Shire of Broome
people • place • prosperity

Risk Management Strategy & Procedures

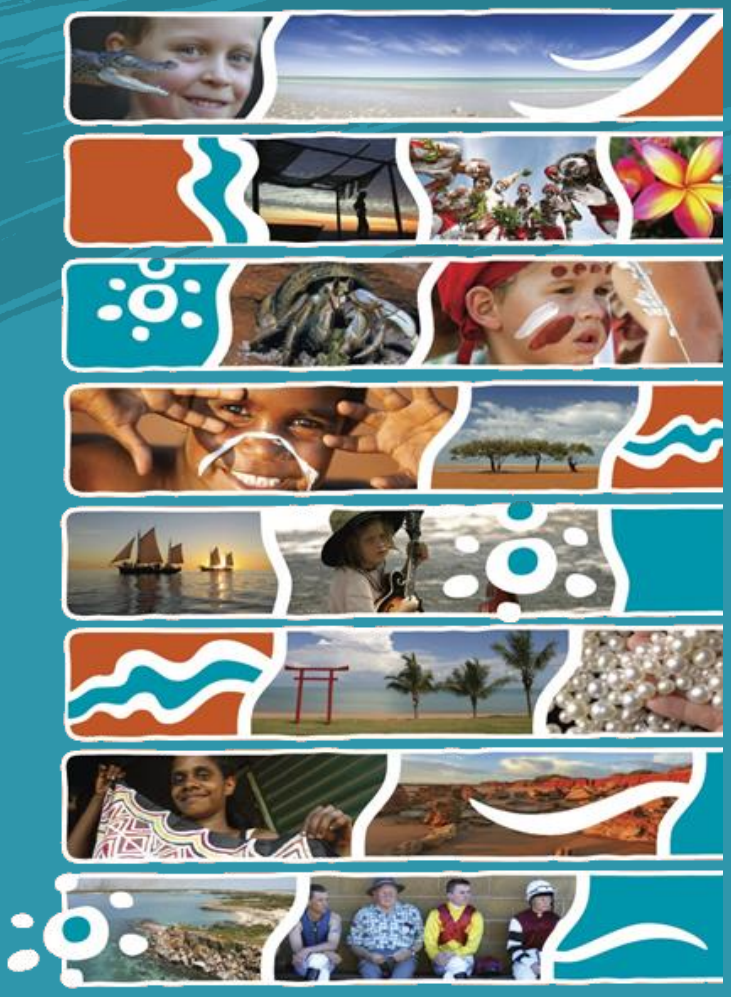


Table of Contents

Introduction

The Risk Management Strategy and Framework for the Shire of Broome ("the Shire") sets out the Shire's approach to the identification, assessment, management, reporting and monitoring of risks. All components of this document are based on Australia/New Zealand Standard ISO 31000:2009 Risk Management.

It is essential that all areas of the Shire adopt these procedures to ensure:

- Strong corporate governance; and
- Compliance with relevant legislation, regulations and internal policy and procedure; and
- Integrated planning and reporting requirements are met; and
- Uncertainty and its effects on objectives is understood.

This Strategy and Framework aims to balance a documented, structured and systematic process with the current size and complexity of the Shire along with existing time, resource and workload pressures.

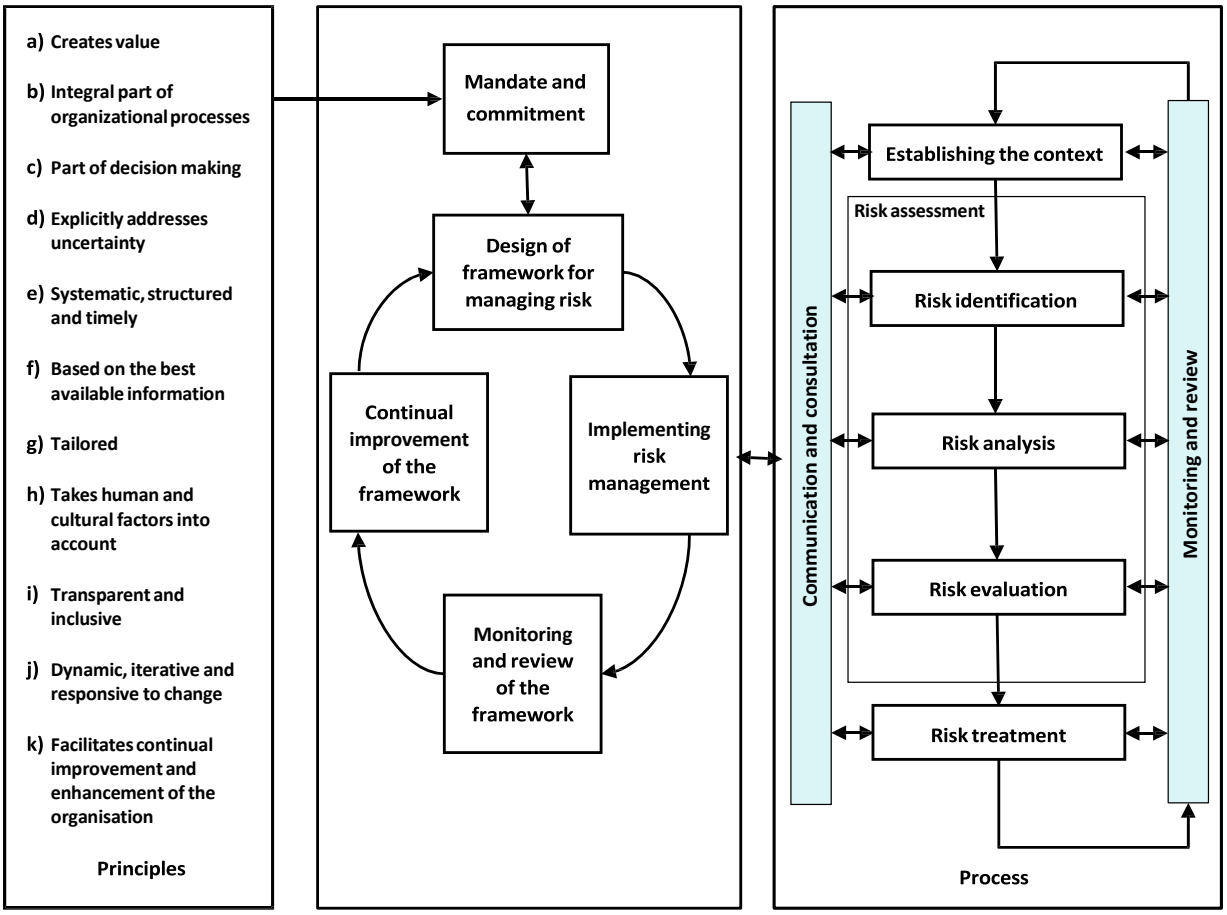


Figure 1: Risk Management Process (Source: AS/NZS 31000:2009)

Risk Management Strategy

Purpose

The Shire of Broome's ("the Shire") Risk Management Strategy and Framework documents the commitment and objectives regarding managing uncertainty that may impact the Shire's strategies, goals or objectives through appropriate decision making and mitigation of potential and inherent risk.

Statement

It is the Shire's Risk Management framework is specific to the Shire of Broome business and organisational context and aligned to the principles outlined in the international risk management standards of AS/NZS ISO 31000:2009. The best practice standards are reflected to assist in the management of all risks that may affect the Shire, its customers, people, assets, functions, objectives, operations and members of the public, in so far as practicable.

A systematic Risk Management approach provides sound rationale and a logical process that leverages opportunity and reduces unacceptable and adverse risk elements. The consistent application of risk assessment and acceptance criteria will better able the organisation to measure decision making and provide sustainable outcomes to the Shire and community.

Risk Management will form part of the strategic, management, operational and project responsibilities and; where possible, be incorporated within the Shire's Integrated Planning Framework. Risk Management is therefore, the responsibility of all Shire employees to identify, evaluate and apply treatments to achieve effective and efficient outcomes.

Definitions (from AS/NZS ISO 31000:2009)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

Risk Management: Coordinated activities to direct and control an organisation with regard to risk.

Risk Management Process: Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

Risk Management Objectives

- Optimise the achievement of the Shires vision, strategies, goals and objectives.
- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Enhance risk versus return within our risk appetite.
- Embed appropriate and effective controls to mitigate risk.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhance organisational resilience.
- Identify and provide for the continuity of critical operations

Risk Appetite

The Shire defined its' risk appetite through the development and endorsement of the Shire's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Procedures, and; are subject to ongoing review in conjunction with this strategy and framework.

All organisational risks to be reported at a corporate level are to be assessed according to the Shire's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisation's appetite and are to be noted within the individual risk assessment and approved by a member of the Executive Management Group.

Roles, Responsibilities & Accountabilities

The CEO is responsible for the allocation of roles, responsibilities and accountabilities.

The Shire's Executive Management Group will determine and communicate the Risk Management objectives and Directorate procedures, as well as direct and monitor implementation, practice and performance.

The Risk Technical Advisory Group is responsible to communicate maintain the appropriateness and effectiveness of the Shire of Broome's systems and procedures in relation to risk management, legislative compliance and internal controls.

Every employee inclusive of Councillors, volunteers and contractors within the Shire is recognised as having a role in risk management, from the identification of risks, to implementing risk treatments and shall be invited and encouraged to participate in the process.

Consultants may be retained at times to advise and assist in the risk management process or management of specific risks or categories of risk.

Monitor & Review

The Shire will implement and integrate a monitor and review process to report on the achievement of the Risk Management Objectives, the management of individual risks and the ongoing identification of issues and trends. This strategy and framework will be kept under review by the Shire's Executive Management Group and its employees. It will be formally reviewed by Council biennially.

Signed: …… Date: _____/_____/_____
Chief Executive Officer

Risk Management Procedures

Governance

Appropriate governance of risk management within the Shire of Broome (the "Shire") provides:

- Transparency of decision making.
- Clear identification of the roles and responsibilities of the risk management functions.
- An effective Governance Structure to support the risk framework.

Framework Review

This Risk Management framework is to be reviewed for appropriateness and effectiveness annually through the Risk Technical Advisory Group and Executive Management Group.

Procedural Operating Model

The Shire has adopted a "Three Lines of Defence" model for the management of risk. This model ensures roles; responsibilities and accountabilities for decision making are structured to demonstrate effective governance and assurance. By operating within the approved risk appetite and framework, the Council, Management and Community will have assurance that risks are managed effectively to support the delivery of the Strategic, Corporate, Operational and Project Plans.

First Line of Defence – Operations/Departments

All departments of the Shire are considered '1st Line'. They are responsible for ensuring that risks within their scope of operations are identified, assessed, managed, monitored and reported. Ultimately, they bear ownership and responsibility for losses or opportunities from the realisation of risk. Associated responsibilities include;

- Establishing and implementing appropriate processes and controls for the management of risk
- Undertaking adequate analysis (data capture) to support the decision-making process of risk.
- Prepare risk acceptance proposals where necessary, based on level of residual risk.
- Retain primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence - Management

Risk Framework Owner acts as the primary '2nd Line'. This position owns and manages the framework for risk management, drafts and implements governance procedures and provides the necessary tools and training to support the 1st line process. The Executive Management Group, in their capacity as Risk Committee, supplements the second line of defence.

Maintaining oversight on the application of the framework provides a transparent view and level of assurance to the 1st & 3rd lines on the risk and control environment. Support can be provided by additional oversight functions completed by other 1st Line Teams (where applicable). Additional responsibilities include:

- Providing independent oversight of risk matters as required.
- Monitoring and reporting on emerging risks.
- Co-ordinating the Shire's risk reporting for the CEO & Executive Management Group and the Risk Technical Advisory Group.

Third Line of Defence –Independent Assessment

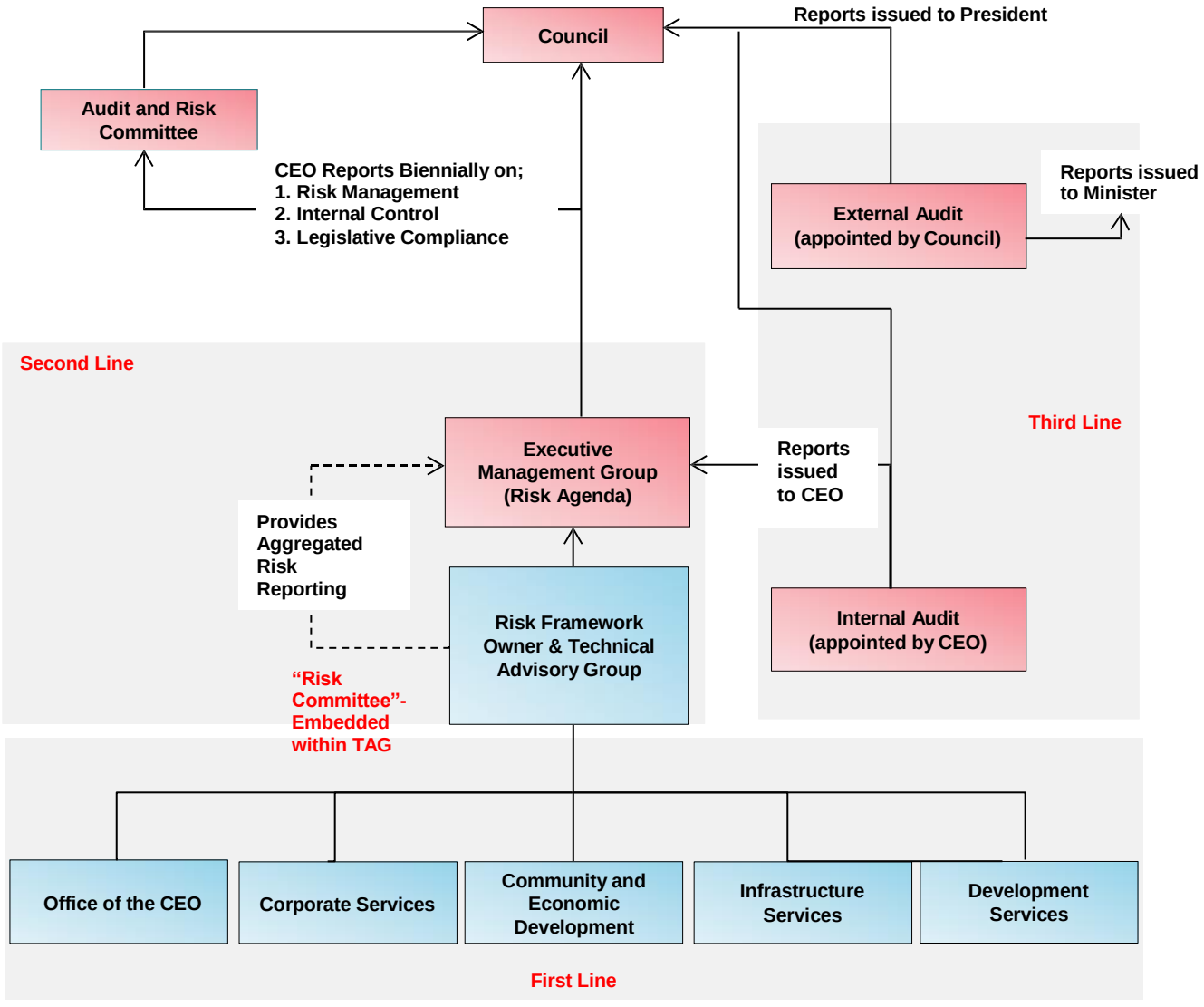
Internal self-audits & External Audits are the '3rd Line' of defence, providing assurance to the Council, Audit Committee and Shire Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit – Appointed by the CEO to report on the adequacy and effectiveness of internal control processes and procedures. The scope of which would be determined by the Executive Management Group and input from the Risk Technical Advisory Group.

External Audit – Appointed by the Council on the recommendation of the Audit Committee to report independently to the President and CEO on the annual financial statements only.

Governance Structure

The following model depicts the current operating structure for risk management within the Shire.



Roles & Responsibilities

CEO & Council

- Review and approve the Shire's Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Appoint / Engage External Auditors to report on financial statements annually.
- Establish and maintain an Audit Committee in terms of the Local Government Act.

Independent Assessment/Auditors

- Support Council in providing effective corporate governance.
- Oversight of all matters that relate to the conduct of external audits.
- Independent, objective and autonomous in deliberations.
- Recommendations to Council on external auditor appointments.

CEO / Executive Management Group

- Undertake internal audits as required under Local Government (Audit) regulations.
- Liaise with Council in relation to risk acceptance requirements.
- Approve and review the appropriateness and effectiveness of the Risk Management Strategy and Procedures.
- Drive consistent embedding of a risk management culture.
- Analyse and discuss emerging risks, issues and trends.
- Document decisions and actions arising from risk matters.
- Own and manage the Risk Profiles at Shire level.
- Determine organisational KPIs for Risk Management

Risk Framework Owner (RFO) / Risk Technical Advisory Group (TAG)

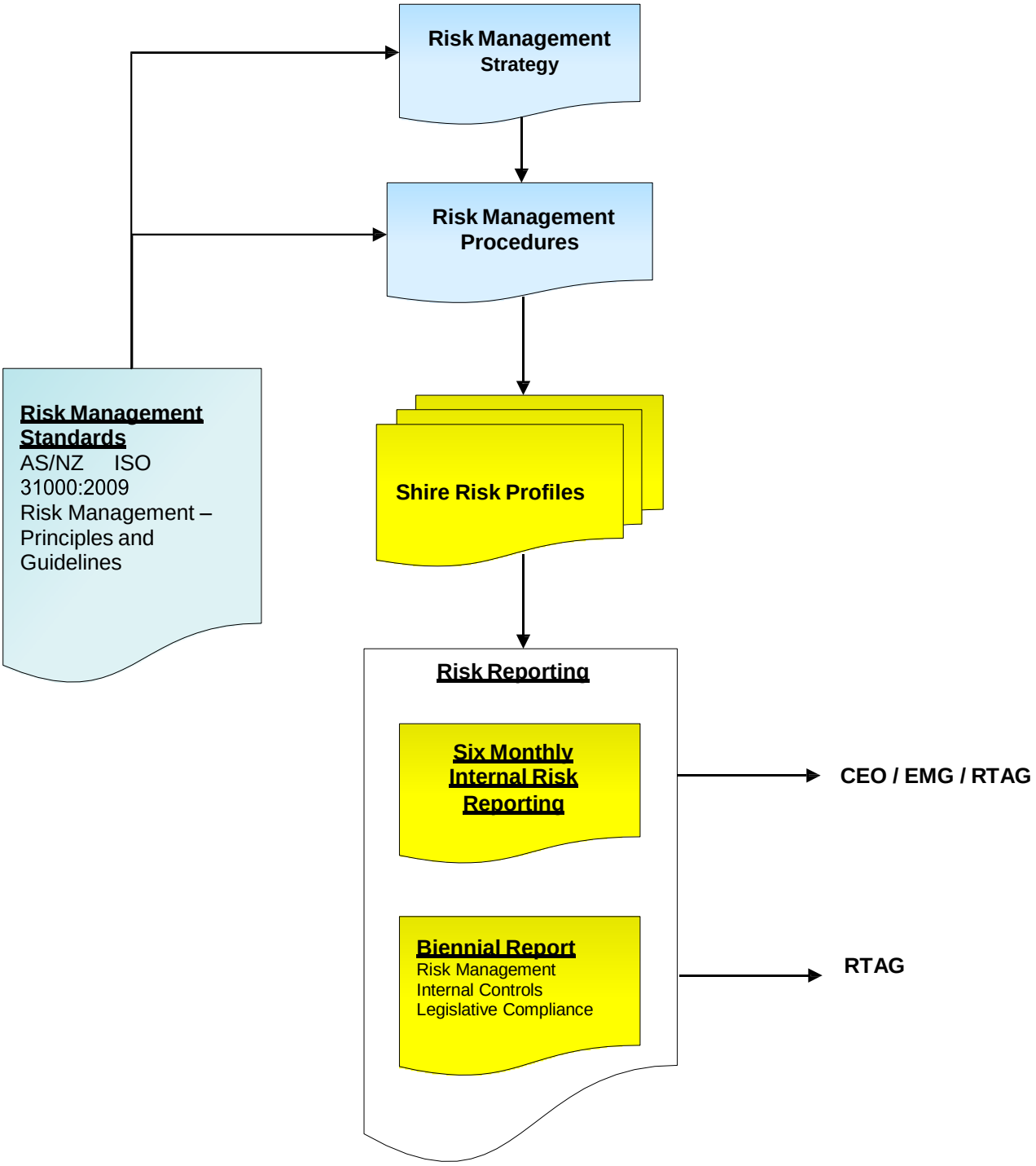
- Oversee and facilitate the Risk Management Strategy and Procedures.
- Champion risk management within operational areas.
- Support reporting requirements for Risk matters.
- Monitor and update Risk Profiles and KPI's for risk.

Operations/Departmental

- Drive risk management culture within work areas.
- Own, manage and report on specific risk issues as required.
- Assist in the Risk & Control Management process as required.
- Highlight any emerging risks or issues accordingly.
- Incorporate 'Risk Management' into Management Meetings, by incorporating the following agenda items; New or emerging risks, review existing risks, control adequacy, Outstanding issues and actions.

Document Structure (Framework)

The following model depicts the relationship between the Risk Management Policy, Procedures and supporting documentation and reports.



Risk & Control Management

All Work Areas of the Shire are required to assess and manage the Risk Profiles on an ongoing basis.

Each Manager, in conjunction with the Responsible Officer is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Shire.
- Reviewed on at least a six monthly basis, or sooner if there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

This process is supported by the use of data inputs, workshops and ongoing business engagement.

Risk & Control Assessment

To ensure alignment with ISO 31000:2009 Risk Management principles, the following approach is to be adopted from a risk and control assessment perspective.

A: Establishing the Context

The first step in the risk management process is to understand the context within which the risks are to be assessed and what is being assessed, this forms two elements:

A.1 Organisational Context

The Shire's risk management 'Assessment and Acceptance criteria' (Appendix A) provide the basic information and guidance regarding the organisational context to conduct a risk assessment. In addition, existing risk themes are to be utilised (Appendix C) where possible to assist in the categorisation of related risks.

Any changes or additions to the risk themes must be approved by the Governance Officer and CEO.

All risk assessments are to utilise these documents to allow consistent and comparable risk information to be developed and considered within planning and decision making processes.

A.2 Specific Risk Assessment Context

To direct the identification of risks, the specific risk assessment context is to be determined prior to and used within the risk assessment process.

For risk assessment purposes the Shire has been divided into three levels of risk assessment context:

- Organisation's Vision
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Existing Strategies / Objectives / Goals

A.2.1 Strategic Context

The Strategic Context refers to the Shire's external environment and high level decision makers. Inputs to establishing the strategic risk assessment context may include;

- Organisations Vision / Mission
- Stakeholder Analysis
- Environment Scan / SWOT Analysis

- Existing Strategies / Objectives / Goals

A.2.2 Operational Context

The Shire's day to day activities, functions, infrastructure and services. Prior to identifying operational risks, the operational area should identify its Key Activities i.e. what is trying to be achieved. Note: these may already be documented in business plans, budgets etc.

A.2.3 Project Context

Project Risk has two main components:

- **Direct** refers to the risks that may arise as a result of project activity (i.e. impacting on current or future process, resources or IT systems) which may prevent the Shire from meeting its objectives
- **Indirect** refers to the risks which threaten the delivery of project outcomes.

In addition to understanding what is to be assessed, it is also important to understand who are the key stakeholders or areas of expertise that may need to be included within the risk assessment.

B: Risk Identification

Using the specific risk assessment context as the foundation, and in conjunction with relevant stakeholders, answer the following questions, capture and review the information within each Risk Profile.

- What can go wrong? / What are areas of uncertainty? (Risk Description)
- How may this risk eventuate? (Potential Causes)
- What are the current measurable activities that mitigate this risk from eventuating? (Controls)
- What are the potential consequential outcomes of the risk eventuating?

C: Risk Analysis

To analyse the risks the Shire's Risk Assessment and Acceptance Criteria (Appendix A) is applied:

- Based on the documented controls, analyse the risk in terms of Existing Control Ratings
- Determine relevant consequence categories and rate how bad it could be if the risk eventuated with existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence with existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the risk rating (Level of Risk).

D: Risk Evaluation

The Shire is to verify the risk analysis and make a risk acceptance decision based on:

- Controls Assurance (are the existing controls in use, effective, documented and relevant)
- Existing Control Rating
- Level of Risk
- Risk Acceptance Criteria (Appendix A)
- Risk versus Reward / Opportunity

The risk acceptance decision needs to be documented and acceptable risks are then subject to the monitor and review process. Note: Individual risks or issues may need to be escalated due to urgency, level of risk or systemic nature.

E: Risk Treatment

For unacceptable risks, determine treatment options that may improve existing controls and/or reduce consequence / likelihood to an acceptable level.

Risk treatments may involve actions such as avoid, share, transfer or reduce the risk with the selection and implementation to be based on;

- Cost versus benefit
- Ease of implementation
- Alignment to organisational values / objectives

Once a control has been fully implemented, the Risk Framework Owner (RFO) is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process (Refer to Risk Acceptance section).

F: Monitoring & Review

The Shire is to review all Risk Profiles at least on a six monthly basis or if triggered by one of the following;

- Changes to context,
- A treatment is implemented,
- An incident occurs or due to audit/regulator findings.

The Risk Framework Owner (RFO) is to monitor the status of risk treatment implementation and report on, if required.

The CEO & Executive Management Group will monitor significant risks and treatment implementation as part of their normal agenda item on a quarterly basis with specific attention given to risks that meet any of the following criteria:

- Risks with a Level of Risk of High or Extreme
- Risks with Inadequate Existing Control Rating
- Risks with Consequence Rating of Extreme
- Risks with Likelihood Rating of Almost Certain

The design and focus of the Risk Summary report will be determined from time to time on the direction of the CEO & Executive Management Group. They will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and appropriate to the Shire.

G: Communication & Consultation

Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process.

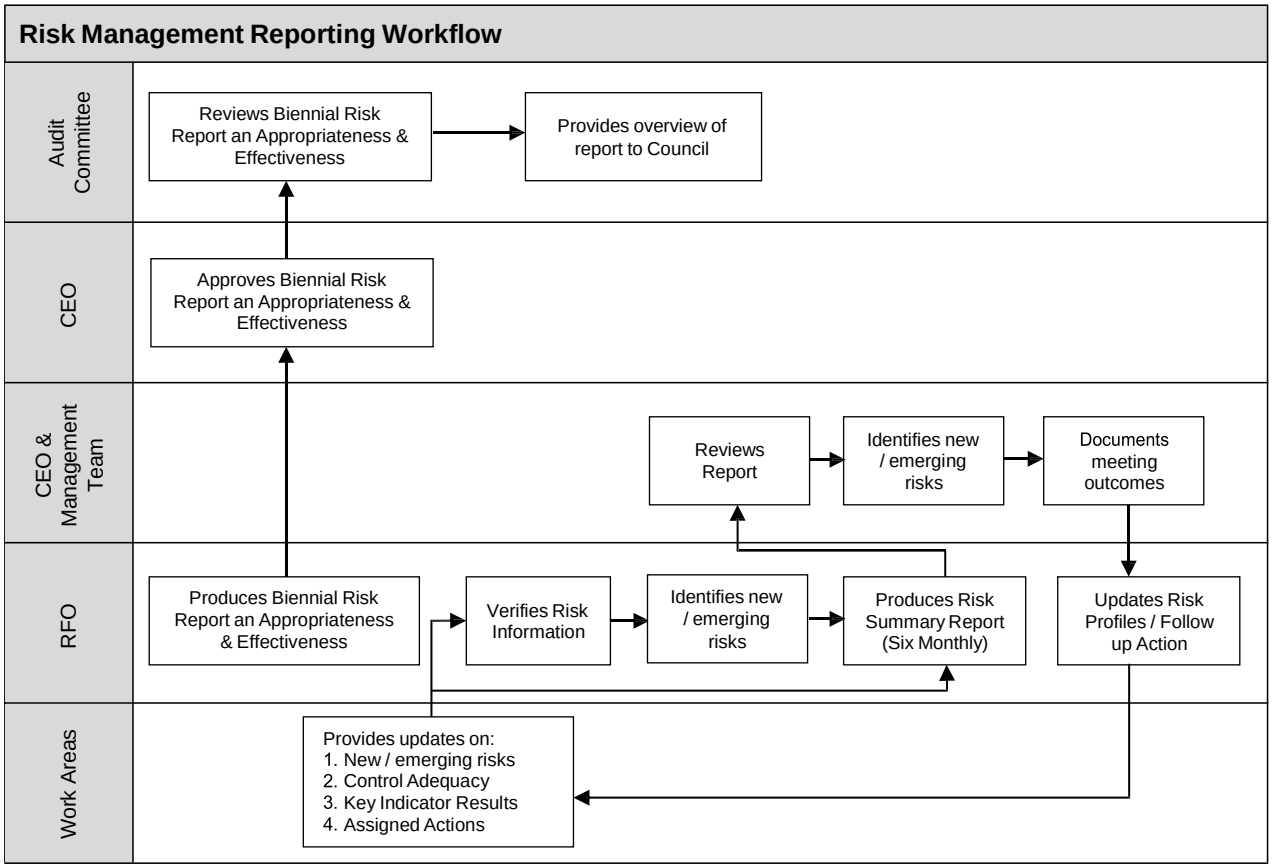
Risk management awareness and training will be provided to staff as part of their OS&H Program.

Risk management will be included within the employee induction process to ensure new employees are introduced to the Shire's risk management culture.

Reporting Requirements

Coverage & Frequency

The following diagram provides a high level view of the ongoing reporting process for Risk Management.



Each Work Area is responsible for ensuring:

- They continually provide updates in relation to new, emerging risks, control effectiveness and key indicator performance to the Responsible Officer.
- Work through assigned actions and provide relevant updates to the Responsible Officer
- Risks / Issues reported to the CEO & Executive Management Group are reflective of the current risk and control environment.

The Responsible Officer is responsible for:

- Ensuring Shire Risk Profiles are formally reviewed and updated, at least on a six monthly basis or when there has been a material restructure, change in risk ownership or change in the external environment.
- Six Monthly Risk Reporting for the CEO & Executive Management Group which contains an overview of the Risk Summary for the Shire.
- Annual Compliance Audit Return completion and lodgment.

Indicators

Indicators are required to be used for monitoring and validating risks and controls. The following describes the process for the creation and reporting of Indicators:

Identification

The following represent the minimum standards when identifying appropriate Indicator risks and controls:

- The risk description and casual factors are fully understood
- The Indicator is fully relevant to the risk or control
- Predictive Indicators are adopted wherever possible
- Indicators provide adequate coverage over monitoring risks and controls.

Validity of Source

In all cases an assessment of the data quality, integrity and frequency must be completed to ensure that the Indicator data is relevant to the risk or dontrol.

Where possible the source of the data (data owner) should be independent to the risk owner. Overlapping Indicators can be used to provide a level of assurance on data integrity.

If the data or source changes during the life of the Indicator, the data is required to be revalidated to ensure reporting of the Indicator against a consistent baseline.

Tolerances

Tolerances are set based on the Shire's risk appetite. They may be set and agreed over three levels:

- Green – within appetite; no action required.
- Amber – the Indicator must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Red – outside risk appetite; the Indicator must be escalated to the CEO & Executive Management Group where appropriate management actions are to be set and implemented to bring the measure back within appetite.

Monitor and Review

All active Indicators are updated as per their stated frequency of the data source.

When monitoring and reviewing Indicators, the overall trend should be considered over a longer timeframe than individual data movements. The trend of the Indicators is specifically used as an input to the risk and control assessment.

Risk Acceptance

Day-to-day operational management decisions are generally managed under the delegated authority framework of the Shire.

Risk acceptance outside of the appetite framework is a management decision to accept, within authority levels, material risks which will remain outside appetite framework (refer Appendix A – Risk Assessment & Acceptance Criteria) for an extended period of time (generally 3 months or longer).

The following process is designed to provide a framework for those outside appetite framework identified risks.
The 'Risk Acceptance' must be in writing, signed by the relevant Manager and cover:

- A description of the risk.
- An assessment of the risk (e.g. Impact consequence, materiality, likelihood, working assumptions etc)
- Details of any mitigating action plans or treatment options in place
- An estimate of the expected remediation date.

Reasonable action should be taken to mitigate the risk. A lack of budget to remediate a material risk outside of appetite is not sufficient justification in itself to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure (i.e. Executive Management Group).

Annual Control Assurance Plan

The annual assurance plan is a monitoring schedule prepared by the Executive Management Group that sets out the control assurance activities to be conducted over the next 12 months. This plan needs to consider the following components.

- Coverage of all risk classes (Strategic, Operational, Project)
- Existing control adequacy ratings across the Shire's Risk Profiles.
- Consider control coverage across a range of risk themes (where commonality exists).
- Building profiles around material controls to assist in design and operating effectiveness reviews.
- Consideration to significant incidents.
- Nature of operations
- Additional or existing 2nd line assurance information / reviews (e.g. HR, Financial Services, IT)
- Frequency of monitoring / checks being performed
- Review and development of Indicators
- Timetable for assurance activities
- Reporting requirements

Whilst this document and subsequent actions are owned by the CEO, input and consultation will be sought from individual Work Areas.

Appendix A – Risk Assessment and Acceptance Criteria

Shire of Broome Measures of Consequence							
Rating	**Health**	**Financial Impact**	**Service Interruption**	**Compliance**	**Reputational**	**Property**	**Environment**
Insignificant 1	Near miss / minor injuries	Less than $10,000	No material service interruption	Minor regulatory or statutory impact	Unsubstantiated, localised low impact on community / stakeholder trust, low profile or no media item	Inconsequential damage	Contained, reversible impact managed by on site response
Minor 2	First aid injuries/ Lost time injury <30 Days	$10,001 - $250,000	Short term temporary interruption – backlog cleared < 1 day	Some temporary non compliances	Substantiated, localised impact on community / stakeholder trust or low media item	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response
Moderate 3	Medical type injuries/ Lost time injury >30 Days	$250,001 - $2,000,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Short term non-compliance but with significant regulatory requirements imposed	Substantiated, public embarrassment, moderate impact on community/stakeholder trust or moderate media profile	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies
Major 4	Long-term disability / multiple injuries	$2,000,001 - $4,000,000	Prolonged interruption of services – additional resources; performance affected< 1 month	Non-compliance results in termination of services or imposed penalties	Substantiated, public embarrassment, widespread high impact on community / stakeholder trust, high media profile, third party actions	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies
Extreme 5	Fatality, permanent disability	More than $4,000,000	Indeterminate prolonged interruption of services – non-performance> 1 month	Non-compliance results in litigation, criminal charges or significant damages or penalties	Substantiated, public embarrassment, widespread loss of community/stakeholder trust, high widespread multiple media profile, third party actions	Extensive damage requiring prolonged period of restitution	Uncontained, irreversible impact

Measures of Likelihood			
Rating	***Definition***	***Frequency***	***Chance of Occurance***
Almost Certain (5)	*The event is expected to occur in most circumstances*	*More than once per year*	*> 90% chance of occurring*
Likely (4)	*The event will probably occur in most circumstances*	*At least once per year*	*60% - 90% chance of occurring*
Possible (3)	*The event should occur at some time*	*At least once in 5 years*	*40% - 60% chance of occurring*
Unlikely (2)	*The event could occur at some time*	*At least once in 10 years*	*10% - 40% chance of occurring*
Rare (1)	*The event may only occur in exceptional circumstances*	*Less than once in 15 years*	*< 10% chance of occurring*

Risk Matrix						
Consequence		**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Likelihood		**1**	**2**	**3**	**4**	**5**
Almost Certain	**5**	**Moderate (5)**	**High (10)**	**High (15)**	**Extreme (20)**	**Extreme (25)**
Likely	**4**	**Low (4)**	**Moderate (8)**	**High (12)**	**High (16)**	**Extreme (20)**
Possible	**3**	**Low (3)**	**Moderate (6)**	**Moderate (9)**	**High (12)**	**High (15)**
Unlikely	**2**	**Low (2)**	**Low (4)**	**Moderate (6)**	**Moderate (8)**	**High (10)**
Rare	**1**	**Low (1)**	**Low (2)**	**Low (3)**	**Low (4)**	**Moderate (5)**

Risk Acceptance Criteria			
Risk Rank	**Description**	**Criteria**	**Responsibility**
LOW	*Acceptable*	*Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring*	*Operational Manager*
MODERATE	*Monitor*	*Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring*	*Operational Manager*
HIGH	*Urgent Attention Required*	*Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring*	*Director*
EXTREME	*Unacceptable*	*Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring*	*CEO/Council*

Shire of Broome Existing Controls Ratings		
Rating	Foreseeable	**Description**
Effective	There is little scope for improvement.	Processes (Controls) operating as intended and / or aligned to Policies & Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested.
Adequate	There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing.
Inadequate	A need for corrective and / or improvement actions exist.	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time.

Appendix B – Risk Profile Template

Risk Theme	Date
This Risk Theme is defined as: *Definition of Theme*	

Potential causes include:
List of potential causes

Key Controls	Type	Date	Shire Rating
List of Key Controls			

Overall Control Ratings:	

Risk Ratings	Shire Rating
Consequence:	
Likelihood:	

Overall Risk Ratings:	

Key Indicators	Tolerance	Date	Overall Shire Result
List of Key Indicators			

Comments *Rationale for all above ratings*

Current Issues / Actions / Treatments	Due Date	Responsibility
List current issues / actions / treatments		

Appendix C – Risk Theme Definitions

Misconduct

Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures or delegated authority. This would include instances of:

- Relevant authorisations not obtained.
- Distributing confidential information.
- Accessing systems and / or applications without correct authority to do so.
- Misrepresenting data in reports.
- Theft by an employee
- Collusion between Internal & External parties

This does not include instances where it was not an intentional breach - refer Errors, Omissions or Delays, or Inaccurate Advice / Information.

External theft & fraud (inc. Cyber Crime)

Loss of funds, assets, data or unauthorised access, (whether attempts or successful) by external parties, through any means (including electronic), for the purposes of;

- Fraud – benefit or gain by deceit
- Malicious Damage – hacking, deleting, breaking or reducing the integrity or performance of systems
- Theft – stealing of data, assets or information (no deceit)

Examples include:

- Scam Invoices
- Cash or other valuables from 'Outstations'.

Business & community disruption

Failure to adequately prepare and respond to events that cause disruption to the local community and / or normal Shire business activities. The event may result in damage to buildings, property, plant & equipment (all assets). This could be a natural disaster, weather event, or an act carried out by an external party (inc. vandalism). This includes;

- Lack of (or inadequate) emergency response / business continuity plans.
- Lack of training to specific individuals or availability of appropriate emergency response.
- Failure in command and control functions as a result of incorrect initial assessment or untimely awareness of incident.
- Inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc

This does not include disruptions due to IT Systems or infrastructure related failures - refer "Failure of IT & communication systems and infrastructure".

Errors, omissions, incorrect advice & delays

Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process. This includes instances of;

- Human errors, incorrect or incomplete processing
- Inaccurate recording, maintenance, testing and / or reconciliation of data.
- Errors or inadequacies in model methodology, design, calculation or implementation of models.

This may result in incomplete or inaccurate information. Consequences include;

- Inaccurate data being used for management decision making and reporting.
- Delays in service to customers
- Inaccurate data provided to customers

This excludes process failures caused by inadequate / incomplete procedural documentation - refer “Inadequate Document Management Processes”.

Failure of IT &/or Communications Systems and Infrastructure

Instability, degradation of performance, or other failure of IT Systems, Infrastructure, Communication or Utility causing the inability to continue business activities and provide services to the community. This may or may not result in IT Disaster Recovery Plans being invoked. Examples include failures or disruptions caused by:

- Hardware &/or Software
- IT Network
- Failures of IT Vendors

This also includes where poor governance results in the breakdown of IT maintenance such as;

- Configuration management
- Performance Monitoring
- IT Incident, Problem Management & Disaster Recovery Processes

This does not include new system implementations - refer "Inadequate Project / Change Management".

Failure to fulfil statutory, regulatory or compliance requirements

Failure to correctly identify, interpret, assess, respond and communicate laws and regulations as a result of an inadequate compliance framework. This could result in fines, penalties, litigation or increase scrutiny from regulators or agencies. This includes, new or proposed regulatory and legislative changes, in addition to the failure to maintain updated legal documentation (internal & public domain) to reflect changes.

This does not include Occupational Safety & Health Act (refer "Inadequate safety and security practices") or any Employment Practices based legislation (refer “Ineffective Employment practices)

It does include the Local Government Act, Health Act, Building Act, Privacy Act and all other legislative based obligations for Local Government.

Inadequate project / change management

Inadequate analysis, design, delivery and / or status reporting of change initiatives, resulting in additional expenses, time requirements or scope changes. This includes:

- Inadequate Change Management Framework to manage and monitor change activities.
- Inadequate understanding of the impact of project change on the business.
- Failures in the transition of projects into standard operations.
- Failure to implement new systems
- Failures of IT Project Vendors/Contractors

Inadequate document management processes

Failure to adequately capture, store, archive, retrieve, provision and / or disposal of documentation. This includes:

- Contact lists.
- Procedural documents.
- 'Application' proposals/documents.
- Contracts.
- Forms, requests or other documents

Inadequate safety and security practices

Non-compliance with the Occupation Safety & Health Act, associated regulations and standards. It is also the inability to ensure the physical security requirements of staff, contractors and visitors. Other considerations are:

- Inadequate Policy, Frameworks, Systems and Structure to prevent the injury of visitors, staff, contractors and/or tenants.

- Inadequate Organisational Emergency Management requirements (evacuation diagrams, drills, wardens etc).
- Inadequate security protection measures in place for buildings, depots and other places of work (vehicle, community etc).
- Public Liability Claims, due to negligence or personal injury.
- Employee Liability Claims due to negligence or personal injury.
- Inadequate or unsafe modifications to plant & equipment.

Inadequate engagement practices

Failure to maintain effective working relationships with the Community (including Local Media), Stakeholders, Key Private Sector Companies, Government Agencies and / or Elected Members. This invariably includes activities where communication, feedback and / or consultation is required and where it is in the best interests to do so. For example;

- Following up on any access & inclusion issues.
- Infrastructure Projects.
- Regional or District Committee attendance.
- Local Planning initiatives.
- Strategic Planning initiatives

This does not include instances whereby Community expectations have not been met for standard service provisions such as Community Events, Library Services and / or Bus/Transport services.

Inadequate asset sustainability practices

Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet, buildings, roads, playgrounds, boat ramps and all other assets and their associated lifecycle from procurement to maintenance and ultimate disposal. Areas included in the scope are;

- Inadequate design (not fit for purpose)
- Ineffective usage (down time)
- Outputs not meeting expectations
- Inadequate maintenance activities.
- Inadequate financial management and planning.

It does not include issues with the inappropriate use of the Plant, Equipment or Machinery. Refer Misconduct.

Inadequate supplier / contract management

Inadequate management of External Suppliers, Contractors, IT Vendors or Consultants engaged for core operations. This includes issues that arise from the ongoing supply of services or failures in contract management & monitoring processes. This also includes:

- Concentration issues
- Vendor sustainability

Ineffective employment practices

Failure to effectively manage and lead human resources (full/part time, casuals, temporary and volunteers). This includes not having an effective Human Resources Framework in addition to not having appropriately qualified or experienced people in the right roles or not having sufficient staff numbers to achieve objectives. Other areas in this risk theme to consider are;

- Breaching employee regulations (excluding OH&S)
- Discrimination, Harassment & Bullying in the workplace
- Poor employee wellbeing (causing stress)
- Key person dependencies without effective succession planning in place
- Induction issues
- Terminations (including any tribunal issues)
- Industrial activity

Care should be taken when considering insufficient staff numbers as the underlying issue could be process inefficiencies.

Ineffective management of facilities / venues / events

Failure to effectively manage the day to day operations of facilities and / or venues. This includes;

- Inadequate procedures in place to manage the quality or availability.
- Ineffective signage
- Booking issues
- Financial interactions with hirers / users
- Oversight / provision of peripheral services (eg. cleaning / maintenance)

Inadequate environmental management.

Inadequate prevention, identification, enforcement and management of environmental issues. The scope includes;

- Lack of adequate planning and management of coastal erosion issues.
- Failure to identify and effectively manage contaminated sites (including groundwater usage).
- Waste facilities (landfill / transfer stations).
- Weed control.
- Ineffective management of water sources (reclaimed, potable)
- Illegal dumping.
- Illegal clearing / land use.

Inadequate management of joint managed lands / assets

Failure to understand and fulfil the Shire's duty and standard of care in the management of joint managed lands / assets;

Shire of Broome
people • place • prosperity