ENTERPRISE RISK MANAGEMENT FRAMEWORK

1. STRATEGIC OBJECTIVE

Enterprise Risk Management practices and procedures are integrated into the Whitsunday Regional Council's strategic, operational and project planning processes and in day to day business practices.

2. POLICY STATEMENT

The Whitsunday Regional Council recognises that risk management is an integral part of good governance and management practice.

The Council endorses the Enterprise Risk Management (ERM) model, which aligns established risk management principles and processes with the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture. The ERM approach requires that:

- Risk management is performed consistently throughout the whole organisation
- Risks are assessed and managed in a context that is relevant to each part of the organisation

The Council's ERM Policy, Framework and Processes are aligned to the current Risk Standard, AS/NZS ISO 31000:2009. Refer to Appendix 1 for commonly used risk management terms and their definitions.

All levels of staff have a role to play in adopting risk management awareness and integrating risk management activities within their business unit environments.

The ERM approach will be inclusive of the following organisational risk areas:

- Strategic – associated with the high level longer term goals, objectives and strategies
- Operational – associated with business functions / operations
- Compliance – associated with regulatory and compliance risks
- Project – associated with defined, significant Council projects

In implementing this Policy the Whitsunday Regional Council will actively:

- identify and prioritise strategic, operational, compliance and major project risks and opportunities using the risk management process;
- ensure risk management becomes part of day to day management and processes;
- provide staff with the procedures necessary to manage risks;
- ensure staff are aware of risks and how to identify, assess and control them; and
- compile and monitor a register of strategic and operational risks in order to achieve continuous improvement in Enterprise Risk Management

The CEO is responsible for the implementation, monitoring and review of the Enterprise Risk Management Framework.

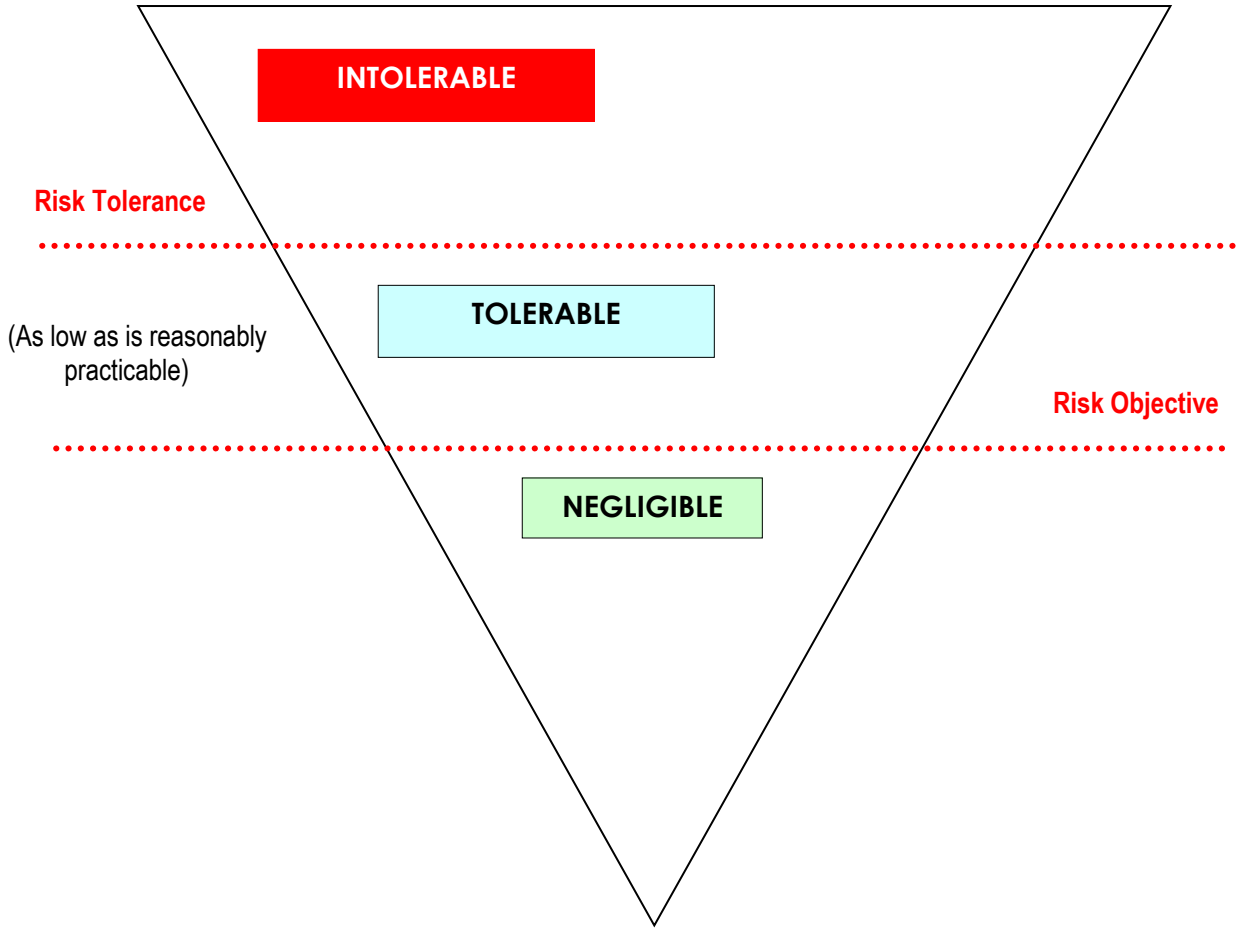
The Policy will be reviewed by the Council on an annual basis.

3. RISK APPETITE

Risk appetite is the amount of risk the organisation is prepared to accept (pursue, retain or take) in the pursuit of achieving its objectives.

Risk appetite has two principle components:

- Risk Tolerance: How much risk can the organisation choose to accept?
- Risk Capacity: How much risk can the organisation afford to take?



As a public authority the Council has a relatively conservative appetite for risk. In particular the Council has **no appetite** for risks which will:

a) Have a significant negative impact on Council's long term financial sustainability
b) Result in major breaches of legislative requirements and/or significant successful legal claims against the Council
c) Compromise the safety and welfare of staff, contractors and/or members of the community
d) Cause significant and irreparable damage to the environment
e) Result in major disruption to the delivery of key Council services
f) Result in widespread and sustained damage to the Council's reputation
g) Result in significant loss of key assets and infrastructure.

The Council has **some appetite** for risks associated with:

a) Improving efficiency, reducing costs and/or generating additional sources of income
b) Maintaining and where necessary improving levels of service to the community.

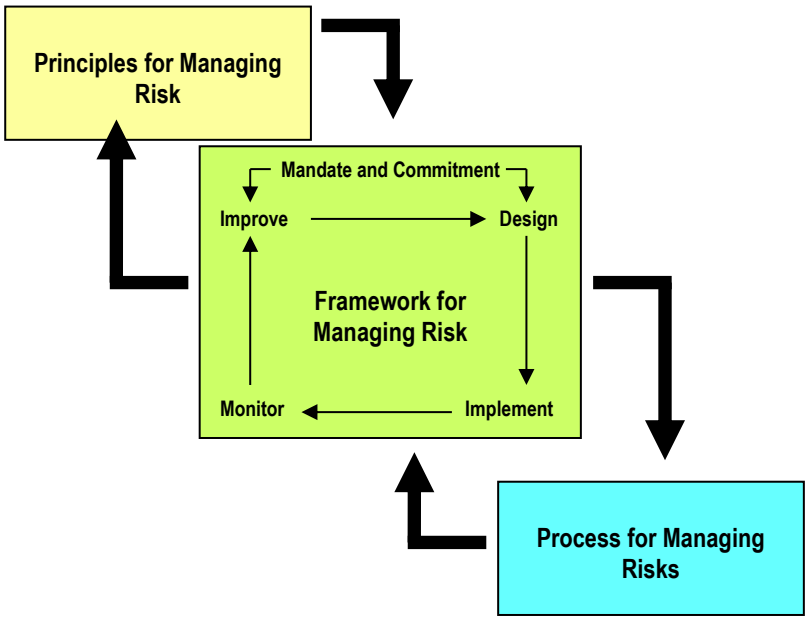
Council's risk tolerance and capacity will be assessed on a case by case basis.

4. ENTERPRISE RISK MANAGEMENT MODEL

The ERM model outlined in the Risk Standard, AS/NZS ISO 31000:2009, is comprised of three key components:

1. **Principles for Managing Risk –** the Standard establishes a number of principles that need to be satisfied before risk management will be effective.
2. **Framework for Managing Risk –** the Standard recommends that organisations should have a framework that integrates the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture.
3. **Process for Managing Risks –** an effective process that can be applied across an entire organisation, to its many areas and levels, as well to specific functions, projects and activities.

The inter-relationship between the three components is illustrated in the diagram below, and in more detail in Appendix 2.



5.1 Principles for Managing Risk

The AS/NZS ISO 31000:2009 Risk Standard Guidelines, recommends the application of the following principles (at all levels) for risk management to be effective.

A. Creates and Protects Value

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product/service quality, project management, efficiently and operations, governance and reputation.

B. Integral Part of all Organisational Processes

Risk Management is not a stand-alone activity that is separate from the main activities and processes of the organisation. Risk management is part of the responsibilities of management and an integral part of all organisational processes, including strategic planning and all project and change management processes.

C. Part of Decision Making

Risk Management helps decision makers make informed choices, prioritise actions and distinguish among alternative courses of action.

D. Explicitly Addresses Uncertainty

Risk Management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

E. Systemic, Structured and Timely

A systematic, timely and structured approach to Risk Management contributes to efficiency and to consistent, comparable and reliable results.

F. Based on the Best Available Information

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgment. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

G. Tailored

Risk Management is aligned with the organisation's external and internal context and risk profile.

H. Takes Human and Cultural Factors into Account

Risk Management recognises the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organisation's objectives.

I. Transparent and Inclusive

Appropriate and timely involvement of stakeholders, and in particular, decision makers at all levels of the organisation, ensures that Risk Management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

J. Dynamic, Iterative and Responsive to Change

As external and internal events occur, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear. Therefore, risk management continually senses and responds to change.

K. Facilitates Continual Improvement of the Organisation

Organisations should develop and implement strategies to improve their risk management maturity alongside other aspects of their organisation.

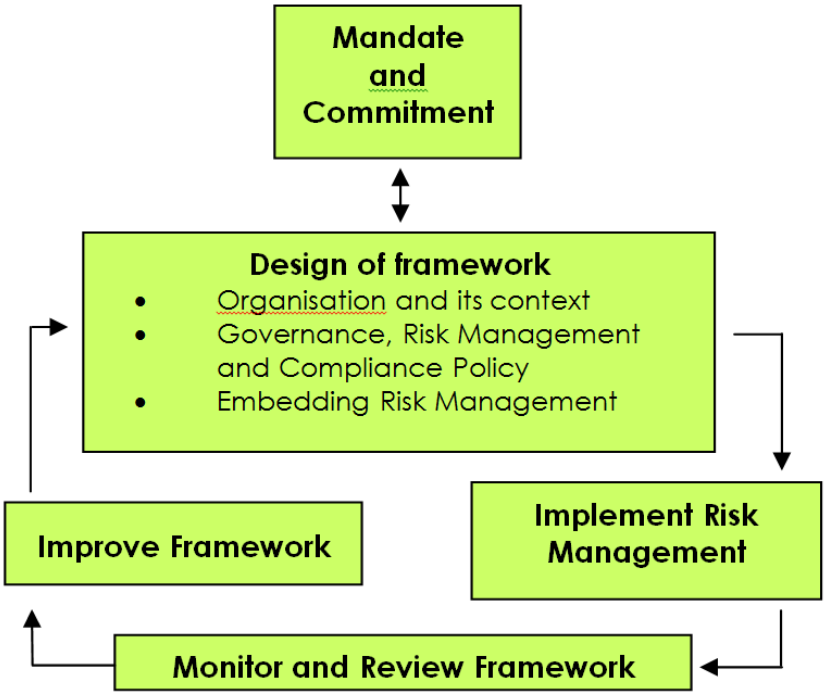
5.2 Framework for Managing Risk

Through Council's Risk Management Policy (mandate) and demonstrated executive and councillor commitment, the Risk Management Framework supports risk management practice, reporting, responsibilities and accountabilities at all management levels.

The success of the Risk Management Framework also depends on the effectiveness of the foundations and processes that embed it throughout the organisation.

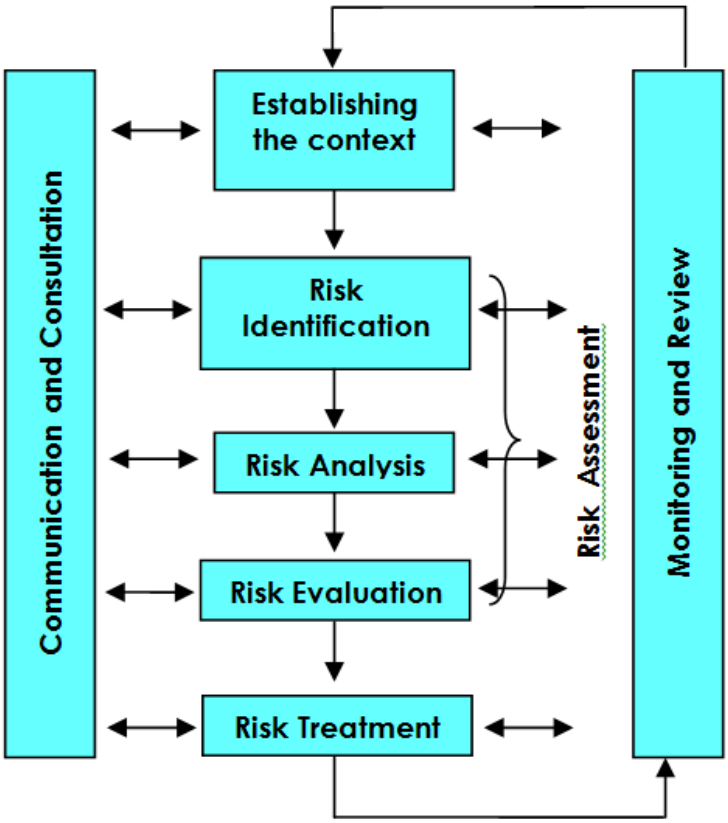
The Framework provides a conceptual structure for communicating risk information, promoting greater awareness and improved co-ordination of risk management processes.

It also identifies how risk management will be monitored and reported.



5.3 Process for Managing Risks

The Council's risk management process follows the Australian/New Zealand Standard – Risk Management AS/NZS ISO 31000:2009, seven-step process, as outlined in the diagram below.



This process provides a structured approach to managing, strategic, operational, compliance and project risks across business units and organisation levels.

Each of these steps are described in more detail in the following sections.

5.3.1 Establishing the context

The context in which the Council assesses risk should be established prior to commencing a risk assessment.

Establishing the context requires an examination of the organisation's external and internal environments, in which the risk identification, analysis and treatment options will be considered. This assists in establishing the assessment criteria for risk and the structure of the analysis.

5.3.2 Risk Identification

The next step in the risk management process is to carry out a risk identification review and document the risks to be managed. Where risks have previously been identified, this step will serve to confirm the completeness of these risks; having particular regard to changes in the business or operating environment.

Identification should include all risks which impact the achievement of the Council's objectives, whether or not they are under the Council's control.

To assist in the risk identification process, it is useful to identify and group risks under relevant categories (refer to Appendix 3).

5.3.3. Risk Analysis

Once all relevant risks have been identified they are analysed in terms of how likely the risk event is to occur (likelihood) and the possible magnitude (consequence) of the risk event. From this analysis the level of inherent risk can be determined.

The methodology to analyse risks involves 2 steps:

1. Risks are measured against established criteria for consequence and likelihood by referring to rating scales agreed to by Council (refer Appendices 3 and 4 – Risk Likelihood and Risk Consequence Ratings). For the Council likelihood is scored from "remote" to "almost certain" and consequence is scored from "negligible" to "critical".

2. The final risk score for each risk is calculated by plotting the likelihood and consequence response scores on the Inherent Risk Rating Matrix (refer Appendix 5) to give a risk rating of Very High, High, Moderate or Low.

Extreme or High Risk Ratings

All inherent (pre-control) risks ranked as "Extreme" or "High" require detailed analysis of mitigating practices / controls to determine the residual risk rating.

Any risk assessed with an inherent risk of extreme or high will be actively managed by the CEO who will determine any delegation of aspects of the process. Where appropriate, a treatment plan will be designed to improve the residual risk status of these risks. The CEO will report to the Council as required on the status of these risks and treatments. Extreme risks will be closely monitored, with any worsening of the extreme risks being reported to the mayor immediately on identification. Any other significant change to the Council's risk exposure in these categories will be reported to the Council as soon as practicable.

Moderate or Low Risk Ratings

"Moderate" or "Low" risks will be reviewed by the person with delegated operational responsibility on an annual basis. The outcome of the review and any significant change to the Council's risk exposure of which they are aware, will be reported to either the relevant Director or CEO.

5.3.4 Risk Evaluation

The purpose of risk evaluation is to make decisions, based on outcomes of the risk analysis, about which risk treatment, whether an activity should be undertaken, and treatment priorities. Compare estimated levels of risk against the criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.

WRC Councillors acknowledge that it is not appropriate, or in the best interests of stakeholders, to eliminate all risk.

The evaluation is to consider whether the current control measures are sufficient and the risk is appropriately managed and therefore acceptable. This will often be the case for lower level risks and in such cases, it may be sufficient to simply monitor the risk to ensure any change in the risk status is identified and reacted to early.

A control can be defined as an existing process, policy, device, practice or other action that acts to minimize negative risk or enhance positive opportunities.

Business improvement opportunities should be identified and prioritised when undertaking an analysis of a risk. Accordingly, a high priority should be given to those significant business improvements, which lead to a high performance outcome for the community. A balance needs to be struck between the costs to implement business improvement opportunities and the benefits to be gained.

Effectiveness of Controls

WRC assesses the effectiveness of the controls it has in place using an effectiveness rating. The Council has determined the residual risk levels (ie risk remaining after the effectiveness of the controls has been considered), based on its risk matrix and formulated the following grid:

Effectiveness of Controls	Descriptor
Extremely effective	Risk is eliminated or transferred
Very effective	Risk is reduced or transferred to a level where it is unlikely to need specific allocation of resources
Effective	Risk is reduced to a level that is acceptable with designated monitoring and reporting implemented
Limited effectiveness	All available and commercially acceptable controls have been implemented but significant risks remain
Ineffective	Risk is not able to be mitigated

5.3.5 Treat Risks

If the current control measures are not sufficient, additional risk treatments are to be identified and considered. Treatments are to be designed to either reduce the likelihood of the risk occurring or to reduce the consequences of the risk were it to occur. Ensure the proposed treatment(s) will reduce the risk level to an acceptable level, i.e. moderate or low.

If, even with proposed additional treatments, it is assessed the risk level will remain at an unacceptable level, serious consideration is to be given as to whether the activity that will create the risk is to be commenced, or continued if already in progress.

A further important consideration is considering risk treatments is the balancing of cost associated with the treatment against the benefit derived from it. In general, the cost incurred in managing risks, need to be commensurate with the benefits gained. Also, consider how risk avoidance regarding one activity can affect the significance of risk in other activities and the total risk profile.

On completion of the risk assessment process, risk treatment action plans will be prepared where additional risk controls are deemed necessary for effective management of the risk exposure. The person with operational delegation will be responsible for ensuring that the plan is prepared and implemented, will monitor progress and will provide summary reporting on the risk, as required.

When determining the most appropriate treatment options, all risks need to be considered and their priority levels compared to each other. The resources available to treat these risks also need to be determined. The aim is to effectively identify and prioritise risks and to treat risks according to their priority in the most effective manner with the resources available. A further consideration is the balancing of cost associated with the control against the benefit derived from it. In general, the cost incurred in managing risk needs to be commensurate with the benefits gained.

Risk Treatment Options

The following risk treatment options will be considered:

1 **Avoid the Risk**
- Do not proceed with the activity likely to generate the risk.

2 **Reduce the likelihood of the occurrence**
- Documented policies and procedures
- Structured training and induction programs
- Effective supervision processes
- Effective monitoring, review, audit and compliance procedures.

3 **Reduce the consequences of the occurrence**
- Appropriate qualifications
- Documented emergency/incident management procedures

4 **Transfer the Risk**
- Outsource the activity to a third party
- Seek legal or other external advice
- Insurance

5 **Accept or Retain the Risk**
- Following cost/benefit analysis.

5.3.6 Monitoring and Review

Auditors are active in monitoring the effectiveness of the controls to ensure that this residual risk remains within prudent limits.

Inherent risks identified as 'high or 'extreme' are considered as material risks and therefore are managed more stringently. Frequency of reporting to the CEO on the continuing effectiveness of the controls in place, will be determined by the CEO on a case by case basis. High risks will be monitored by the CEO and ELT. Extreme risks will be managed by the CEO on an ongoing basis and will be monitored closely by the Council. Any worsening of the risk is to be immediately reported to the Council.

Risk Register

The Risk Register sets out the identified risks (including the material risks), impact, risk assessment, existing controls, residual risk, proposed treatment and responsible manager. Risks identified as inherently 'low' or 'medium' are considered acceptable. However, these risks will be managed and monitored regularly to ensure they remain acceptable to the changing environment and WRC.

Council will develop and maintain the register through the CAMMS Integrated Risk Manager software, which combines all of the risks identified at the strategic, operational and project levels.

5.3.7 Communication and Consultation

Communication and consultation are an important element during each step of the risk management process. Effective communication is essential to ensure that those responsible for implementing risk management, and those with a vested interest (stakeholders), understand the basis on which risk management decisions are made and why particular actions are required.

It is important that a communication approach recognises the need to promote risk management concepts across a broad spectrum of management and staff, from the Executive Management Team to operational staff, and to staff from a range of locations and business areas.

WRC has used a consultative process involving staff, Directors, and Councillors to identify its material risks and to undertake appropriate risk assessments.

The CEO and Directors have responsibility for communicating and consulting with their staff to ensure risks are identified, appropriate controls are in place and any necessary treatments are addressed in relation to the operational activities of Council.

The CEO and the Directors shall report, on their respective delegated area of responsibility, as required by the CEO, but additionally at any other time when there is a significant change in the Council's risk exposure. The reports will provide details on:

- The status of risks and risk treatments with an inherent risk rating of high or extreme in the risk register; and
- Any additional action required.

5. ROLES AND RESPONSIBILTIES

Council

The Council is responsible for the implementation, monitoring and review of the Risk Management Policy and the Enterprise Risk Management Framework.

The Risk Management Policy will be reviewed on an annual basis. The annual review will occur each April in conjunction with the scheduled preparation of the Annual Budget and Operational Plan.

Executive Team

The CEO and Directors have responsibility for communicating and consulting with their staff to ensure risks are identified, appropriate controls are in place and any necessary treatments are addressed in relation to the operational activities of Council.

The CEO is responsible for promoting and supporting risk management as a core business process at the strategic and operational levels of the organisation and to be accountable to the Council for strategic risk management and reporting.

The Executive Management Team promote and support the implementation of the risk management policy, framework and process at all levels, and ensure the implementation, promotion, review and maintenance of this policy.

Management and Staff

Management and staff are responsible for ensuring that the principles and processes of the framework are integrated into their work practices so that all high and extreme risks are identified, assessed, treated, managed and monitored in accordance with the framework.

Each organisational unit is responsible for the ongoing monitoring of their risks in accordance with the Framework and Risk Register.

6. TRAINING

To ensure the successful implementation of risk management throughout Council, appropriate training in risk management will be provided to management and employees.

Training content encompasses the Risk Standard, AS/NZS ISO 31000:2009 including the Enterprise Risk Management model, Council's ERM Policy, Framework and Process.

Training on the use of CAMMS Integrated Risk Manager software will be provided to managers and relevant employees.

Council's Human Resources team will ensure:

- All new employees receive through the induction process, instructions on Risk Management and Code of Conduct.
- All employees receive regular risk management awareness training (at minimum every 3 years).

7. RELATED DOCUMENTATION

Standard Number	Standard Title
AS/NZS ISO 31000:2009	Risk Management – Principles and Guidelines
AS 8000-2003	Good Governance Principles
AS 8001-2008	Fraud and Corruption Control
AS 8002-2003	Organisational Codes of Conduct
AS/NZS 5050:2010	Business continuity - Managing disruption-related risk

8. DOCUMENT REVIEW

	Date	Responsible Officer	Tracking Number
Last Review:	24th March 2016	Graham Jarvis, Director Corporate Services	
Next Review:	24th March 2017		

APPENDICES

1. Terms and Definitions

The following terms and definitions apply to this document:

Compliance:

Adhering to the requirements of laws, industry and organisational standards and codes, principles of good governance and accepted community and ethical standards

Consequence:

Outcome or impact of an event.

Control:

An existing process, policy, device or practice that acts to minimise the adverse affects of risk or enhance positive opportunities.

Control Assessment:

Systematic review of processes to ensure that controls are still effective and appropriate.

Risk Assessment:

Is the process of identifying, analyzing and evaluating risk.

Enterprise Risk Management:

The process of planning, organising, leading and controlling the activities of the organisation in order to minimise the adverse effects of risk. The process includes all risks including financial, strategic and operational.

Frequency:

A measure of the number of occurrrences per unit of time.

Hazard:

A source of potential harm or a situation with a potential to cause loss.

Inherent risk:

The initial level of risk that exists before risk treatment measures have been taken.

Likelihood:

A qualitative description of probability or frequency.

Loss:

Any negative consequence or adverse effect, financial or otherwise.

Residual risk:

The remaining level of risk after risk treatment measures have been taken.

Risk:

Effect of uncertainty on objectives. The level of risk is the combination of the likelihood of a risk occuring and the consequences if it does occur.

Risk analysis:

A systematic process to understand the nature of and to determine the level of risk.

Risk Appetite:

Amount and type of risk that an organisation is prepared to persue, retain or take

Risk Assessment:

Is the process of identifying, analyzing and evaluating risk.

Risk Attitude:

The organisation's approach to assess and eventually pursue, retain, take or turn away from risk.

Risk Criteria:

Terms of reference by which significance of risk is assessed.

Risk evaluation:

Process of comparing the level of risk agaiinst the risk criteria.

Risk identification:

The process of determining what, where, when,why and how something could happen.

Risk Management:

The culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.

Risk Management Framework:

Set of elements of an organisations management system concerned with managing risk.

Risk Management Process:

The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk reduction:

Actions taken to lessen the likelihood, negative consequence, or both, associated with a risk.

Risk retention:

Acceptance of the burden of loss, or benefit of gain from a particular risk.

Risk transfer:

Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

Risk treatment:

Process of selection and implementation of measures to modify risk.

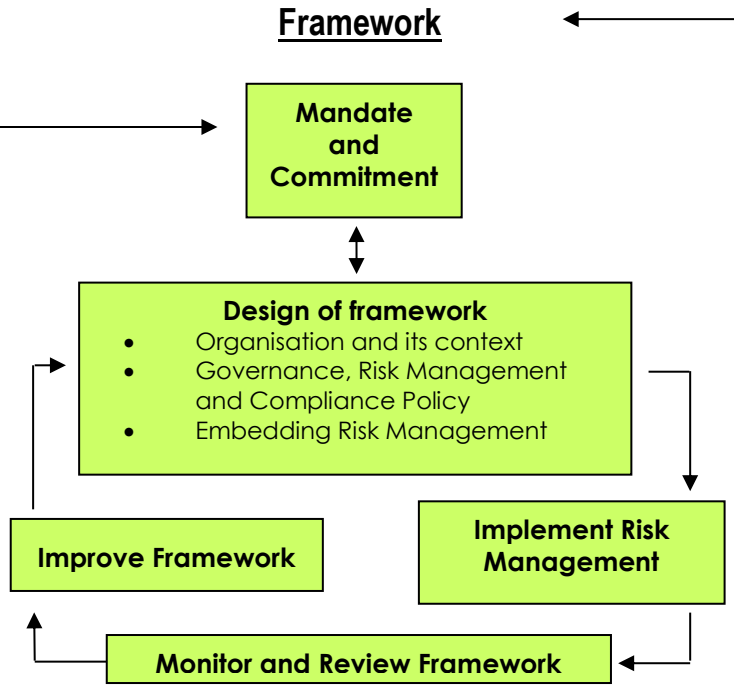
Stakeholders:

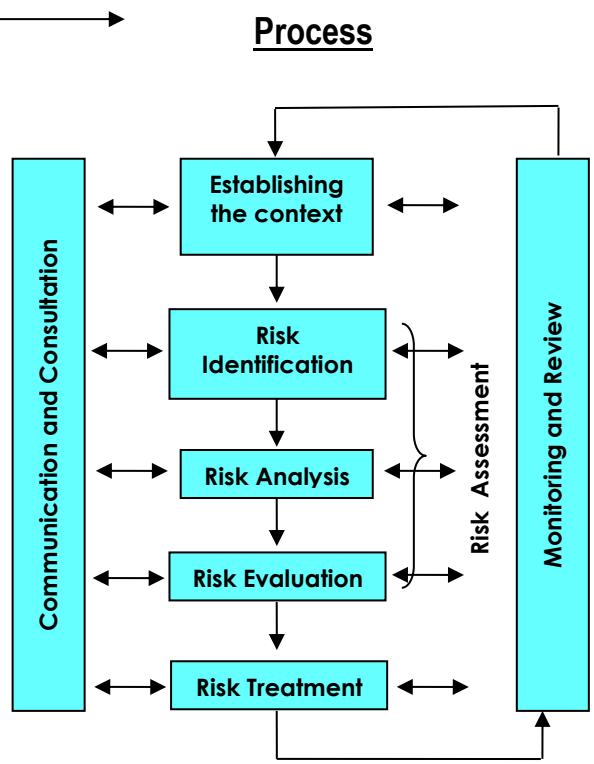
Those people or organisations who may affect, be affected by, or perceive themselves to be affected by, a decision, activity or risk.

2. Enterprise Risk Management Model

Principles for managing risk

1) Creates and protects value
2) Integral part of all organisational processes
3) Part of decision making
4) Explicitly addresses uncertainty
5) Systematic, structured and timely
6) Based on the best available information
7) Tailored
8) Takes human and cultural factors into account
9) Transparent and inclusive
10) Dynamic, iterative and responsive to change
11) Facilitates continual improvement of the organisation.





3. Risk Likelihood Rating

The likelihood rating refers to the potential for the risk to happen, for example its probability or frequency. The likelihood that an event will occur is not always easy to assess. Subjective biases may give rise to different assessments by different people. To avoid this situation, and in order to provide a degree of consistency across the organisation in assessing likelihood, the following table is to be used as a guide.

Rating Name	Rating Description
Almost Certain	Is expected to occur in most circumstances
Likely	Probably occur in most circumstances
Possible	Might occur at some time in the future
Unlikely	Could occur at some time but it considered unlikely to occur at any time in the future
Remote	May occur only in exceptional circumstances

4. Risk Consequence Rating

The consequences, i.e., the outcome or impact of an event, are to be determined against the relevant category of criteria for a consistent approach to determine a level.

Name	Description
Insignificant	Effect is minimal
Minor	Event requires minor levels of resource and input for easy remediation
Moderate	Some objectives affected
Major	Some important objectives affected or cannot be achieved
Catastrophic	Disaster with potential to lead to collapse or having a profound effect

5. Risk Rating Matrix

The overall risk rating is determined by finding the point of intersection between the likelihood rating (vertical axis) and the consequence rating (horizontal axis).

		Consequence				
		Level 1 Insignificant	Level 2 Minor	Level 3 Moderate	Level 4 Major	Level 5 Catastrophic
Likelihood	Almost Certain	**Moderate**	**Moderate**	**High**	**Extreme**	**Extreme**
	Likely	**Low**	**Moderate**	**High**	**High**	**Extreme**
	Possible	**Low**	**Low**	**Moderate**	**High**	**Extreme**
	Unlikely	**Low**	**Low**	**Low**	**High**	**High**
	Remote	**Low**	**Low**	**Low**	**Moderate**	**High**

6. Risk Consequence Matrix

		Consequences				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Risk Category	**Health and Safety**	Staff issue causing negligible impact. Injuries requiring first aid or incidence of non-treatment injuries	General morale and attitude problems. Injury involving lost time in the workplace.	Widespread staff issues cause failure to deliver several minor strategic objectives and recoverable failure of day to day service. Hospital admission for 1-2 days.	Staff issues cause widespread failure to deliver essential services. Temporary disability or hospital admission for <3 days	Death or permanent disability or long term hospital admissions
	Environmental	Minor adverse event that can be remedied immediately.	Isolated instances of environmental damage requiring effort to fix in the short term	Adverse events that cause widespread damage but reversible in the short to medium term. May incur cautionary notice of infringement notice.	Significant adverse event causing widespread damage which may be reversed through appropriate remedial action in the medium term. Penalties may apply.	Major adverse environmental event requiring continual long term remedial action. Significant penalties may apply.
	Financial	Financial impact (expenditure or revenue) <$20,000 Budget variation manageable in the short term.	Financial impact (expenditure or revenue) between $20-$250k Budget variation manageable without impact on bottom line of budget absorbed over current financial year	Financial impact (expenditure or revenue) between $250k-$500k Impact on budget beyond current financial year but manageable within next financial year	Financial impact (expenditure or revenue) between $500k-$2 million Impact on budget with recovery over proceeding two or three financial years	Financial impact (expenditure or revenue) <$2 million impact on budget with recovery over preceding three or more financial years
	Information Technology	Interruption to a service not requiring any further remedial action and with minimal impact on customers	Interruption to a service requiring further remedial action and with moderate impact on customers	Interruption to core business function or essential service with significant customer impact for up to 48 hours	Interruption to core business function or essential service for 2-7 days	Interruption to core business function or essential service greater than 7 days
	Infrastructure and Assets	Some damage where repairs are required however facility or infrastructure is still operational.	Short term loss or damage where repairs required to allow the infrastructure to remain operational using existing internal resources	Short to medium term loss of key assets and infrastructure where repairs required to allow the infrastructure to remain operational. Cost outside of budget allocation.	Widespread, short term to medium term loss of key assets and infrastructure. Where repairs required to allow the infrastructure to remain operational. Cost significant and outside of budget allocation.	Widespread, long term loss of substantial key assets and infrastructure. Where infrastructure requires total rebuild or replacement.
	Legal / Compliance	Dispute resolved through internal process or expertise.	Dispute resolved through legal advice	Corporation directed to undertake specific activities to remedy breaches in legislation that may require the involvement of legal firms.	Deliberate breach or gross negligence / formal investigations from third party (Ministerial Involvement, Ombudsman or ICAC).	Major breach of legislation resulting in major corporation penalties, fines, ICAC investigation that may result in legal action against corporation staff; or class action.
	Political	Political activity that requires minor changes in operations	Political activity that requires changes in operations	Political activity that requires changes in operations with budget and resource implications	Political activity that requires changes in operations with significant ongoing budget or resource implications	Political activity that results in irreparable damage.
	Reputation	Issue may result in a number of adverse local complaints	Issue may attract limited media coverage	Issue may attract regional and state media coverage through various mediums with minimal consequence	Issue may attract significant State and National media coverage with some effect on Council's reputation	Prolonged adverse media attention. Staff and Elected members forced to resign.
	Service Delivery	Interruption to a service not requiring any further remedial action and with minimal impact on customers	Interruption to a service requiring further remedial action and with moderate impact on customers	Interruption to core business function or essential service with significant customer impact for up to 48 hours	Interruption to core business function or essential service for 2-7 days	Interruption to core business function or essential service for more than 7 days