processes	*Risk assessment* is a process that is made up of three separate processes: risk identification, risk analysis, and risk evaluation.	ISO 31000-2018

	Risk identification is a process that is used to find, recognize, and describe the risks that could affect the achievement of objectives. *Risk analysis* is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and on sequences and to examine the controls that exist. *Risk evaluation* is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable	
Risk category	A class or group of risk events based on their risk consequence **Risk categories** are used by Council to classify risk events as a basis for risk management including risk reporting and risk management decision making	
Risk owner	A *risk owner* is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.	ISO 31000-2018
Risk tolerance	A series of limits which, depending on the organisation may either be: • In the nature of absolute limits, beyond which the organisation does not wish to proceed (i.e. The organisation cannot deal with risks beyond these limits): or • In the nature of alarms that alert the organisation to an impending breach of tolerance risks. Risk tolerance can be expressed in terms of absolutes, for example “we will not expose more than x% of our capital to losses in a certain line of business” or “we will not deal with certain types of customer”.	IRM Risk Appetite and Tolerance Guidance paper
Risk Treatment	***Risk treatment* is a risk modification process.** It involves selecting and implementing one or more treatment options. Once a treatment has been implemented, it becomes a control or it modifies existing controls. You have many treatment options. You can avoid the risk, you can reduce the risk, you can remove the source of the risk, you can modify the consequences, you can change the probabilities, you can share the risk with others, you can simply retain the risk, or you can even increase the risk in order to pursue an opportunity.	ISO 31000-2018
Residual Risk	Risk remaining after risk treatment.	ISO 27001

Attachment B: Reference publications

The following publications have been referenced in the production of this Guideline and should be referenced for future information.

Title and Publisher	Description
ISO 31000 – 2018 Risk Management Guidelines	ISO 31000:2018 provides guidelines on managing risk faced by organizations. The application of these guidelines can be customised to any organization and its context. ISO 31000:2018 provides a common approach to managing any type of risk and is not industry or sector specific. ISO 31000:2018 can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.
ISO 31000 – 2009 Risk Management and Principles	ISO 31000:2009 provides principles and generic guidelines on risk management. ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector. ISO 31000:2009 can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.
ISO 31000-2018 Plain English definitions	The guide ISO 31000 risk management definitions translate definitions into plain English in order to make them easier to understand.
Internal Audit Guidelines (2010) Division of Local Government. NSW Department of Premier and Cabinet	These Guidelines are Director General's Guidelines for the purposes of section 23A of the Local Government Act 1993, issued by the Chief Executive, Local Government under delegated authority. The Guidelines are designed to provide council's with assistance to implement internal audit and risk management. The Guidelines also include appropriate structures, functions, charter and membership of audit and risk management committees.
HB 158 2010 Delivering assurance based on ISO 3100 – 2009 Risk Management Principles and Guidelines	HB 158 2010 draws on the institute of Internal Auditors International Professional Practices Framework with respect to using and assuring the ISO 31000 2009 risk management process. In particular, it describes how to use the risk management process to 1. Develop a risk-based assurance strategy and program 2. Plan an assurance engagement 3. Report the assurance program 4. Design controls The Handbook also provides a guide to assessing the adequacy of risk management framework and process.
HB 203-2012 Managing environment related risk	Handbook HB 203 3012 discusses how AS/NZS ISO 2009 can be used to help an organisation manage environmental-related risks, including risks to the environment and from the environment

Please note: ISO 32000-2009 Risk Management Principles and Guidelines has been revised to ISO 32000-2018 Risk Management Guidelines

Attachment C: Response to risk management principles

The following table summarises those principles and identifies the approach adopted by Council's ERM Framework in response to each:

AS/NZS ISO 31000 Principles	Bland Shire Council Approach
Risk management creates and protects value Risk management contributes to the demonstrable achievement of objectives and improvement of performance	The ERM Framework identifies and focuses on Council's strategic, operational and project objectives and supports their achievements Risk management processes clearly establish objectives as a basis for risk assessment
Risk management is an integral part of all organisational process Risk management is part of the responsibilities of management and an integral part of Council process, including strategic planning and all project and change management processes	The ERM Framework identifies a range of Council functions where risk management will be applied, and includes strategic, operational and Project risks. The ERM framework will be integrated into Council's induction process and training strategy. A common approach, methodology will be applied across Council with records maintained in a common database.
Risk management is part of decision making Risk Management helps decision makers make informed choices, priorities actions and distinguish among alternate courses of action	The ERM Framework identifies Council processes where risk management will inform more effective decision-making. These activities include strategic planning, development of business cases. Council demonstrates, and a range of strategic , operational and project reporting functions' Risk appetite and tolerance have been defined to inform decision making and business rules have been developed that define common expectations for risk response
Risk management explicitly address uncertainly Risk management explicitly takes account of uncertainly, the nature of that uncertainly and how it can be addressed	Council's Policy recognises and accepts uncertainties applicable in Council's current operating environment.
Risk management is systematic, structured and timely. A systematic, timely and structured approach contributes to efficiency and the consistent, comparable and reliable results	The ERM Framework supported by Bland Shire Council's policies and procedures contributes to a structured approach that includes minimum timeframes or frequencies for risk assessments, risk response, risk reporting, and for reviewing and updating the ERM Framework.
Risk management is based on the best available information Inputs are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement.	The risk management processes embedded within the ERM Framework encourage the use of cross-functional teams. Improvement process will include an assessment of the adequacy of information and the effectiveness of risk management process.
Risk management is tailored.	The ERM Framework has been customised to reflect Council's internal and external environment. This is reflected in Council's risk appetite and tolerance statements. Council's risk profile and in

AS/NZS ISO 31000 Principles	Bland Shire Council Approach
Risk management is aligned Council's external and internal context and risk profile.	recognition of the integration of risk management within Council's existing processes.
Risk management takes human and cultural factors into account Risk management recognises the capabilities, expectations and intentions of external and internal stakeholders that can facilitate or hinder achievement of Council's objectives	The ERM Framework recognises Council's current resourcing levels and governance structures – particularly the role and responsibilities of the MANEX. The ERM Framework is aligned with Bland Shire Council's Community Strategic Plan 2017-2022 ensuring consultation and meaningful planning around human and cultural factors and assisting with risk mitigation.
Risk management is transparent and inclusive Appropriate and timely involvement of stakeholders at all levels ensures that the risk management remains relevant and up to date.	ERM management processes recognise the contributions of multiple levels of management. Risk registers will remain accessible to management with defined responsibility for keeping the information up to date.
Risk management is dynamic, iterative and responsive to change Risk management continually identifies and responds to change.	Risk assessment requirements are integrated into business case and project management process.
Risk management facilitates continual improvement of the organisation Council should develop and implement strategies to improve risk management maturity alongside all other aspects of their organisation	Assurance and improvement processes are explicitly defined in the ERM Framework and include a mechanism for regular review of Council's risk maturity.

7. Scope:

This procedure will apply to:

- both Council staff and Councillors
- permanent employees, whether full-time or part-time
- temporary or casual employees
- consultants
- individual contractors working for the Council.
- employees of contractors providing services to Bland Shire Council
- other people who perform Council official functions whose conduct and activities could be investigated by an investigating authority, including volunteers.

8. Roles and Responsibilities:

Role	Responsibilities
All Councillors	• Are responsible for the adoption and commitment to Enterprise Risk Management and its policies as well as oversight of Council's risk management framework through the normal course of good governance. • Act at all times in a manner consistent with Council values and Council policies, including the requirements of the ERM framework. • Take relevant steps to manage Council's risk exposure.
All staff	• Act at all times in a manner consistent with Council values and Council policies, including the requirements of the ERM framework • Take practical steps to manage Council's risk exposure with their area of activity and responsibility, including the identification of emerging risks and opportunities • Notify or escalate information about risks and opportunities to ensure an effective and timely response • Identify emerging risks requiring attention • As risk owners take responsibility for the effective management of specific risks as nominated in Council's risk data base
Senior Management Team (MANEX)	• Lead the development of ERM culture across Council • Set priorities for the implementation of ERM framework to maximise value to Council • Ensure the effective implementation and operation of Council's ERM framework • Define and communicate Council's risk appetite and tolerance • Assess and manage strategic risks, including the assessment of emerging risks within Council and the local Government sector to ensure that appropriate action is being taken by Council • Monitor the management of operational risks and direct risk responses as required • Nominate risk owners for all high-ranked-operational risk • Provide direction regarding responses to strategic, operational and project risks, as required • Identify strategic projects having potential to significantly impact on the achievement of Council's strategic objectives • Monitor risks associated with strategic projects • Provide direction to the Risk and Insurance Officer • Provide direction in response to reports and recommendations provided • Resolve urgent sensitive, complex or Council wide management issues that cannot be resolved by staff

General Managers Office	• Develop and document Council’s corporate strategy (including plans, reports and other documents) in accordance with the IP&R framework that includes Council objectives, and provides a basis for strategic and operational risk assessment • Implement a risk-based assurance strategy (including Council’s internal audit program) • Implement or delegate actions in response to advice provided by the Audit Committee
Directors	• Ensure the ERM framework is being effectively implemented and operated within their areas of responsibility • Participate in strategic, operational and project risk assessments • Manage operational risks within their directorate • Promote a culture that encourages the open and transparent discussions of risk • Escalate high-ranked risks to MANEX (as appropriate) • Approve Service Unit Business Plans, Business Cases and Project Plans – defining planned strategies for managing service and project risks • Plan and facilitate the progressive implementation of the ERM framework and the development of a risk-aware culture • Establish and monitor key performance indicators for the implementation and operation of the ERM framework • Ensure resources to support the implementation of the ERM framework • Support the formal review and update of the ERM framework • Promote the ERM framework across Council
Managers	• Ensure that the ERM framework is being effectively implemented and operated within their areas of responsibilities • Participate in operational and project risk assessments • Manage risks within the Business Unit • Develop strategies for the management of applicable operational risks and document these strategies in the Business Unit • Report operational risks monthly to the Director • Escalate risks to a Director for resolution (as appropriate)
Coordinators and Team Leaders	• Manage risks within functional areas • Contribute to the development of Service Unit Business Plans (where required) • Escalate risks to Managers and/or Directors to support the achievement of operational objectives (where required)
Project Managers	• Develop strategies for the management of project risks and document these strategies • Assess and manage project risks • Include project specific risk management requirements and methodology in the project plan • Ensure the effective management of risks within the project team to support the achievement of project objectives • Escalate risks to the Project Control Group, the project sponsor or MANEX (where required)
Risk & Insurance Officer	• Provide specialist risk management support and training to staff to ensure a consistent risk management approach across Council • Facilitate the progressive implementation of the ERM framework and the development of a risk-aware culture

	• Promote the communication of risks within and between Council's various Business Units and Directorates • Provide information to the Audit Committee regarding Council's risk exposure and the operation of the ERM framework • Coordinate day-to-day risk management activities across Council • Identify opportunities for improvement of the ERM framework • Report quarterly to MANEX regarding the performance of the ERM framework including recommendations to achieve performance targets • Identify training and development needs to achieve the required risk management competencies across Council • Coordinate resources to support the implementation of the ERM framework • Facilitate the formal review and update of the ERM framework • Promote the ERM framework across Council
Audit, Risk and Improvement Committee	• Provide independent assurance, advice and assistance to Council on risk management control, governance and external accountability responsibilities as defined in the Audit Committee Constitution

9. Legislation and Supporting Documents:

The Integrated Planning and Reporting Framework

Bland Shire Council has a tiered structure of external focused and internally focused strategies that align with the NSW Office of Local Government Integrated Planning and Reporting (IP&R) framework.

These documents identify strategic objectives and community outcomes, operational objectives, and key performance indicators that establish the primary basis for strategic and operational risk assessment across Council.

- Bland Shire Council Community Strategy Plan 2012-2027
- Combined Delivery Program & Operational Plan 2018 – 2022
- Resourcing Strategy 2018 – 2028
- Revenue Policy 2018 – 2019
- Office of Local Government Internal Audit Guidelines
- Audit, Risk & Improvement Committee Charter
- Business Continuity
- Internal Audit and Risk Management Policy for NSW Public Sector 2009
- ISO 31000:2018 Risk management - Guidelines
- Work Health and Safety Act 2011
- Risk Appetite Statement
- Risk Management Policy
- Risk Management Plan
- Work Health and Safety Policy
- Investment Policy
- Incident Reporting & Investigation Policy.

10. Relationship to Community Strategic Plan:

Under the theme of *Our Leadership - A well run Council acting as the voice of the community*, this procedure fits within the Delivery Program Objective 12: Lead the Community, specifically Strategy 12.4 – Review and implement Council policies and comply with WHS and Risk Management requirements.