5.2. ENTERPRISE RISK MANAGEMENT GENERAL POLICY AND GUIDELINES REVIEW

REPORT AUTHOR(S) Joanne Jacobson, Executive Manager People and Governance

DEPARTMENT People and Governance

RECOMMENDATION

That Council:

1) Adopt the updated Enterprise Risk Management Policy, and

2) Endorse the updated Enterprise Risk Management Framework and Guidelines.

EXECUTIVE SUMMARY

Managing risk is an essential component of an organisation's operations to ensure that the corporate goals and objectives can be achieved. The review and update of Council's Risk Management Policy and accompanying Guidelines confirms Council's commitment to the ongoing maintenance of a robust risk management culture within the organisation.

BACKGROUND

The Australian Standard AS ISO 31000:2018 'Risk Management Guidelines' is the tool of choice for risk managers in establishing a risk management framework. An integral part of the risk management framework is to establish the organisation's Risk Management Policy and accompanying Framework and Guidelines.

COMMENT

Council's Enterprise Risk Management General Policy has been updated to reference the new Australian Standard - Risk Management Guidelines (AS ISO 31000:2018). In addition, changes have been made to the Roles and Responsibilities listed in the policy to reflect the new Organisational Structure introduced late 2018.

The Enterprise Risk Management Framework and Guidelines has also been updated to reflect the new Standard. In addition a Risk Appetite Statement has been added at Appendix A as required by the Queensland Audit Office in their interim Management letter dated May 2019.

FINANCIAL/RESOURCE IMPLICATIONS

Nil

RISK MANAGEMENT IMPLICATIONS

The Policy and Guidelines reinforces Council's commitment to manage risk to ensure the organisation's goals and objectives can be achieved.

CORPORATE/OPERATIONAL PLAN, POLICY REFERENCE

This report has been prepared in accordance with the following:

Corporate Plan 2014-2019 Initiatives:

Theme 5 – Governance

5.1.2 - Implement a robust enterprise risk management culture to identify and manage potential risks.

5.2.2 - Implement adopted policies and guidelines to ensure consistency in administrative management which also encourages innovation in Council operations.

COUNCIL'S ROLE

Council can play a number of different roles in certain circumstances and it is important to be clear about which role is appropriate for a specific purpose or circumstance. The implementation of actions will be a collective effort and Council's involvement will vary from information only through to full responsibility for delivery.

The following areas outline where Council has a clear responsibility to act:

Regulator	Meeting the responsibilities associated with regulating activities through legislation or local law.

CONSULTATION

Internal: Management
External: Nil

ATTACHMENTS

1. Enterprise Risk Management Policy #424907 **[5.2.1 - 3 pages]**
2. ERM Framework Guideline Document #428359 **[5.2.2 - 20 pages]**

DOUGLAS SHIRE COUNCIL

ENTERPRISE RISK MANAGEMENT GENERAL POLICY

Intent

This policy outlines Council's commitment to the development and maintenance of an enterprise risk management framework.

Scope

This policy applies to all elected representatives and staff who are involved in the identification and management of risks associated with Council achieving its goals, objectives and operational activities.

Reference

Legislation: *Local Government Regulation 2012*

Other: Australian AS ISO 31000:2018 Risk Management – Guidelines

Provisions

Douglas Shire Council recognises that as a public authority it is exposed to a broad range of risks which, if not managed, could adversely impact on the organisation achieving its strategic objectives. Therefore Council will implement a systematic risk management methodology to identify and address, where practical, areas of potential risk within Council. Any methodologies adopted will be consistent with *Australian Standard AS ISO 31000:2018 Risk Management – Guidelines*.

The intent of this policy is to create an environment where Council, management and staff assume responsibility for risk management, through consistent risk management practices.

Objectives

The objectives of this policy are:

- Align Council activities to and support business objectives identified in Council's Corporate and Operational Plans;
- Maintain and improve reliability and quality of service provided by Council, within Council's controls and capabilities;
- Minimise or eliminate adverse impacts from Council's services or infrastructure on the community, visitors and the environment;
- Capitalise on opportunities identified for Douglas Shire Council;
- Safeguard Council's employees, contractors, committees, volunteers, assets, financial sustainability, property, reputation and information;
- Promote risk management principles as a strategic tool to ensure better informed decision making throughout Council; and
- Embed a culture of risk management across the Council.

Principles

The following principles will be adopted to ensure that the objectives are achieved:

- Apply a risk management framework which is consistent with the current *Australian Standard AS ISO 31000:2018 Risk Management – Guidelines* for making decisions on how best to identify, assess and manage risk throughout all departments of Council;
- Prioritise identified risks and implement treatments progressively based on the level of risk assessed and the effectiveness of the current treatments;
- Integrate risk management with existing planning and operational processes, including the Corporate Plan;

- Take into account relevant legislative requirements and political, social and economic environments in managing risks;
- Create a culture of risk awareness throughout the organisation through training, induction, promotion and risk review and reporting mechanisms; and
- Ensure resources and operational capabilities are identified and responsibility for managing risk is allocated.

Definitions

Risk **-** A risk to the business is any action or event that has an effect of uncertainty on objectives of Douglas Shire Council. It is measured in terms of consequence and likelihood.

Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

Risk Management - Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council.

Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

Enterprise Risk Management (ERM) **-** Enterprise risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity) and includes the coordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

Risk Register - The risk register lists identified and assessed risks.

Roles and Responsibilities

Council	Council is responsible for adoption of this policy and retains the ultimate responsibility for risk management and for determining the appropriate level of risk that it is willing to accept in the conduct of Council business activities. Council will review the effectiveness of the risk management systems.
Chief Executive Officer	Council's Chief Executive Officer is responsible for identifying, evaluating and managing risk in accordance with this policy through a formal enterprise-wide risk management framework. Formal risk assessments must be performed at least once a year as part of the business planning and budgeting process. The Chief Executive Officer will report to Council annually on the progress made in implementing a sound system of risk management and internal compliance and control across Council's operations.
Management Team	Council's Management Team will perform the function of the Risk Management Committee which has oversight of developing the risk management framework and monitoring risk treatment. The team will ensure the risk management framework identifies high-level strategic risks and aligns with the Internal Audit Plan. The Management Team will ensure that the results of its reviews are provided to Council for update of the Council's risk profile as appropriate. The Management Team will also ensure periodic reviews of the risk management

	framework are carried out by Internal Audit pursuant to the Internal Audit Plan.
Coordinators / Team Leaders	Council's Coordinators and Team Leaders are responsible for the accuracy and validity of risk information reported to the Council. In addition, this will ensure clear communication throughout the organisation of Council's position on risk.
Employees including casual staff, contractors and volunteers	All employees are responsible for management of risks within their areas of responsibility as determined under any risk treatment plans. Employees will be responsible for the timely completion of activities contained within these risk treatment plans. Awareness sessions will be conducted routinely to ensure that employees are familiar with risk management and how it is applied within Council.
Risk Monitoring	Council utilises a number of functions, including Internal Audit, to perform independent and objective monitoring over its risk areas, including if necessary, conducting reviews over Council's operations and risk areas by external agencies. The scope of the work undertaken by all of these functions and the reviews by external agencies will be considered in conjunction with Council's risk profile at least annually. This will assess the independent monitoring of key risk areas within Council's risk profile.

Policy Review

This Policy will be reviewed when any of the following evaluations occur:

- Audit reports relating to risk management activities being undertaken by Council indicate that a policy review from a legislative, compliance or governance perspective is justified;
- Relevant legislation, regulations, standards and policies are amended or replaced; and
- Other circumstances as determined from time to time by the Chief Executive Officer or through a resolution of Council.

Notwithstanding the above, this policy and Council's risk management framework will be reviewed at least annually by Council's Management Team to review its effectiveness and to ensure its continued application and relevance.

This policy is to remain in force until otherwise determined by Council.

Manager Responsible for Review: Executive Manager People & Governance

ADOPTED: 29/04/2014
REVISED: 25/06/2019
DUE FOR REVISION: 1/05/2023

DOUGLAS
SHIRE COUNCIL

Enterprise Risk Management Framework and Guidelines

June 2019

Contents

1 Statement of Commitment....1
2 Introduction....1
3 Definitions....2
4 Risk Management Principles....2
5 Risk Management Framework....3
6 Basis, Roles and Responsibilities....4
7 Risk Management Process....4
7.1 Communicate and Consult....5
7.2 Establish the Context....5
7.3 Risk Assessment....5
7.3.1 Identify Risks....5
7.3.2 Analyse Risks....6
7.3.3 Evaluate Risks....8
7.3.4 Risk Register....9
7.4 Treatment of Risks....9
7.5 Monitor and Review....10
8 Recording the Risk Management Process....11
9 Reviewing the Risk Management Framework and Guidelines....11
10 Communication....11
APPENDIX A – RISK APPETITE STATEMENT....12
APPENDIX B – DOUGLAS SHIRE COUNCIL ENTERPRISE RISK MANAGEMENT GENERAL POLICY....14
APPENDIX C – RISK ASSESSMENT TEMPLATE....17
APPENDIX D – RISK TREATMENT PLAN....18

1 Statement of Commitment

The major risk for most organisations is that they fail to achieve their stated strategic business or project objectives, or are perceived to have failed by their stakeholders. Douglas Shire Council is committed to establishing an environment that is not unduly risk averse, but one that enables risks to be logically and systematically identified, analysed, evaluated, treated, monitored and managed. Risk is inherent in all of Council's activities and a formal and systematic process will be adopted to minimise and where possible eliminate all risks that directly or indirectly impact on the Council's ability to achieve the vision and strategic objectives outlined in the Corporate Plan.

Douglas Shire Council is aware that managing risk is not just about avoiding or minimising adverse outcomes, but also has a positive application, in that the proactive analysis of potential risks can also assist the organisation in achieving new and potential opportunities.

This Enterprise Risk Management Guidelines has been developed to demonstrate the Council's commitment, by detailing the integrated Risk Management framework to be employed by all staff members, contractors, committees and volunteers engaged in Council business and defining the responsibilities of individuals and committees involved in managing risk.

In addition the Guidelines have been developed to:

- Ensure risk management is an integral part of strategic planning, management and day to day activities of the organisation;
- Promote a robust risk management culture within the Council;
- Enable threats and opportunities that face the organisation to be identified and appropriately managed within Council's risk appetite and budget;
- Facilitate continual improvement and enhancement of Council's processes and systems;
- Improve planning processes by enabling the key focus of the organisation to remain on core business and service delivery;
- Encourage ongoing promotion and awareness of risk management throughout Council.

2 Introduction

In order for Council to deliver the strategies and achieve the objectives as outlined in the Corporate Plan, Council needs to identify and manage risks. Risk is an event or action, which has the potential to prevent Douglas Shire Council from achieving its corporate objectives. A risk can also be defined as an opportunity that is not being maximised by the Council to meet its objectives.

Enterprise Risk Management (ERM) is the management of risk not only in conventional hazard categories such as health and safety, IT, finance, but in the full spectrum of strategic and operational risk. ERM is the structured approach of aligning strategy, processes, people, technology and knowledge with the purpose of evaluating and managing risk.

Enterprise means the removal of traditional functional, divisional, departmental or cultural barriers. Importantly having a structured approach provides guidance to managing existing and perceived risks that have potential to impact on the organisation's commitment to fulfil its business objectives.

Effective risk management is governed by an organisation's commitment to risk management. Council's risk management process is outlined in this document.

3 Definitions

Risk: A risk to the organisation is any action or event that has the potential to impact on the achievement of our business objectives.

Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

Risk Management: Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council. Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

Enterprise Risk Management (ERM): Enterprise risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information communication technology, compliance, security and business continuity) and includes the coordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

Risk Register: A list of identified and assessed risks directly related to either a particular directorate or to the whole of Council. Risk Registers can be held at either Corporate, Operational, Project or Event level.

Likelihood: The chance of something happening, whether defined, measured or determined objectively or subjectively (probability or frequency).

Consequence: The outcome of an event affecting objectives (impact/magnitude). An event can lead to a range of consequences. A consequence can be certain or uncertain and can have a positive or negative effect on objectives. Consequences can be expressed qualitatively or quantitatively.

Risk Appetite: The amount and type of risk that Council is prepared to pursue, retain or tolerate. It is expressed in the form of a Risk Appetite Statement (Appendix A).

Risk Owner: The person with the accountability and authority to manage a risk. The owner may delegate some duties in relation to managing the risks for which they are responsible, however they are ultimately accountable for the risks allocated to them.

Risk Treatment: The process to modify existing risks or new risks. Some options for treating a risk can include: Retaining, Transferring, Sharing, Avoiding or Controlling.

Risk Treatment Action Plans: The document that outlines the steps to be taken to reduce unacceptable risks to achievable and acceptable levels. This includes details on current controls; required risk treatments; improvement opportunities; resources; timing; reporting and accountabilities. Action Plans must be reviewed on a regular basis to ensure controls are actually working.

4 Risk Management Principles

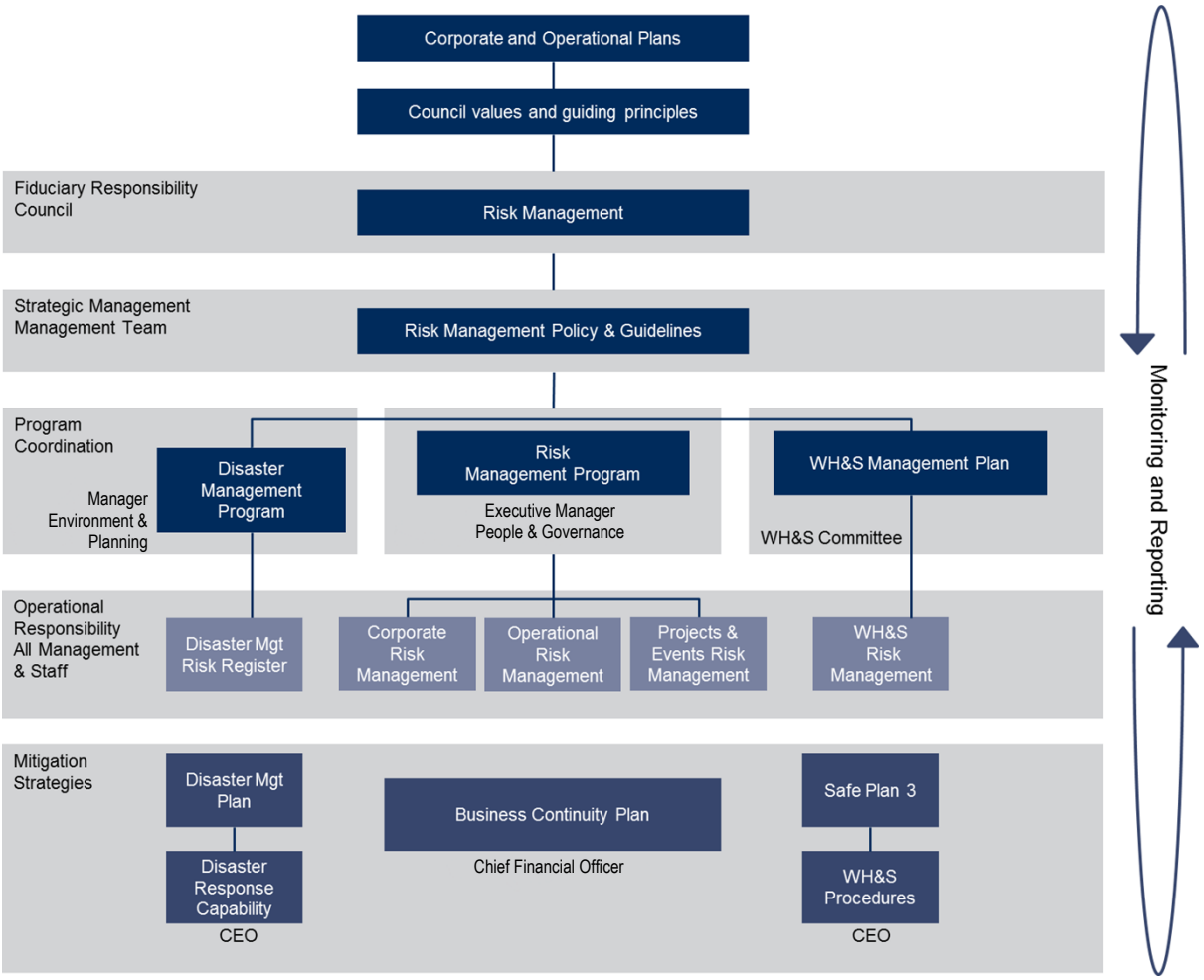
For risk management to be effective, an organisation should comply with the following principles.

Risk management:

- Creates and protects value;
- Is an integral part of organisational processes;
- Is part of decision making;
- Explicitly addresses uncertainty;
- Is systematic, structured and timely;
- Is based on the best available information;
- Is tailored;
- Takes human and cultural factors into account;
- Is transparent and inclusive;
- Is dynamic, iterative and responsive to change; and
- Facilitates continual improvement of the organisation.

5 Risk Management Framework

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



6 Basis, Roles and Responsibilities

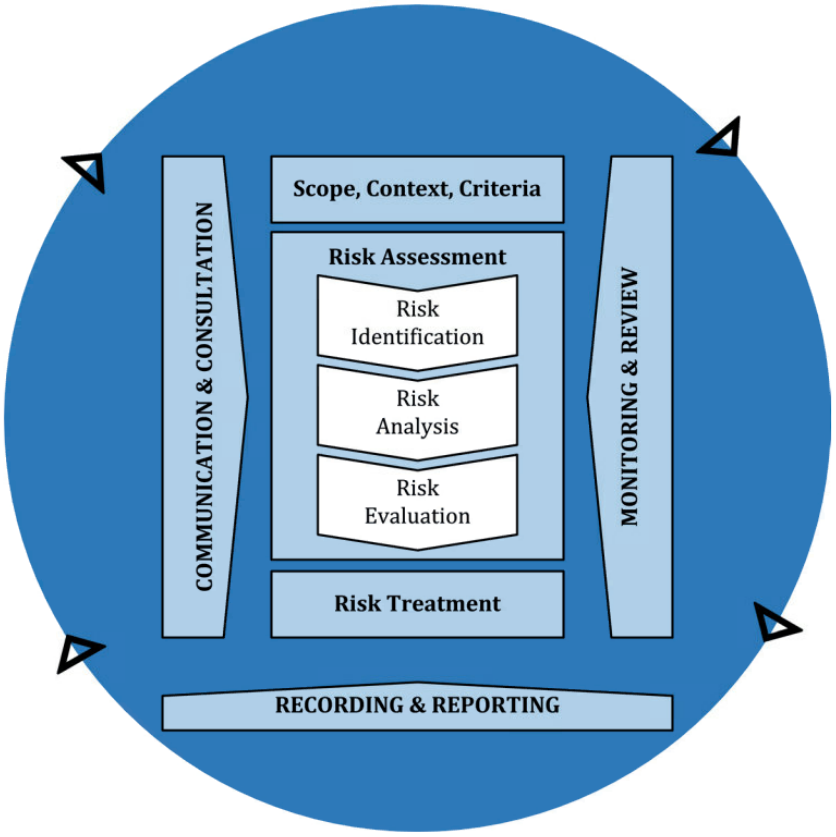
Please refer to Council's Risk Management Policy (Appendix B).

7 Risk Management Process

The process adopted by Douglas Shire Council to manage risks is in accordance with *AS ISO 31000:2018 Risk Management – Guidelines*. This process involves the systematic application of policies, procedures and practices to the activities of:

- communicating and consulting,
- establishing the context, and
- assessing,
- treating,
- monitoring, reviewing,
- recording and
- reporting risk.

The following diagram represents the components of the Risk Management process. Each of these components is explained further below.



Source: Australian Standard for Risk Management – AS ISO 31000:2018

7.1 Communicate and Consult

It is an essential part of the risk management process to develop and implement an effective framework to communicate and consult with all relevant stakeholders, internal and external as appropriate, at each stage of the risk management process and concerning the process as a whole. The level of communication and consultation will vary depending on the level of interest and or influence of that particular stakeholder individual or group. Communication and consultation is necessary at every stage of the Risk Management process.

7.2 Establish the Context

Stage one of the process establishes the strategic, organisational and risk management context in which the rest of the process will take place. This includes the criteria against which risk will be evaluated, the risk appetite of the organisation and corrective actions for the different rating achieved in the assessment of the risks.

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

A written statement of context is to be documented and communicated at the appropriate levels within the organisation.

7.3 Risk Assessment

7.3.1 Identify Risks

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

Categories of risk for the organisation at a strategic and operational level may include, but are not limited to:

Risk Categories	Definition	Code
Financial (Revenue & Costs)	Covers financial capacity, availability of capital, the current economic environment, financial management and reporting, knowledge management, efficiency of systems, processes and organisational structure.	F
Information Technology & Data	Covers the security, function and management of information technology systems, hardware, processes and data.	ITD
Infrastructure Assets/Property	Covers infrastructure asset capacity and management, buildings, equipment, project delivery, inventory and sourcing.	IA
Environment	Covers environmental performance of Council's operations and adverse outcomes relating to air, fauna, flora, water, waste, noise, land sustainability (including Climate Change), hazardous materials and heritage.	EN
Operational – Business Continuity	Covers business continuity issues, (including Information Technology issues), including those attributable to natural and man-made disasters.	BC
Strategic/Corporate Governance – Reputation - Political	Covers Council's reputation with the community, customer service and capability as a regulator. Also the external political environment in which Council operates, including inter-governmental relations, state and national policies and relations with special interest groups.	RE/PO
Workplace Health & Safety	Covers Workplace Health and safety issues.	WHS
Legal Compliance, Regulatory & Liability	Covers legal compliance and liabilities attributable to non-compliance with Acts, regulations, statutory obligations, including class actions, public liability claims, product liability, professional indemnity and public health and safety.	LRL

7.3.2 Analyse Risks

This stage determines the inherent risks and then calculates any residual risks taking into consideration any existing controls in place (existing processes and procedures). Risks are analysed in terms of consequence and likelihood in the context of those controls. The analysis will consider the range of potential risk exposure consequences and how likely those consequences are to occur. The Consequence and Likelihood are then combined to produce an estimated level of risk known as the Overall Risk Rating.

Determining Likelihood

In determining the **likelihood** of each risk, the following ratings and definitions have been applied. In making your assessment you have to remember that some events happen once in a lifetime, others can happen almost every day. Judgement is required to determine the possibility and frequency that the specific risk is likely to occur.

Likelihood Table

Description	Definition - Likelihood of Occurrence
Rare (L1)	Event may occur once in every 10+ years
Unlikely (L2)	Event may occur once in every 5 – 10 years
Possible (L3)	Event may occur once in every 2 – 5 years
Likely (L4)	Event may occur once in every 1 – 2 years
Almost Certain (L5)	Event may occur within one year

Determining Consequence

In determining the consequence of each risk, the following ratings and definitions have been applied. There are five levels used to determine consequence and when considering how risks may impact on the organisation it is also important to think about the non-financial elements as well.

Consequence Table

Description	Qualitative Definition - Consequence
Insignificant (C1)	An event, where the impact can be absorbed; no injuries; low financial loss
Minor (C2)	An event, the consequences of which can be absorbed but management effort is required to minimise the impact; first aid treatment; low-medium financial loss
Moderate (C3)	A significant event, which can be managed under normal circumstances; medical treatment; medium financial loss
Major (C4)	A critical event, which, with proper management can be continued; extensive injuries; loss of service provision; major financial loss
Catastrophic (C5)	A disaster, which could lead to the collapse of the organisation; death; huge financial loss

Quantitative parameters have been developed (Refer Consequence Matrix) to enable the organisation to consistently assign consequence ratings to potential risks. These quantitative measures assign the organisation's risk tolerance parameters applicable to each of the five consequence levels. This approach ensures that all staff can rate the consequence of a risk occurring against the organisation's established parameters, instead of their own personal choice.

Consequence Matrix

Consequence	Rating	Financial (Revenue & Costs)	Information Technology & Data	Infrastructure Assets/Property	Environment	Operational – Business Continuity	Strategic/Corporate Governance- Reputation – Political	Workplace Health & Safety	Legal Compliance, Regulatory & Liability
Catastrophic	5	Huge financial loss (e.g.> 10% of revenue or budget).	Extensive loss of/damage to assets and/or infrastructure. Permanent loss of data. Widespread disruption to the business.	Widespread substantial/permanent damage to assets and/or infrastructure.	Long-term large scale damage to habitat or environmental. Serious/repeated breach of legislation/licence conditions. Cancellation of licence and/or prosecution.	The continuing failure of Council to deliver essential services. The removal of key revenue generation.	Loss of State Government support with scathing criticism and removal of the Council. National media exposure. Loss of power and influence restricting decision making and capabilities.	Fatality or significant irreversible disability.	Extensive breach involving multiple individuals. Extensive fines and litigation with possible class action. DLG review or Administrator appointed
Major	4	Major financial loss (e.g. 5% to 10% of revenue or budget).	High risk of loss/corruption of data; significant catch-up will be required. Business continuity plans should be implemented.	Significant/permanent damage to assets and or infrastructure.	Severe impact requiring remedial action and review of processes to prevent re-occurrence. Penalties and/or directions or compliance order incurred	Widespread failure to deliver several major strategic objectives and service plans. Long-term failure of Council causing lengthy service interruption.	State media and public concern/exposure with adverse attention and long-term loss of support from Council residents. Adverse impact and intervention by State Government.	Extensive injuries. Lost time of more than 4 working days.	Major breach with possible fines or litigation. DLG or Administrator may be involved. Critical failure of internal controls, may have signification and major financial impact
Moderate	3	High financial loss (e.g. 2% to 5% or revenue or budget).	Moderate to high loss of IT. Some data may be permanently lost. Workarounds may be required.	Moderate to high damage requiring specialist/contract or equipment to repair or replace.	Moderate impact on the environment; no long term or irreversible damage. May incur cautionary notice or infringement notice.	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service interruption for a week.	Significant state wide concern/exposure and short to mid term loss of support from Council residents. Adverse impact and intervention by another local government & LGAQ	Medical treatment. Lost time of up to 4 working days	Serious breach involving statutory authorities or investigation. Prosecution possible with significant financial impact. Possible DLG involvement. Moderate impact of legislation/regulations.
Minor	2	Minor financial loss (e.g. ½% to 2% of revenue or budget).	Minor loss/damage to IT and communications. Some data catch-up may be required.	Minor loss/damage. Some repairs may be required.	Minor localised impact; one-off situation easily remedied.	Temporary and recoverable failure of Council causing intermittent service interruption for several days.	Minor local community concern manageable through good public relations. Adverse impact by another local government.	First aid treatment. No lost time	Minor breach with no fine or litigation. Contained non-compliance or breach with short term significance with minor impact. Some impact on normal operations.
Insignificant	1	Low financial loss (e.g. < ½% of revenue or budget.).	Negligible loss or damage to IT hardware and communications. No loss of data.	Negligible damage to or loss of assets.	Minor breach of environmental policy /practices. Negligible impact on the environment	Negligible impact of Council, brief service interruption for several hours to a day.	Transient matter, e.g. Customer complaint resolved in day to day management. Negligible impact from another local government	No injury	Isolated non-compliance or breach. Minimal failure managed by normal operations. Insignificant legislation/regulations.

Determining the overall Risk rating

After the **consequence** and **likelihood** ratings have been determined they are combined in a matrix to determine the overall risk rating for each risk. The extent of the consequences and the extent of the likelihood risks will be assessed using a scale containing **Low, Moderate, High and Extreme.**

The table below illustrates how the combination of the consequence and likelihood generates the overall risk rating.

Risk Assessment Matrix

Likelihood	Rating	Consequence				
		1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	5	Medium L5/C1	High L5/C2	HighL5/C3	Extreme L5/C4	Extreme L5/C5
Likely	4	Medium L4/C1	Medium L4/C2	High L4/C3	High L4/C4	Extreme L4/C5
Possible	3	Low L3/C1	Medium L3/C2	High L3/C3	High L3/C4	High L3/C5
Unlikely	2	Low L2/C1	Low L2/C2	Medium L2/C3	Medium L2/C4	High L2/C5
Rare	1	Low L1/C1	Low L1/C2	Medium L1/C3	Medium L1/C4	High L1/C5

7.3.3 Evaluate Risks

Risks need to be evaluated and prioritised to ensure that management effort is directed towards resolution of the most significant organisational risks first. The initial step is to evaluate whether to accept or manage the risks further with reference to the Risk Appetite Statement.

The next step is to determine the effectiveness, and or existence of, controls in place to address the identified risks. The following table will assist to determine the effectiveness, and or existence of, controls in place to address the identified risks.

Control Assessment	Description
Adequate	• The controls address the identified risk and there is little scope for improvement. • There is no convincing cost/benefit justification to change the approach.
Opportunities for Improvement	• The controls contain some inadequacies and scope for improvement can be identified. • There is some cost/benefit justification to change the approach.
Inadequate	• The controls do not appropriately address the identified risk and there is an immediate need for improvement actions. • There is a significant cost/benefit justification to change the approach.

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

7.3.4 Risk Register

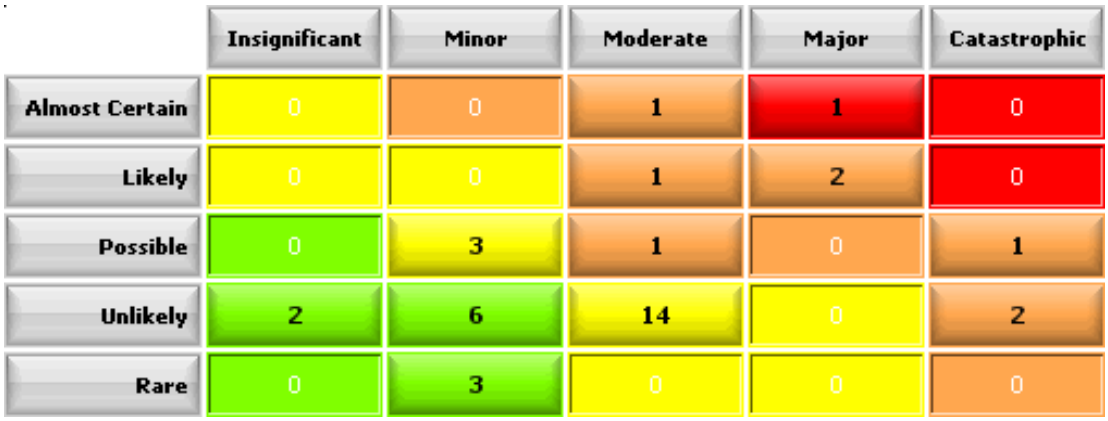
A Risk Register is developed to record and assess each risk identified as part of the risk identification stage.

The application of the stages of the risk assessment process noted above ensure there is consistency in the determination of the current risk severity level, taking into account the existing controls and their level of effectiveness in mitigating or addressing the risk. (Refer to Appendix C for a Risk Assessment Template.)

Risk Profile diagram

At the completion of the assessment process, a risk profile diagram will be developed to highlight each of the risks identified and their overall risk rating.

The risk profile diagram (example below) will highlight to the CEO and Management Team the key risk exposures and number of risks within each rating range across the organisation. The risks will be categorised as **Extreme, High, Moderate and Low** to assist management to target those risks that have the greatest potential impact on the organisation.



	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	0	0	1	1	0
Likely	0	0	1	2	0
Possible	0	3	1	0	1
Unlikely	2	6	14	0	2
Rare	0	3	0	0	0

7.4 Treatment of Risks

After evaluating each risk and appropriate controls, it is the responsibility of the manager to implement the suitable treatment. Treatment needs to be appropriate to the significance and priority of the residual risk. As a general guide:

Risk Treatment Options	
Accept	Where the risk cannot be avoided, reduced or transferred. Usually likelihood and consequences are low.
Control	Reduce the likelihood of occurrence or the consequences (eg: implement procedures or internal controls).
Transfer	Shift all or part of the responsibility to another party who is best able to control it (eg: an insurer who can bear consequences of losses).
Avoid	Decide not to proceed with the activity or project.

Determine the most effective treatment options by considering the:

- Cost/benefit of each option including the cost of implementation (do not consider financial considerations only; organisational, political, social and environmental factors should also rank)
- Use of proven risk controls
- Anticipated level of risk remaining after implementation of risk treatment. The final acceptance of this risk will be a matter for the appropriate Manager to decide.

Once treatment options for individual risks have been selected, they should be assembled into action plans, risk treatment plans or strategies. The outcome of an effective risk treatment plan is knowledge of the risks Council can tolerate and a system that minimises those risks that it cannot tolerate.

The decision to accept a risk will be determined by the agreed table indicating proposed corrective action and the risk appetite criteria established by the Council. For example a Low risk is accepted and only requires monitoring should circumstances change. For other risks, a specific management plan may be required to be developed and implemented which may include consideration of funding. Risk treatment strategies need also to be considered to ensure that no new risks are introduced.

The approach for treatment of risks is:

Risk Level	Appropriate Management Response
Extreme	**Needs Active Management:** A risk action plan must be established and implemented
High	**Needs Regular Monitoring:** Existing good controls should be maintained and any additional risk actions required should be defined and implemented
Moderate	**Needs Periodic Monitoring:** Risk should be monitored in conjunction with a review of existing control procedures
Low	**No Major Concern:** Significant management effort should not be directed towards these risks

Escalation Plan

Procedures should be in place for notifying the appropriate persons according to the risk rating, in particular where a risk may escalate due to changed or unforeseen circumstances.

Reports on risk ratings and associated escalation plans will be provided throughout the organisation to assist all staff in managing risk.

7.5 Monitor and Review

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

Both monitoring and reviewing should be a planned part of the risk management process and tailored to the needs of the organisation and the significance of the risks identified. It should be undertaken on at least an annual basis.

The continual process of monitoring and reviewing is required to ensure ongoing effective risk treatments and the continual improvement of the risk management standards.

- ***Monitoring*** – assess whether current risk management objectives are being achieved. Council can use inspections, incident reports, self-assessments and audits to monitor its risk management plan.

- ***Review*** – assess whether the current risk management plan still matches Douglas Shire Council's risk profile. The risk management plan may be reviewed by studying incident patterns, legislative changes and organisational activities.

Possible methods for review:

- Internal check program/audit or independent external audit;
- External scrutiny (appeal tribunal, courts, commission of inquiry);
- Physical inspection;
- Program evaluation; and
- Reviews of organisational policies, strategies and processes.

When completing the review process, it is important the context in which the original risk was developed is reassessed. The review should also be informed by reports and recent events and include consideration of:

- Completeness of the register;
- Continued existence of controls;
- Adequacy of controls;
- Risk ratings;
- Treatment strategies;
- Risk owner; and
- Risk review date.

8 Recording the Risk Management Process

Each stage of the Risk Management process must be recorded appropriately. All Risk Assessments and Risk Treatment Action Plans must be documented, retained and easily accessible for future reference. Even if a risk is assessed to be Low and a decision is taken to do nothing, the reasoning that led to the decision must be recorded.

9 Reviewing the Risk Management Framework and Guidelines

In order to ensure that the risk management process is effective and continues to support the organisation's performance, all aspects of the risk management process will be periodically reviewed.

The Risk Management Framework and Guidelines, Risk Management Policy and Risk Registers will be reviewed to ensure that they are still appropriate and continue to reflect the organisation's risk activities and tolerances.

Based on the results of monitoring and reviews, decisions will be made on how the Risk Management Framework can be improved. These improvements should lead to improvements in the management of risk and its risk management culture.

10 Communication

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

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

Following reviews of the Framework and Guidelines as specified any changes will be communicated to the relevant Risk Owners and other stakeholders to ensure that the Enterprise Risk Management process remains dynamic and relevant.

APPENDIX A – RISK APPETITE STATEMENT

Council seeks to manage risk carefully. Risk appetite is the amount and type of risk that Council is prepared to pursue, retain or tolerate.

Council's overall risk appetite is 'risk adverse', however Council accepts the taking of calculated risks, the use of innovative approaches and the development of new opportunities to improve service delivery and achieve its objectives provided that the risks are properly identified, evaluated and managed to ensure that exposures are acceptable.

The following are examples of Council's risk appetite over the main areas of consequence:

Financial (Revenue & Costs)

- There is no appetite for risks that have a significant negative impact on Council's long term financial sustainability.
- There is a moderate appetite for activities that may provide additional income streams or enhance economic diversity.

Information Technology & Data

- We have a low appetite for system failures or information and data security breaches.

Infrastructure Assets / Property

- Council has a low appetite for reputational risks that may result in complaints from the community around expectations regarding the maintenance or provision of facilities.

Environment

- There is no appetite for the creation of new contaminated sites or activities that may lead to new sites.
- There is considerable appetite for decisions that promote ecologically sustainable development.

Operational / Business Continuity

- We have a low appetite for operational risks arising from failure to meet customer commitments and/or suitability of advice.
- We have a low appetite for third party partner (contractors) failure.
- There is considerable appetite for improvements to service delivery.
- There is considerable appetite for improved efficiency of Council's operations.

Strategic / Corporate Governance – Reputation – Political

- We have no appetite for internal fraud, collusion, theft and associated reputational risk.
- Council has no appetite for any misconduct based activities by Councillors, employees or external parties.
- We have a low appetite for risks arising from inadequately trained staff or failed internal processes.
- We have a medium appetite in terms of the operational risk associated with the implementation of change and key strategic plans.

Workplace Health & Safety

- There is no appetite for compromising staff safety and welfare.
- There is a low appetite for activities that may affect public safety.

Legal Compliance, Regulatory & Liability

- There is no appetite for non-compliance with legal, professional and regulatory requirements.

- There is no appetite for major breaches or activities that may result in successful litigation against Council or for the non-reporting of breaches to appropriate authorities once they are recognised.

KEY: considerable appetite / medium appetite / low appetite / no appetite

APPENDIX B – DOUGLAS SHIRE COUNCIL ENTERPRISE RISK MANAGEMENT GENERAL POLICY

Intent

This policy outlines Council's commitment to the development and maintenance of an enterprise risk management framework.

Scope

This policy applies to all elected representatives and staff who are involved in the identification and management of risks associated with Council achieving its goals, objectives and operational activities.

Reference

Legislation: *Local Government Regulation 2012*

Other: Australian AS ISO 31000:2018 Risk Management – Guidelines

Provisions

Douglas Shire Council recognises that as a public authority it is exposed to a broad range of risks which, if not managed, could adversely impact on the organisation achieving its strategic objectives. Therefore Council will implement a systematic risk management methodology to identify and address, where practical, areas of potential risk within Council. Any methodologies adopted will be consistent with *Australian Standard AS ISO 31000:2018 Risk Management – Guidelines*.

The intent of this policy is to create an environment where Council, management and staff assume responsibility for risk management, through consistent risk management practices.

Objectives

The objectives of this policy are:

- Align Council activities to and support business objectives identified in Council's Corporate and Operational Plans;
- Maintain and improve reliability and quality of service provided by Council, within Council's controls and capabilities;
- Minimise or eliminate adverse impacts from Council's services or infrastructure on the community, visitors and the environment;
- Capitalise on opportunities identified for Douglas Shire Council;
- Safeguard Council's employees, contractors, committees, volunteers, assets, financial sustainability, property, reputation and information;
- Promote risk management principles as a strategic tool to ensure better informed decision making throughout Council; and
- Embed a culture of risk management across the Council.

Principles

The following principles will be adopted to ensure that the objectives are achieved:

- Apply a risk management framework which is consistent with the current *Australian Standard AS ISO 31000:2018 Risk Management – Guidelines* for making decisions on how best to identify, assess and manage risk throughout all departments of Council;
- Prioritise identified risks and implement treatments progressively based on the level of risk assessed and the effectiveness of the current treatments;

- Integrate risk management with existing planning and operational processes, including the Corporate Plan;
- Take into account relevant legislative requirements and political, social and economic environments in managing risks;
- Create a culture of risk awareness throughout the organisation through training, induction, promotion and risk review and reporting mechanisms; and
- Ensure resources and operational capabilities are identified and responsibility for managing risk is allocated.

Definitions

Risk - A risk to the business is any action or event that has an effect of uncertainty on objectives of Douglas Shire Council. It is measured in terms of consequence and likelihood.

Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

Risk Management - Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council.

Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

Enterprise Risk Management (ERM) - Enterprise risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity) and includes the coordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

Risk Register - The risk register lists identified and assessed risks.

Roles and Responsibilities

Council	Council is responsible for adoption of this policy and retains the ultimate responsibility for risk management and for determining the appropriate level of risk that it is willing to accept in the conduct of Council business activities. Council will review the effectiveness of the risk management systems.
Chief Executive Officer	Council's Chief Executive Officer is responsible for identifying, evaluating and managing risk in accordance with this policy through a formal enterprise-wide risk management framework. Formal risk assessments must be performed at least once a year as part of the business planning and budgeting process. The Chief Executive Officer will report to Council annually on the progress made in implementing a sound system of risk management and internal compliance and control across Council's operations.
Management Team	Council's Management Team will perform the function of the Risk Management Committee which has oversight of developing the risk management framework and monitoring risk treatment. The team will ensure the risk management framework identifies high-level strategic risks and aligns with the Internal Audit Plan. The Management Team will ensure that the results of its reviews are provided to Council for update of the Council's risk

	profile as appropriate. The Management Team will also ensure periodic reviews of the risk management framework are carried out by Internal Audit pursuant to the Internal Audit Plan.
Coordinators / Team Leaders	Council's Coordinators and Team Leaders are responsible for the accuracy and validity of risk information reported to the Council. In addition, this will ensure clear communication throughout the organisation of Council's position on risk.
Employees including casual staff, contractors and volunteers	All employees are responsible for management of risks within their areas of responsibility as determined under any risk treatment plans. Employees will be responsible for the timely completion of activities contained within these risk treatment plans. Awareness sessions will be conducted routinely to ensure that employees are familiar with risk management and how it is applied within Council.
Risk Monitoring	Council utilises a number of functions, including Internal Audit, to perform independent and objective monitoring over its risk areas, including if necessary, conducting reviews over Council's operations and risk areas by external agencies. The scope of the work undertaken by all of these functions and the reviews by external agencies will be considered in conjunction with Council's risk profile at least annually. This will assess the independent monitoring of key risk areas within Council's risk profile.

Policy Review

This Policy will be reviewed when any of the following evaluations occur:

- Audit reports relating to risk management activities being undertaken by Council indicate that a policy review from a legislative, compliance or governance perspective is justified;
- Relevant legislation, regulations, standards and policies are amended or replaced; and
- Other circumstances as determined from time to time by the Chief Executive Officer or through a resolution of Council.

Notwithstanding the above, this policy and Council's risk management framework will be reviewed at least annually by Council's Management Team to review its effectiveness and to ensure its continued application and relevance.

This policy is to remain in force until otherwise determined by Council.

Manager Responsible for Review: Executive Manager People & Governance

ADOPTED: 29/04/2014
REVISED: 25/06/2019
DUE FOR REVISION: 1/05/2023

APPENDIX C – RISK ASSESSMENT TEMPLATE

Enterprise Risk Management - Risk Assessment Template										
Division/Group					Date					
Department					Function/Activity					
Section										
Risk Type					Critical BCP Process				Yes/No	
Risk	Risk Category	L	C	Inherent Level of Risk	Inherent Priority Rating	Control Measures	L	C	Residual Level of Risk	Residual Priority Rating

APPENDIX D – RISK TREATMENT PLAN

Risk Number	Category	Description
Accountable Officer		

Date		*Date*					
Likelihood		Likelihood					
Conseq. Level		Conseq. Level					
Inherent Risk Rating		Residual Risk Rating					

Source of Risk: *(How might the risk arise?)*	
Risk Treatment: *(What can be done to avoid the risk, control, transfer or finance the risk?)*	
Performance Measure: *(How will you know the risk treatment is working?)*	
What is the plan?	
Resources Required: *(What physical, human or financial resources required?)*	
Associated Documents: *(InfoExpert Doc ID)*	
Timeline:	

Matters arising from review:	
Date reviewed by MT:	
Matters arising from review:	
Date reviewed by MT:	
Matters arising from review:	
Date reviewed by MT:	
Matters arising from review:	
Date reviewed by MT:	