RISK MANAGEMENT FRAMEWORK

Table of Contents

WHAT IS RISK?

Often people think of risk as what might go wrong in an organisation. But a more precise definition is the effect of uncertainty on an organisation's objectives. In this regard, risk includes both potential threats to achieving those objectives (negative risk), and potential opportunities for achieving those objectives (positive risk).

Threats and opportunities come and go, or evolve, as an organisation's internal dynamics change, as its relationships with stakeholders change, and as the external environment in which it operates changes. Keeping abreast of the risks that may affect your organisation must therefore be an ongoing activity.

Katherine Town Council recognises that risk is inherent in carrying out all of its business strategies and operations and that without a robust system for identifying and managing risks, Council is vulnerable to uncertainties and lost opportunities and is unlikely to be resilient in the face of change or adversity.

THE PRINCIPLES OF RISK MANAGEMENT

The Australian Standard (AS ISO 31000:2018) contains eleven Principles which provide useful guidance for integrating risk management into an organisation. These Principles are that risk management:

1. creates and protects value
2. is an integral part of all organisational processes
3. is part of decision-making
4. explicitly addresses uncertainty
5. is systematic, structured and timely
6. is based on the best available information
7. is tailored to the organisation's requirements
8. takes human and cultural factors into account
9. is transparent and inclusive
10. is dynamic, iterative and responsive to change
11. facilitates continual improvement of the organisation.

RISK MANAGEMENT PRINCIPLES
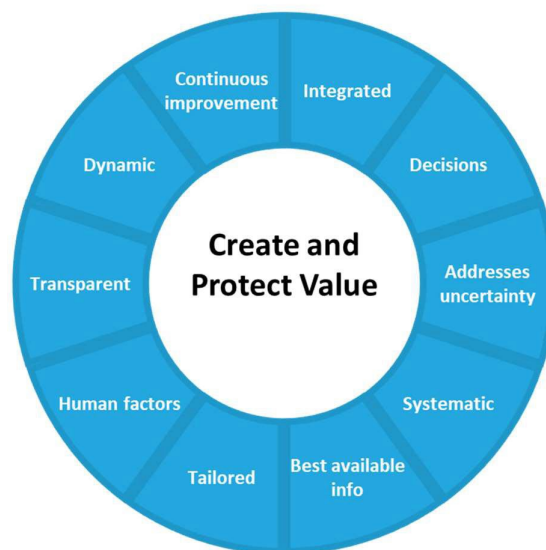
COUNCIL'S RISK MANAGEMENT APPROACH

Council will ensure that risk management is a key consideration in all business practices and decision-making processes. Council's Risk Management Framework provides the foundations and organisational arrangements necessary to embed a proactive, structured and consistent approach to risk management throughout the organisation.

Council seeks to implement an effective risk management system which conveys to managers they are responsible for ensuring that risks are identified, controls are established, documented, maintained and adhered to across the council and to all employees that they are responsible for adhering to those controls.

Ultimately Council seeks to achieve an environment where, with the provision of ongoing guidance, Council staff retain the skills to effectively contribute to achieving Council's objectives, whilst endeavouring to protect Council, its staff, the community, key stakeholders and assets from the adverse effects of risks.

The Risk Management Framework applies to all levels of the organisation – elected members, Council staff, management, key stakeholders, contractors, service providers and the like. It extends to all of Council's current and future strategic and operational activities, business practices, policies, strategies, plans and procedures, as well as new opportunities for the organisation and the community.

COUNCIL'S OBJECTIVES

Through the implementation of an integrated and consistent approach to risk management, Council aims to achieve the following risk management objectives:

- An organisational culture of reliable, informed, evidence-based planning and decision making
- A consistent approach to the identification, assessment and treatment of risks
- Improved operational effectiveness and efficiency
- Staff accountability for risk identification and treatment
- Improved corporate governance, controls and performance
- Improved community and stakeholder confidence and trust by providing assurance that risks are appropriately managed
- Reduced liability exposure and financial loss
- Safeguarding of Council's resources - its people, finance, property and reputation.

RISK MANAGEMENT CULTURE

Council will effectively communicate and engage with staff at all levels of the organisation to build a positive risk awareness culture that encourages all staff to proactively manage risks. Council will do this by:

- 'setting the tone at the top', ensuring elected members and Council's leadership team promote and commit to risk management in a positive and proactive manner and communicate this with all staff
- engaging with staff about the benefits of risk management
- communicating risk management roles and responsibilities
- providing risk management support and resources including easily accessible risk management tools, and
- integrating risk management into strategic and business planning processes.

KEY RISK CATEGORIES

Nine categories of risk have been established:

| Category	Description
People and Culture	Risks associated with human resource management, organisational culture and change management. This includes non-workplace health and safety risks that impact on the ability of employees to attend work and perform their duties (i.e. industrial action etc).
Health and Safety	Risks associated with protecting the health, safety and wellbeing of employees, volunteers, contractors and others within Council's duty of care. This covers workplace health and safety risks that impact on the ability of employees to attend work and perform their duties (i.e. injury, illness, pandemic etc).
Financial Sustainability	Risks associated with the financial management of Council and its ability to fund Council services now and into the future. This covers risks related to revenue, expenditure, budget management, investments and debt management and accuracy of financial information.
Legal and Governance	Risks associated with Council either knowingly or unknowingly breaching legislation, regulations, policies or procedures. This covers risks related to fraud and corruption or being exposed to liability in relation to any matter.
Reputation	Risks associated with Council's perceived or actual reputation with the community, government, regulators, the media, Council employees, or other stakeholders. This covers risks of a political nature.
Service Delivery	Risks associated with the daily operational management of Council and its ability to deliver services to the community. This also covers risks related to the effectiveness of internal services, systems and processes, and business continuity.
Information and Technology	Risks associated with the provision of ICT infrastructure, services and systems for Council and the community. This covers risks related to the loss or theft of data and information, and cyber security.
Asset Management	Risks associated with the planning, design, construction and maintenance of Council infrastructure and assets. This covers risks related to fit for purpose considerations and the damage or loss of assets and property.
Environment	Risks associated with Council's operations that have potential or actual negative environmental, ecological or cultural heritage impacts, regardless of whether these are reversible or irreversible in nature. This also covers risks associated with the impact of climate change on Council's assets and operations.

RISK APPETITE

Council has an obligation to the community to ensure that it does not accept high levels of risk that might impact on community wellbeing, amenity or the ongoing sustainability and viability of Council. Accordingly, Council generally has a low appetite for unmitigated risks across all of its operations, assets and objectives. However, given the significant growth that the Katherine region will experience in coming years, Council may need to take some calculated risks to ensure that infrastructure and services meet the needs of its current and future communities.

Council has no tolerance for risks that may compromise the safety and welfare of staff, the community, contractors and volunteers. Similarly, 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.

THE RISK MANAGEMENT PROCESS

The risk management process consists of seven steps. Each step of the risk management process is considered in detail below.
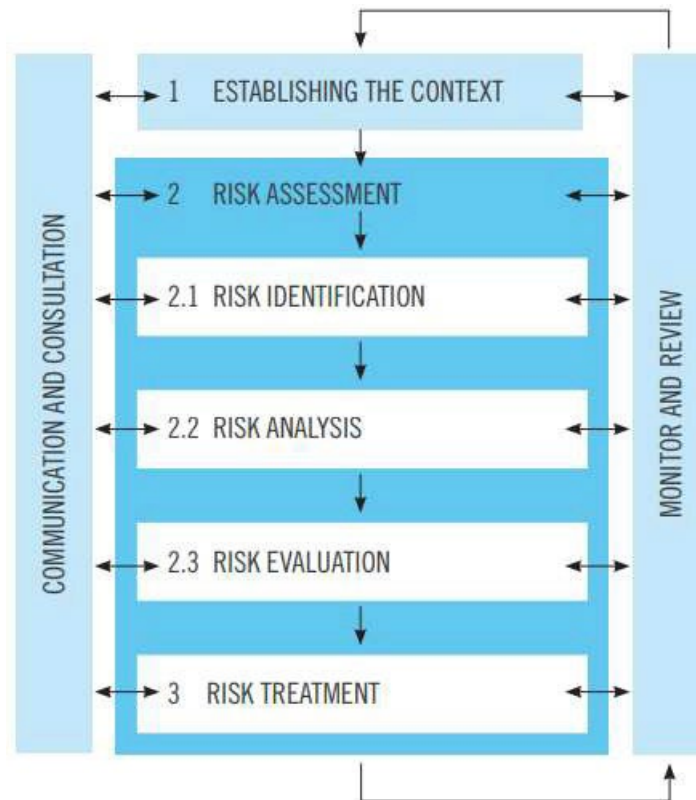
Source: Australian Standard for Risk Management AS ISO 3100:2018

While the steps are shown separately within this process, the risk management process is a continuous loop.

Establishing 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 ratings achieved in the assessment of the risks. In considering context, it is essential to consider the broader external environment in which the organisation operates and not just internal matters.

Risk identification

Identifying risks involves consideration of what, how, why and when events might occur that could have an impact on achieving the objectives of the activity or operation. During this process consideration is to be given to Council's nine risk categories (outlined previously).

A variety of methods can be used to identify risks, such as interviewing individuals, team brainstorming and SWOT analysis. Relevant, appropriate and up to date information is important to identify risks.

A Risk Register is developed to record and assess each risk identified. The application of the stages of the risk assessment process will ensure there is consistency in the determination and documentation of the risk severity level, taking into account the existing controls and their level of effectiveness in mitigating or addressing the risk.

Risk analysis

Risk analysis is undertaken to determine and understand the level of risk being faced. It involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, control measures and their effectiveness. Risk analysis provides input to risk evaluation, decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment and methods.

This stage determines the inherent risks and then calculates any residual risks taking into consideration any existing controls in place (such as 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.

In determining the likelihood of each risk, the following ratings and definitions are applied. In making an assessment it is important to remember that while some events happen infrequently, others can happen almost every day. Judgement is required to determine the possibility and frequency that the specific risk is likely to occur. Table 1 outlines the measures of likelihood.

Table 1: Measures of Likelihood

Level	Rating	Description	Estimated Probability
5	Almost certain	The event is expected to occur in most circumstances in the current environment; frequent past event history	>90%
4	Likely	The event will probably occur in most circumstances in the current environment; some recurring past event history	61-90%
3	Possible	The event might occur at some time; some past warning signs or previous event history	21-60%
2	Unlikely	The event could occur at some time, no event history	20-20%
1	Rare	The event may occur but only in exceptional circumstances; no past event history	<2%

In determining the consequence of each risk, the following ratings and definitions are applied. Table 2 outlines the five levels used to determine consequence when considering how risks may impact Council.

Table 2: Consequence levels

Level	Consequence rating	Description
1	Insignificant	An event, where the impact can be absorbed; no injuries; low financial loss
2	Minor	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
3	Moderate	A significant event, which can be managed under normal circumstances; medical treatment; medium financial loss
4	Major	A critical event, which, with proper management can be continued; extensive injuries; loss of service provision; major financial loss
5	Catastrophic	A disaster, which could lead to the collapse of the organisation; death; huge financial loss

Quantitative parameters have been developed (refer to **Attachment 1 – Measures of Consequence**) to enable Council to consistently assign consequence ratings to potential risks. These quantitative measures assign Council'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 Council's established parameters, instead of their own personal choice.

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 likelihood and consequences will be assessed using a scale containing Low, Medium, High and Extreme. Table 3 below illustrates how the combination of the consequence and likelihood generates the overall risk rating.

Table 3: Overall risk rating

Consequence		1	2	3	4	5
Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	5	MEDIUM	HIGH	HIGH	EXTREME	EXTREME
Likely	4	LOW	MEDIUM	HIGH	HIGH	EXTREME
Possible	3	LOW	MEDIUM	MEDIUM	HIGH	HIGH
Unlikely	2	LOW	LOW	MEDIUM	MEDIUM	HIGH
Rare	1	LOW	LOW	LOW	LOW	MEDIUM

As each risk is assessed, it will be assigned to an owner who will be responsible for managing it. Risk owners are usually senior managers or staff who have authority to manage risks and to allocate resources for risk treatment actions. Assigning ownership to risks is an important element in integrating risk management into Council's operations because it improves accountability for managing risks within acceptable, or valid, levels of tolerance and for escalating any risks deemed unacceptable.

Risk evaluation

The purpose of risk evaluation is to support decisions. It involves comparing the results of the risk analysis with the Council's established risk criteria to determine if the level of risk is acceptable or additional action is required to continue with the activity or operation being assessed. Options may be to do nothing; consider additional risk treatment options; undertake further analysis; maintain existing controls; reconsider objectives; or cease the activity until risks can be managed, and it should consider the wider context and the action and perceived consequences to both internal and external stakeholders.

Risk treatment

Risk treatment involves the development and implementation of additional controls, such as systems and procedures, to address the risk. Risk treatment is an iterative process of formulating and selecting risk treatment options; planning and implementing risk treatment; assessing the effectiveness of the treatment; deciding on whether the remaining risk is acceptable and if not acceptable, implementing further controls. Depending on the activity or operation that is being assessed and the priority of the risk, risk treatment strategies can involve the development and implementation of long- or short-term risk treatment action plans.

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 annual monitoring unless 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. Table 4 outlines Council's appropriate management response for each level of assessed risk.

Table 4: Management response

RANK	DESCRIPTION	CRITERIA FOR RISK ACCEPTANCE	RESPONSIBILITY
EXTREME	Urgent attention and active management	Consider ceasing activity or accept the risk ONLY if strong controls and treatment plans are in place. Monthly monitoring and review.	CEO/Council
HIGH	Regular monitoring	Existing strong controls should be maintained, and any additional risk actions required should be defined and implemented. Monthly monitoring and reporting.	Director/CEO
MEDIUM	Periodic monitoring	Review existing controls. Periodic (quarterly) monitoring and reporting.	Manager
LOW	No major concern	Management effort should not be directed towards these risks. Annual monitoring and reporting.	Manager

Communication and consultation

Communication and consultation with relevant internal and external stakeholders are to be undertaken at all stages of the risk assessment process to bring different areas of expertise together, ensure different views are appropriately considered, provide sufficient information to facilitate risk oversight and decision-making and to build a sense of inclusiveness and ownership among those affected by the risk. It involves promoting awareness and understanding, as well as seeking feedback and information to support decisions made throughout the process.

Monitoring and review

Monitoring and review of the risk management process, its implementation and outcomes provide continued quality and effectiveness and identifies opportunities for improvement. It ensures that identified risks and controls remain relevant, controls remain effective and that any new risks are appropriately identified, recorded and managed appropriately. It should be a planned and documented part of each stage of the process and associated responsibilities should be clearly defined.

The risk management process and its outcomes are required to be documented and reported regularly to ensure continued communication in relation to risk management activities and outcomes, to provide information for decision-making, to improve risk management activities and to assist interaction with stakeholders.

The Audit and Risk Management Committee is an independent advisory body established within Council under the section 86 of the *Local Government Act 2019*.

The Audit and Risk Management Committee plays a central role in independently reviewing Council's internal control processes and provides elected members with a level of assurance on the effectiveness of the Council's financial and corporate governance practices as well as compliance with legislative and regulatory requirements. The Audit and Risk Management Committee can assist in identifying areas where changes are required to reduce the risk of Council's exposure to fraud or unauthorised transactions.

The role of the Audit and Risk Management Committee includes:

- Monitoring the effectiveness of the audit function and the implementation of audit recommendations
- Providing an independent line of reporting by the auditor to Council
- Reviewing compliance with legislative requirements, contracts, standards and best practice guidelines
- Reviewing and recommending to Council the annual financial statement

- Monitoring changes in accounting and reporting requirements
- Reviewing policies relating to codes of conduct, conflicts of interest, misconduct, fraud and revenue.

The Risk Register will be reviewed annually by the Risk Framework Owner, in consultation with elected members, managers and staff, the Audit and Risk Management Committee and other relevant stakeholders.

ROLES AND RESPONSIBILITIES

The risk management responsibilities at the various levels of the organisation are defined below:

Role	Responsibilities
All staff	- All employees and volunteers are required to identify and manage risks in their area of operation and responsibility. - Report risk related incidents in a timely manner.
Elected members	- Set the organisational risk appetite and acknowledge the need for resources to support the achievement of risk management objectives. - Consider risk in the exercise of policy setting and decision-making and advice relating to risk management contained in Council reports. - Give due consideration to recommendations from Council's Audit and Risk Management Committee. - Foster a risk aware culture.
Chief Executive Officer	- Foster a risk aware culture. - Provide advice to Council about risks and controls and report known potential risks, emerging risks or major incidents to Council in a timely manner. - Ensures overall accountability, authority and resources for risk management. - Establish internal controls and associated frameworks. - Develop, review and refine Council's Strategic Risk Register and Risk Management Framework.
Leadership team	- Provide advice to Council on the risk appetite, promote risk management across the organisation and ensure risk management is embedded in their area of operation. - Ensure the allocation of appropriate resources for the implementation and maintenance of Council's Risk Management Framework. - Assist the CEO to develop, review and refine Council's Strategic Risk Register and Risk Management Framework.
Directors and managers	- Manage strategic and operational risk in their respective areas of accountability and responsibility and to support employees in identifying, managing and communicating risk. - Promote effective risk management in support of an organisational risk aware culture.
Risk Framework Owner	- Provide leadership, organisational awareness and engagement of risk management. - Ensure the effective implementation of the risk management framework. - Monitor risk register and risk treatment plans/controls and report regularly to the CEO on risks. - Oversight Council insurance policies and claims, to ensure that Council has adequate cover. - Review and update the risk register annually.
Audit and Risk Management Committee	- Endorse the Risk Management Framework and ensure that risk management processes and procedures appropriately identify and manage Council's risks. - Review and monitor risks and controls and provide recommendations to Council. - Ensure Council strategic risk direction is aligned with industry best practice standards.

DEFINITIONS

Consequence means the outcome of an event; it can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Control means any measure that maintains and/or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which mitigate and/or modify risk.

Level of risk (risk rating) means the magnitude of a risk or combination of risks, expressed in terms of the combination of consequence and their likelihood.

Likelihood means chance of the risk happening**.**

Operational risk means those risks that arise in day-to-day operations, and which may require specific and detailed response and monitoring regimes. If not treated and monitored, operational risks could potentially result in major adverse consequences for the agency.

Risk means the likelihood of something happening that will have an adverse impact upon objectives, and/or harmful consequences. Risk is measured in terms of consequences and likelihood and covers threats and opportunities.

Risk appetite means the level of risk that Council is willing to accept, at any point in time, in achieving its strategic objectives, and when delivering services and projects for the community.

Risk Framework Owner (RFO) means the Director, Corporate Services.

Risk management means the set of co-ordinated activities applied in the organisation to direct and control risk.

Risk register means the centralised reporting tool used to record risk, controls, and opportunities.

Risk treatment means the process of selecting and implementing measures or 'treatment options' to modify risks or their potential consequences.

Strategic risk means risks that may affect Council's ability to meet its strategic objectives and require oversight by Council executives. Elected members and the Audit and Risk Management Committee.

ASSOCIATED COUNCIL POLICIES/DOCUMENTS

Workplace Health and Safety Policy and Directives

Fraud and Corruption Control Policy Protection Plan

Audit and Risk Management Committee Charter 2020

Investment Policy

Procurement Policy

Asset Management Policy

REFERENCES AND RELATED LEGISLATION

Local Government Act 2019

Local Government (General) Regulations 2021

Work Health and Safety (National Uniform Legislation) Act 2011

AS/NZS ISO 31000:2018 Risk management – Principles and guidelines (ISO 31000)

ATTACHMENT 1 – MEASURES OF CONSEQUENCE

Level	1	2	3	4	5
Rating	Insignificant	Minor	Moderate	Major	Catastrophic
People and Culture	Negligible capability impact or effect on service delivery	Minor impact to capability that could be filled internally, some impact on service delivery	Unavailability of core staff leading to reduced service delivery	Unavailability of critical staff significantly impacting service delivery	Protracted unavailability of critical skills/people preventing core activities from being undertaken
Health and Safety	No injury but hazard identified	Minor personal injury, first aid required	Injury or illness, medical treatment required	Lost time injury or illness requiring hospitalisation and numerous days off work	Fatality(ies) or permanent disability or ill-health
Financial Sustainability	Less than $2,000	$2,000 - $20,000	$20,001 - $200,000	$200,001 - $500,000	More than $500,000
Legal and Governance	Isolated non-compliance of minimal significance; minor fine; internal staff warning	Minor breach of legal obligations; improvement notice; minor fine / penalty (<$10K)	Substantial breach of legal obligations; adverse finding; substantial fine / penalty (>$10k)	Significant breach of legal obligations; adverse finding with long term significance; significant fine / penalty (>$100K)	Major breach of legal obligations; adverse findings against Council and / or individuals; major fines or penalties (>$500k); possible imprisonment; dismissal of Council
Reputation	Unsubstantiated, localised low impact on key stakeholder trust, low profile or no media item	Substantiated, localised impact on key stakeholder trust or low media item	Substantiated, public embarrassment, moderate impact on key stakeholder trust or moderate media profile	Substantiated, public embarrassment, widespread high impact on key stakeholder trust, high media profile, third party actions	Substantiated, public embarrassment, widespread loss of key stakeholder trust, high widespread multiple media profile, third party actions
Service Delivery	No material service interruption	Temporary interruption to an activity – backlog cleared with existing resources	Interruption to service unit/(s) deliverables – backlog cleared by additional resources	Prolonged interruption of critical core service deliverables – additional resources required; performance affected	Indeterminate prolonged interruption of critical core service deliverables – non-performance

Level	1	2	3	4	5
Rating	Insignificant	Minor	Moderate	Major	Catastrophic
Information and Technology	Compromise of information otherwise available in the public domain	Minor compromise of confidential information	Substantial compromise of sensitive or confidential information	Extensive compromise of sensitive or confidential information or cyber attack	Significant and ongoing compromise of confidential information or widespread cyber attack
Asset Management	Inconsequential damage	Localised damage rectified by routine internal procedures	Localised damage requiring external resources to rectify	Significant damage requiring internal and external resources to rectify	Extensive damage requiring prolonged period of restitution / complete loss of plant, equipment and building
Environment	No environmental damage	Minor instances of environmental damage that could be reversed	Isolated but significant instances of environmental damage that might be reversed with intensive efforts	Severe loss of environmental amenity and danger of continuing environmental damage	Major widespread loss of environmental amenity and progressive irrecoverable environmental damage