Kowanyama Aboriginal Shire Council

Enterprise Risk Management Framework and Guidelines

Contents

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. Kowanyama Aboriginal Shire Council (KASC) 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.

Kowanyama Aboriginal 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;
- 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 the 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 Kowanyama Aboriginal 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 and this process is outlined in Council's Risk Management Framework and Guidelines which is in line with the Australian Standard AS/NZS ISO 31000:2009 Risk management – Principles and guidelines.

3 Definitions

Risk: A risk to the business 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 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 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 create new risks. Options for treating a risk 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.

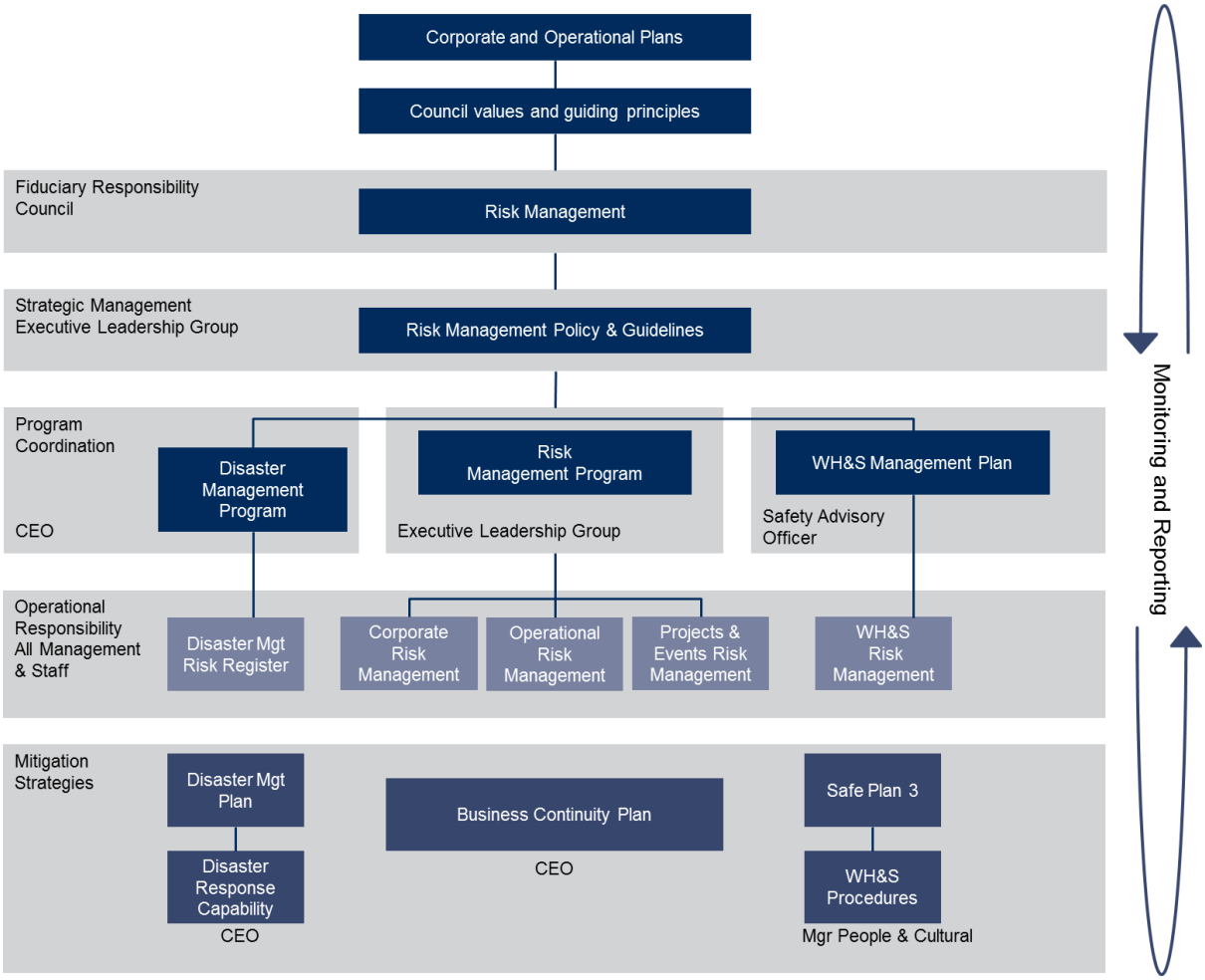
4 Risk Management Principles

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

- Risk management creates and protects value;
- Risk management is an integral part of organisational processes;
- Risk management is part of decision making;
- Risk management explicitly addresses uncertainty;
- Risk management is systematic, structured and timely;
- Risk management is based on the best available information;
- Risk management is tailored;
- Risk management takes human and cultural factors into account;
- Risk management is transparent and inclusive;
- Risk management is dynamic, iterative and responsive to change; and
- Risk management 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. Council is currently developing our risk management framework in line with the following structure:



6 Basis, Roles and Responsibilities

Please refer to Council's Enterprise Risk Management Policy

7 Risk Management Process

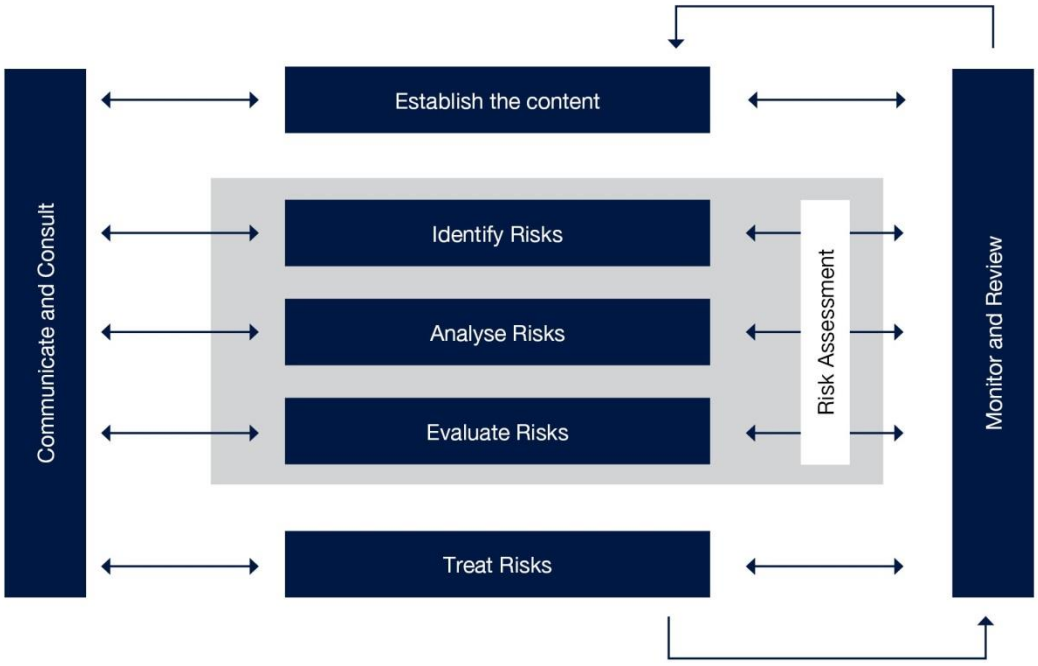
The process adopted by Kowanyama Aboriginal Shire Council to manage risks is in accordance with *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines*. This process is the application of the structured risk management methodology to be used to assess; prioritise; treat and monitor risks identified. The risk management process may capture inherent risk (prior to taking into account controls in place), residual risk (after taking into account controls in place), or both.

The main elements of an effective Risk Management approach are as follows:

- Communicate and Consult
- Establish the Context
- Risk Assessment
    - Identify Risks
    - Analyse Risks

- Evaluate Risks
- Treat Risks
- Monitor and Review

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



Source: Australian/New Zealand Standard for Risk Management – AS/NZS ISO 31000:2009

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.

In establishing the context for these Risk Management Guidelines, existing risk management processes were reviewed, interviews and workshops were held with key personnel and a Risk Management Policy was developed. (Refer to Appendix A for Council's Risk Management Policy).

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 (Exposure Types)
Property Covers infrastructure asset capacity and management, project delivery, inventory and sourcing.
Provision of Service Performance Risks associated with the delivery and/or disruption of Council services. Also covers business continuity issues including those attributable to natural and man-made disasters.
Regulatory Covers legal compliance and liabilities attributable to non-compliance with statutory obligations, including class actions, public liability claims, product liability, professional indemnity and public health and safety.
Reputation Covers Council's reputation with the community, customer service and capability as a regulator.
Management Effort Covers the external environment in which Council operates, including inter-governmental relations, state and national policies, disaster management, special events and interest groups.
Environment Covers environmental performance of Council's operations including adverse outcomes relating to air, fauna, flora, water, waste, noise & vibration, land, sustainability, hazardous materials and heritage
Financial (Revenue & costs) Financial and Economic covers financial capacity, availability of capital, the current economic environment, financial management and reporting, knowledge management, efficiency of systems, processes and organisational structure.

People Includes human resource, industrial relations and organisational culture particularly relating to staff values, standards of integrity and public accountability. Also covers Work Health and Safety issues, injury management and workers compensation
Information & Data Risks relating to the security, storage, function and management of information technology systems and processes

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, other 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	Likelihood of Occurrence
Almost Certain	The event is expected to occur in most circumstances, say several times per month
Likely	The event will probably occur in most circumstances, say once per year
Possible	The event might occur, say once in every 2-3 years
Unlikely	The event could occur at some time, say once in every 4-8 years
Rare	Event may only occur in only exceptional circumstances

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	An event, that the impact can be absorbed; no injuries; low financial loss
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
Moderate	A significant event which can be managed under normal circumstances; medical treatment; medium financial loss
Major	A critical event, which with proper management can be continued; extensive injuries; loss of production capability; major financial loss
Catastrophic	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

Rating/ Descriptor	Financial (Revenue & Costs)	Information & Data	Property	People	Provision of Service/ Performance	Environment	Reputation	Regulatory	Management Effort
Insignificant	Below $50K	Negligible loss of or damage to IT and communications. No loss of data.	Negligible damage to or loss of assets.	No significant injuries. No significant impact on personnel.	Short-term, localised interruption to service/performance	Minor breach of environmental policy/practices. Negligible impact on the environment.	Negligible impact on reputation.	Isolated breaches/minor incidents.	An event, the impact of which can be absorbed through normal activity.
Minor	$50K to $250K	Minor loss/damage to IT and communications. Some data catch-up may be required.	Minor loss/damage. Some repairs may be required.	Small number of injuries, first aid or out-patients treatment required. Some inconvenience to personnel.	Minor, temporary disruption to services. Minor inconvenience to client(s).	Minor localised impact, one-off situation easily remedied.	May cause some complaints (justified or unjustified).	Segmented incidents. More moderate breaches attracting a "warning".	An event, the impact of which can be absorbed, but management effort is needed.
Moderate	$250K to $500K	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.	A number of injuries requiring hospitalisation and long-term treatment. Moderate disruption to work routines and schedules.	Some serious disruption to services, some contravention of legal/contractual obligations.	Moderate impact on the environment, no long-term or irreversible damage. May incur cautionary notice or infringement notice.	Significant complaints. Some adverse publicity.	Breaches resulting in sanctions, fines and referrals for further investigation.	A significant event can be managed under normal circumstances.
Major	$500K to $1M	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.	Major disruption to work routines and practices. Additional resources may be required. Significant number of serious injuries requiring hospitalisation and long-term treatment. Small number of fatalities.	Major, long-term disruption to services. Serious breach of legal/contractual obligations.	Severe impact requiring remedial action and review of processes to prevent re-occurrence. Penalties and/or direction or compliance order incurred.	Adverse publicity in regional/national media. Embarrassment to the organisation.	Significant fines and sanctions resulting in operating restrictions and disruptions.	A critical event that with appropriate management can be overcome.
Catastrophic	$1M+	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 disruption to work practices and routines. Impact on well-being of personnel. Extensive life-threatening impact, potentially large numbers of serious injuries and fatalities.	Long-term/irreversible impact on ability to deliver client services.	Long-term large scale damage to habitat or environment. Serious/repeated breach of legislation/licence conditions. Cancellation of licence and/or prosecution.	Widespread, ongoing national and possibly international media attention. Severe embarrassment to the organisation. Viability of the organisation in its current form is questionable.	Intervention and extended sanctions causing extended disruption/loss of control over operations.	A critical event or disaster that could lead to the collapse of the business.

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, Medium, High and Extreme.**

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

Risk Assessment Matrix

Likelihood	**Consequence**				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost certain	**M**	**H**	**H**	**E**	**E**
Likely	**M**	**M**	**H**	**H**	**E**
Possible	**L**	**M**	**H**	**H**	**H**
Unlikely	**L**	**L**	**M**	**M**	**H**
Rare	**L**	**L**	**M**	**M**	**H**

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 in this Risk Evaluation stage 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.

Rating	Control Assessment	Description
5	**Excellent**	Effective treatments implemented, communicated and monitored on a regular basis to determine the level of effectiveness
4	**Good**	Well documented and implemented, but with some room for improvement. Good communication and understanding of treatments
3	**Fair**	In place, but not well implemented, documented or monitored to determine their level of relevance
2	**Marginal**	Informal and inconsistent, not well communicated, implemented in an ad hoc manner.
1	**Poor**	Ineffectual measures, not communicated, sparsely implemented and of little value

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 B for a Risk Register 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 senior executive 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.

Likelihood	**Consequence**				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost certain	**1**	**5**	**2**	**1**	
Likely	**2**	**1**	**1**	**5**	
Possible	**4**	**1**			
Unlikely	**7**	**3**	**4**	**1**	**1**
Rare	**4**	**3**	**3**	**2**	**5**

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:

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 Director 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 be considered to ensure that no new risks are introduced.

The approach for treatment of risks is:

E	**Extreme risk** – Immediate action required. Task is not to be undertaken until detailed research and planning is completed and decision making in consultation with Senior Management Team.
H	**High risk** – Senior management attention and action required.
M	**Moderate risk** – Management responsibility must be specified and action required as soon as possible.
L	**Low risk** – Manage by routine procedures and unlikely to require additional resource.

Escalation Plan

We will introduce procedures 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 Kowanyama Aboriginal 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 C

Risk Management Action Plan Template

Risk ID No	**Description**	**Risk Event** *What might happen?*	**Source of Risk** *How might the risk arise?*	**Risk Treatment** *What can be done to avoid the risk, control, transfer or finance the risk?*	**Resources Required** *What physical, human or financial resources required*	**Performance Measure** *How will you know the risk treatment is working?*	**Timeline**	**Responsibility** *Name and position*

Reviewing Officer:_____ Date:_____

Comments:_____