

Risk Management Governance Framework

- Risk Management Policy
- Risk Management Procedures

Approved by the Chief Executive Officer

August 2014

Version: 1.0

Shire of Denmark

9 September 2014 - Attachment 9.5.1

Table of Contents

- Introduction 2
- Risk Management Policy 3
 - Purpose 3
 - Policy 3
 - Definitions (from AS/NZS ISO 31000:2009) 3
 - Risk: 3
 - Risk Management: 3
 - Risk Management Process: 3
 - Risk Management Objectives 4
 - Risk Appetite 4
 - Roles, Responsibilities & Accountabilities 4
 - Monitor & Review 4
- Risk Management Procedures 5
 - Governance 5
 - Framework Review 5
 - Operating Model 5
 - Governance Structure 6
 - Roles & Responsibilities 7
 - Document Structure (Framework) 8
 - Risk & Control Management 9
 - Risk & Control Assessment 9
 - Communication & Consultation 11
 - Reporting Requirements 12
 - Coverage & Frequency 12
 - Key Indicators 13
 - Identification 13
 - Validity of Source 13
 - Tolerances 13
 - Monitor & Review 13
 - Risk Acceptance 14
 - Annual Risk Monitoring Plan 14
- Appendix A – Risk Assessment and Acceptance Criteria 15
- Appendix B – Risk Profile Template 18
- Appendix C – Risk Theme Definitions 19

Introduction

The Policy and Procedures form the Risk Management Framework for the Shire of Denmark (“the Shire”). It 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 apply these procedures to ensure:

- Strong corporate governance.
- Compliance with relevant legislation, regulations and internal policies.
- Integrated Planning and Reporting requirements are met.
- Uncertainty and its effects on objectives is understood.

This 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.

Further information or guidance on risk management procedures is available from LGIS Risk Management.

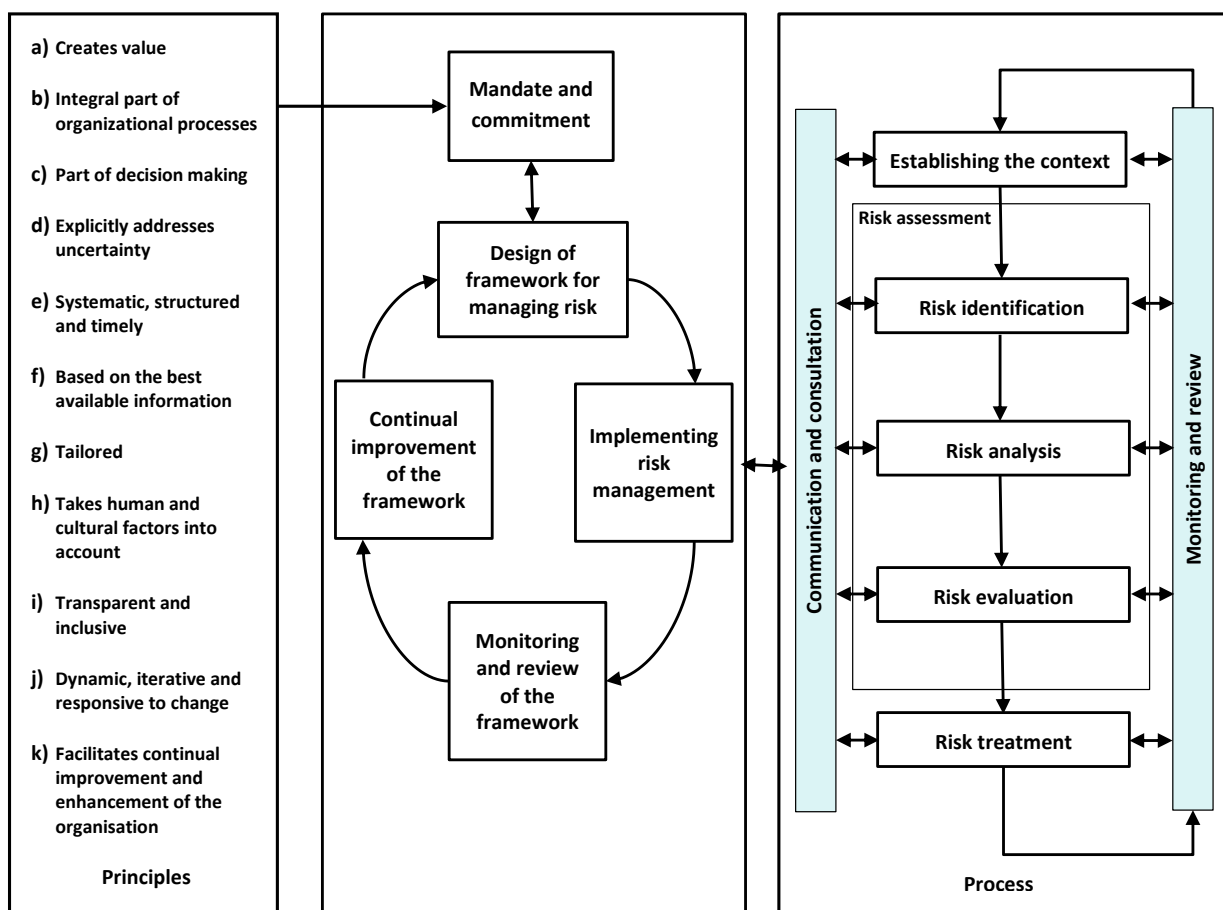


Figure 1: Risk Management Process (Source: AS/NZS 31000:2009)

Risk Management Policy

Purpose

The Shire of Denmark's ("the Shire") Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Shire's strategies, goals or objectives.

Policy

It is the Shire's Policy to achieve best practice (aligned with AS/NZS ISO 31000:2009 Risk management), in the management of all risks that may affect the Shire, its customers, people, assets, functions, objectives, operations or members of the public.

Risk Management will form part of the Strategic, Operational, Project and Line Management responsibilities and where possible, be incorporated within the Shire's Integrated Planning Framework.

The Shire's Management Team will determine and communicate the Risk Management Policy, Objectives and Procedures, as well as direct and monitor implementation, practice and performance.

Every employee 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.

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

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 our vision, mission, 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 has quantified its risk appetite through the development and endorsement of the Shire’s Risk Assessment and Acceptance Criteria (Appendix A). The criteria and Risk Management Procedures may be reviewed by the CEO from time to time in keeping with the objectives of this Policy.

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 organisations appetite and are to be noted within the individual risk assessment.

Roles, Responsibilities & Accountabilities

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures that may be amended from time to time by the CEO (Organisation Procedure Manual).

Monitor & Review

The CEO 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 policy will be reviewed by the Council as required.

Date of Adoption:

Date of Review:

Risk Management Procedures

Governance

Appropriate governance of risk management within the Shire of Denmark (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

The Risk Management Framework is to be reviewed for appropriateness and effectiveness by the Chief Executive Officer in conjunction with the Management Team as required.

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 Plans.

First Line of Defence

All operational areas 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 (in line with these procedures).
- Undertaking adequate analysis (data capture) to support the decision-making process of risk.
- Preparing risk acceptance proposals where necessary, based on level of residual risk.
- Retaining primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence

The Human Resources / Risk Management Officer acts as the primary ‘2nd Line’. This position, in liaison with the CEO, manages the framework for risk management, drafts and implements governance procedures and provides the necessary tools and training to support the 1st line process.

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 & Management Team and the Audit Committee.

Third Line of Defence

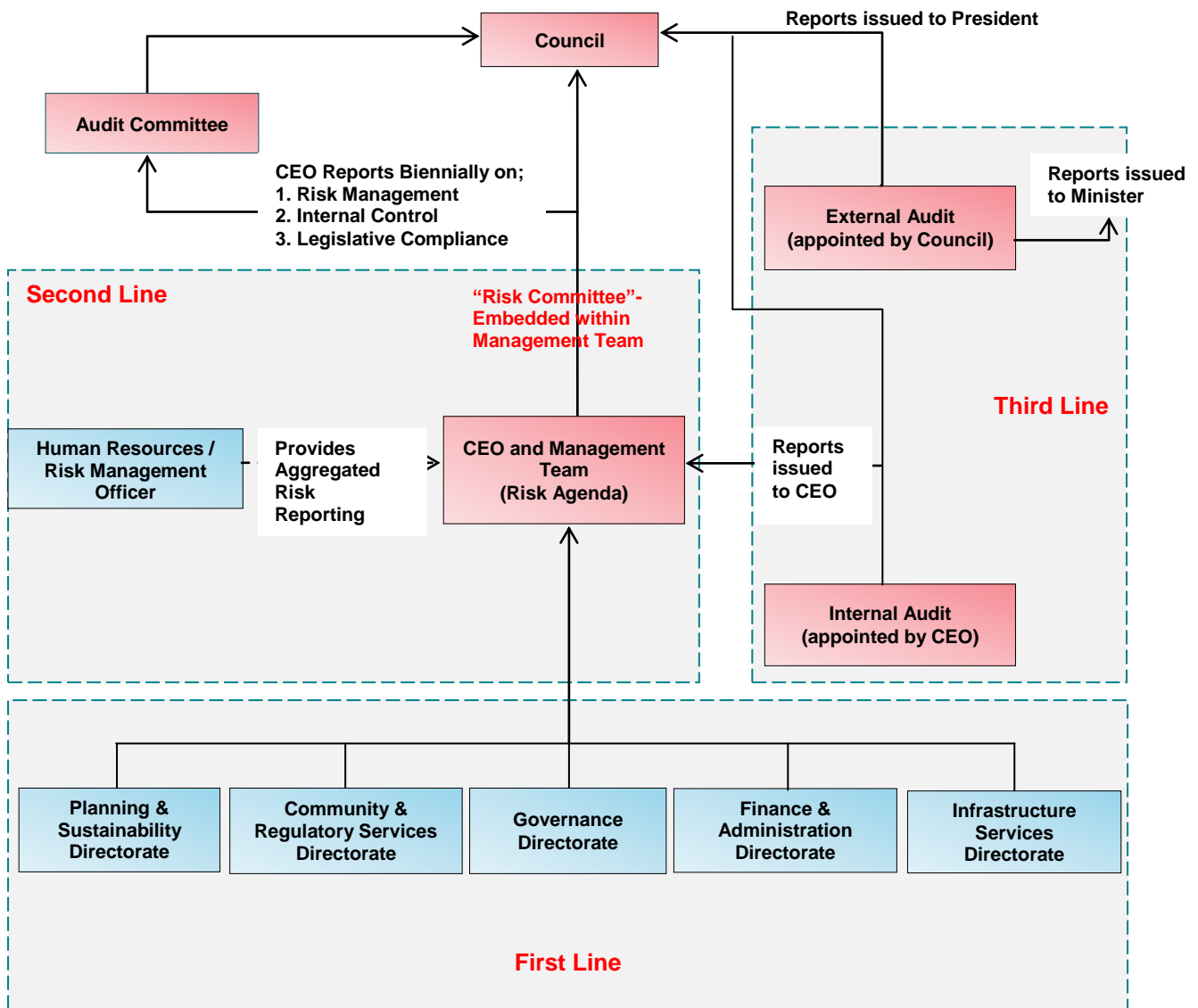
Internal & External Audit are the third line of defence, providing independent assurance to the Council, Audit Committee and Shire Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

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 CEO in accordance with Regulation 5 of the Local Government (Financial Management) Regulations 1996 and Regulation 17 of the Local Government (Audit) Regulations 1996.

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 diagram depicts the current operating structure for risk management within the Shire.



Roles & Responsibilities

Council

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

Audit Committee

- Support Council to provide effective corporate governance.
- Oversight of all matters that relate to the conduct of External Audits.
- Must be independent, objective and autonomous in deliberations.
- Make recommendations to Council on External Auditor appointments.

CEO / Management Team

- Appoint Internal Auditors 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 Framework.
- 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.

Human Resources / Risk Management Officer

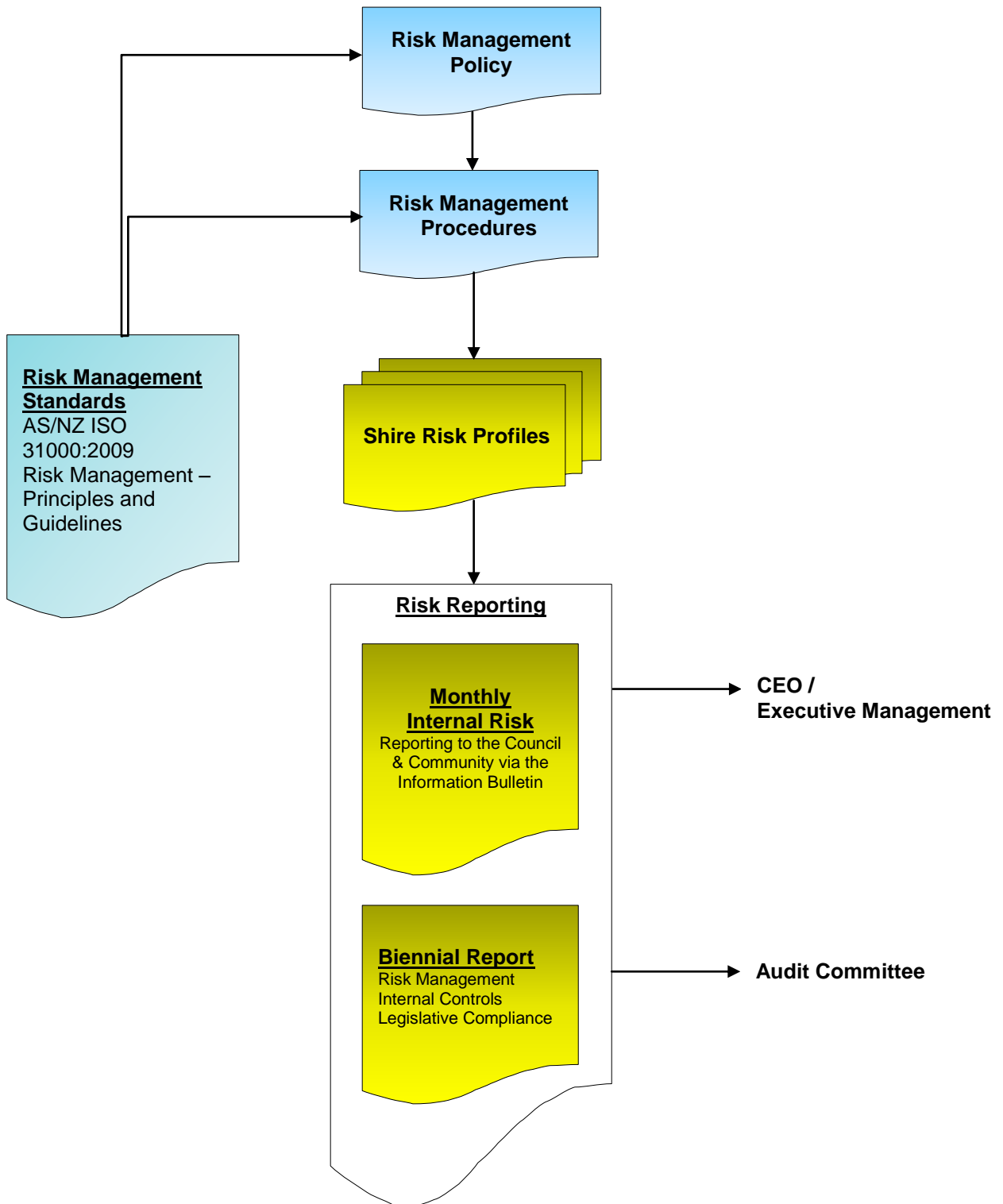
- Oversee and facilitate the Risk Management Framework in liaison with the CEO.
- Support reporting requirements for Risk matters.

Directorates

- 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, Team and Toolbox meetings by incorporating the following risk agenda items;
 - Risk Management
 - New or emerging risks.
 - Review existing risks.
 - Control adequacy.
 - Outstanding issues and actions.

Document Structure (Framework)

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



Risk & Control Management

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

Each Director, in conjunction with the Human Resources / Risk Management Officer is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Shire.
- Reviewed on at least an annual basis, unless 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 key data inputs, workshops and ongoing business engagement.

Importantly, Risk Management is a journey not a destination.

Not all Risks need to be mapped or controlled - and in initial years on that journey, risk assessment at the Shire of Denmark will be conducted as follows;

- When major decisions are to be made.
- When key strategies are to be developed.
- As part of operational planning where appropriate.
- Prior to commencement and at key milestones of important projects and programs.
- When existing processes are improved or upgraded.
- When new processes are designed or developed.

Risk & Control Assessment

To ensure alignment with AS/NZ ISO 31000:2009 Risk Management, the following approach is to be adopted from a Risk & Control Assessment perspective:

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:

Organisational Context

The Shire's Risk Management Procedures provide the basic information and guidance regarding the organisational context to conduct a risk assessment; this includes Risk Assessment and Acceptance Criteria (Appendix A) and any other tolerance tables as developed. 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 or Risk Assessment & Acceptance Criteria must be approved by the Human Resources / Risk Management 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.

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:

1. Strategic Context

This constitutes the Shire's external environment and high-level direction. Inputs to establishing the strategic risk assessment environment may include;

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

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.

3. Project Context

Project Risk has two main components:

- **Risk in Projects** 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.
- **Project Risk** 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.

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 could 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? (Consequences).

Risk Analysis

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

- Based on the documented current controls, and previous history, 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).

Risk Evaluation

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

- Controls Assurance (i.e. are the existing controls in use, effective, documented, up to date 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 its systemic nature.

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 treatment selection and implementation to be based on;

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

Once a treatment has been fully implemented, the Human Resources / Risk Management Officer 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).

Monitoring & Review

The Shire is to review all Risk Profiles on a regular basis and at least annually 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 Human Resources / Risk Management Officer is to monitor the status of risk treatment implementation and report on to the CEO, if required.

The CEO & Management Team will monitor significant risks and treatment implementation as part of their normal agenda item on a regular 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 Catastrophic.
- 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 & Management Team. They will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and appropriate to the Shire.

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.

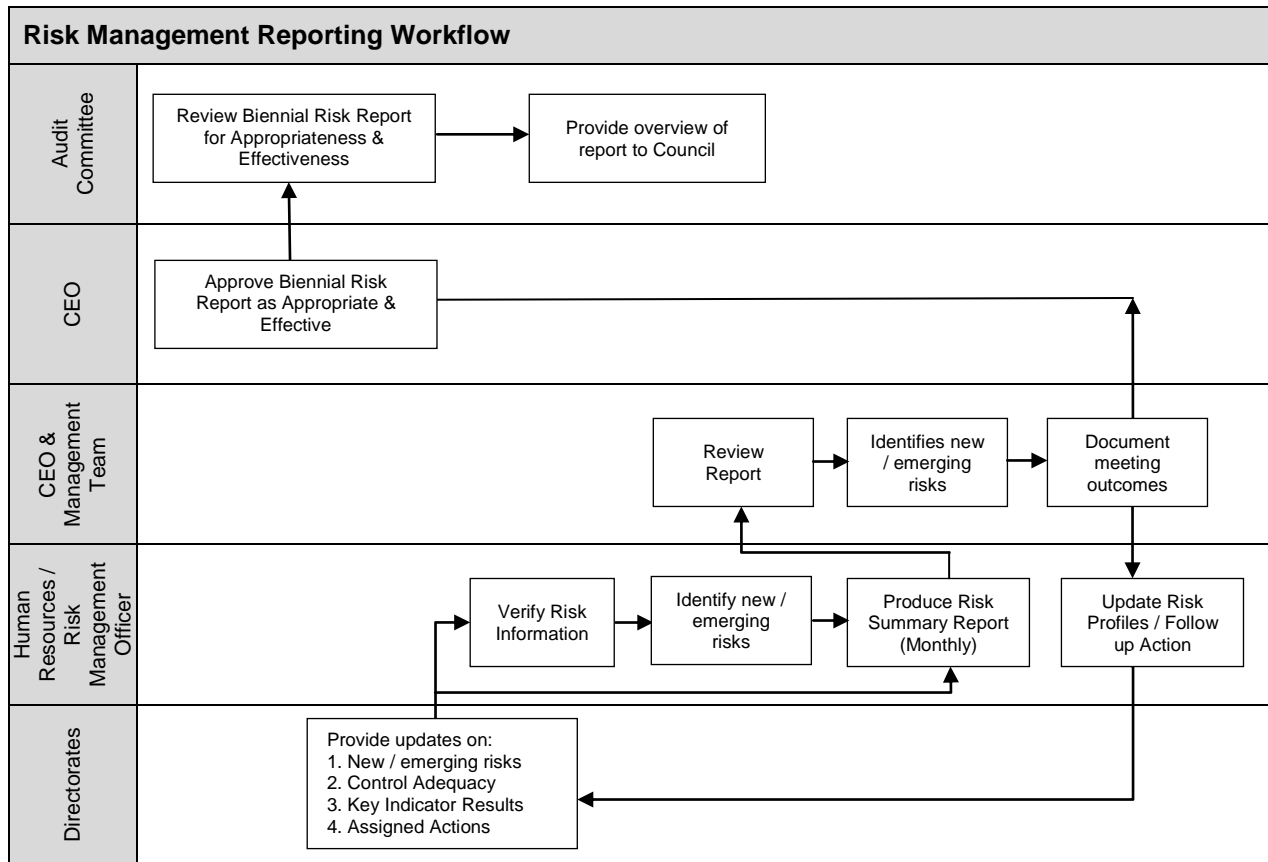
Appropriate risk management awareness and training will be provided to employees as applicable.

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 Directorate is responsible for ensuring:

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

The Human Resources / Risk Management Officer is responsible for:

- Ensuring Shire Risk Profiles are formally reviewed and updated, at least on an annual basis or when there has been a material restructure, change in risk ownership or change in the external environment.
- Producing a monthly Risk Report for the CEO & Management Team which contains an overview Risk Summary for the Shire.
- Annual Compliance Audit Return completion and lodgement in conjunction with the Director of Finance & Administration.

Key Indicators

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

Identification

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

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

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

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

Tolerances

Tolerances are set based on the Shire's Risk Appetite. They are set and agreed over four levels:

- **Green** – within appetite; no action required, minimal monitoring required.
- **Yellow** – just outside appetite but will require some monitoring to ensure that it does not escalate.
- **Amber** – the Key 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 Key Indicator must be escalated to the CEO & Management Team where appropriate management actions are to be set and implemented to bring the measure back within appetite.

Monitor & Review

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

When monitoring and reviewing Key Indicators, the overall trend must be considered over a longer timeframe instead of individual data movements. The trend of the Key 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 general competencies and authorisations framework of the Shire.

Risk Acceptance 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 identified risks.

The 'Risk Acceptance' must be in writing, authorised by the relevant Director 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.

A lack of budget / funding 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. Management Team).

Annual Risk Monitoring Plan

The Annual Risk Monitoring Plan is a schedule prepared by the Human Resources / Risk Management Officer and approved by the CEO that sets out the control assurance activities to be conducted over the next 12 months. This plan should 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).
- 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 Key Indicators.
- Timetable for monitoring activities.
- Reporting requirements.

Whilst this document and subsequent actions are owned by the Human Resources / Risk Management Officer, input and consultation will be sought from individual Directorates.

Appendix A – Risk Assessment and Acceptance Criteria

Shire of Denmark Measures of Consequence							
Rating (Level)	Health	Financial Impact	Service Interruption	Compliance	Reputational	Property	Environment
Insignificant (1)	First aid injuries	Less than \$10,000	No material service interruption	No noticeable regulatory or statutory impact	Unsubstantiated, low impact, low profile or 'no news' item	Inconsequential damage.	Contained, reversible impact managed by on site response
Minor (2)	Medical type injuries	\$10,001 - \$50,000	Short term temporary interruption – backlog cleared < 1 day	Some temporary non compliances	Substantiated, low impact, low news item	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response
Moderate (3)	Lost time injury <30 Days	\$50,001 - \$250,000	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, moderate news profile	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies
Major (4)	Lost time injury >30 Days	\$250,001 - \$1,000,000	Prolonged interruption of services – additional resources; performance affected < 1 month	Non-compliance results in termination of services or imposed penalties	Substantiated, public embarrassment, high impact, high news profile, third party actions	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic (5)	Fatality, permanent disability	More than \$1,000,000	Indeterminate prolonged interruption of services – non-performance > 1 month	Non-compliance results in litigation, criminal charges or significant damages or penalties	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact

Shire of Denmark Measures of Likelihood			
Level	Rating	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances	More than once per year
4	Likely	The event will probably occur in most circumstances	At least once per year
3	Possible	The event should occur at some time	At least once in 3 years
2	Unlikely	The event could occur at some time	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	Less than once in 15 years

Shire of Denmark 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)

Shire of Denmark Risk Acceptance Criteria			
Risk Rank	Description	Criteria	Responsibility
LOW (1-4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager / Supervisor
MODERATE (5-9)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager / Supervisor
HIGH (10-16)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Director / CEO
EXTREME (20-25)	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 Denmark 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		
<p>This Risk Theme is defined as; <i>Definition of Theme</i></p>			
<p>Potential causes include; <i>List of potential causes</i></p>			
Key Controls	Type	Date	Shire Rating
<i>List of Key Controls</i>			
Overall Control Ratings:			
Consequence Category	Risk Ratings		Shire Rating
	Consequence:		
	Likelihood:		
Overall Risk Ratings:			
Key Indicators	Tolerance	Date	Overall Shire Result
<i>List of Key Indicators</i>			
<p>Comments <i>Rationale for all above ratings</i></p>			
Current Issues / Actions / Treatments		Due Date	Responsibility
<i>List current issues / actions / treatments</i>			

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 in transaction processing, or Inaccurate Advice.

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 Disruption

A local physical event causing the inability to continue business activities and provide services to the community; this may or may not result in Business Continuity Plans being invoked. This does not include disruptions due to:

- IT Systems or infrastructure related failures should be captured under "Failure of IT Systems and Infrastructure".
- Contractor / Supplier issues should be captured under "Inadequate Supplier / Contract Management".
- People issues should be captured under "Inappropriate People Management".

Damage to Physical Assets

Damage to buildings, property, plant & equipment (all assets) that does not result in a disruption to business objectives (refer Business Disruption); this could be a result of a natural disaster or other events, or an act carried out by an external party (Inc. graffiti and / or vandalism).

Errors, omissions, delays

Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process or legislative or policy impositions or constraints. 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 Change Management".

Failure to meet 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;

- Issues in relation to OH&S – refer "Inadequate employee and visitor safety and security"
- Procurement, disposal or tender process failures – refer "Inadequate Procurement, Disposal or Tender Practices"
- HR based legislation – refer "ineffective People Management"

Providing Inaccurate Advice / Information

Incomplete, inadequate or inaccuracies in professional advisory activities to customers or internal staff. This could be caused by using unqualified staff, however it does not include instances relating Breach of Authority.

Inadequate 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.

This includes Directorate or Service Unit driven change initiatives except new Plant & Equipment purchases. Refer "Inadequate Plant and Equipment design, delivery and maintenance"

Inadequate Organisation or Community Emergency Management

Failure to adequately conduct Prevention, Preparation, Response and Recovery (PPRR) in the organisation structure and community elements, inclusive of the management of all emergencies. This includes;

- Lack of (or inadequate) emergency response 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.

(References: AS 3745; AS 1851; AIIMS 4 Management Principles)

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 Employee or Visitor Safety & Security

Non-compliance with Occupation Health & Safety (OH&S) Regulations and physical security requirements. This risk includes issues relating to:

- Inadequate Policy, Frameworks, Systems and Structure to prevent the injury of visitors, staff, contractors and/or tenants in the provision of a working or business environment.
- 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 engagement of Community / Stakeholders / Elected Members

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 Road Maintenance.

Inadequate Procurement, Disposal or Tender Practices.

Failures in the procurement, acquisition, acceptance or disposal process for assets as governed by the Local Government Act 1995. This risk theme also relates to and includes;

- Lack of formalised process to identify specific requirements prior to procurement.
- Acceptance of assets without reference to a formalised process to ensure correct receipt and / or notification of receipt (transfer of ownership).
- Disposing of P & E (either through sale or decommissioning) that did not meet expectations from either a time or financial perspective.
- Failures in the Tender process from RTF preparation, advertising, due diligence and awarding.

Inadequate Asset Management

Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet assets in addition to community use based assets including playgrounds, boat ramps and other maintenance based assets. Areas includes in the scope are;

- Inadequate design (not fit for purpose).
- Ineffective usage (down time).
- Outputs not meeting expectations.
- Inadequate maintenance activities.
- Inadequate or unsafe modifications.

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

Inadequate Stock Management

Lack of stock to ensure continuity of operations or oversupply of stock resulting in dormant (non-performing) assets. Stock includes, consumables, stationery, spare parts and / or other items used for

operational purposes. This could be a result of an ineffective stock management system / processes or the peripheral processes in the issuance and / or recording of 'transactions'.

It does not include theft or loss of stock through ineffective operations; refer;

- Theft – “Misconduct” or “External Theft or Fraud”.
- Ineffective operations – “Errors, Omissions or Delays”.

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.

It does not include failures in the tender process; refer “Inadequate Procurement, Disposal or Tender Practices”.

Ineffective People Management

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 inefficiency.

Ineffective Management of Facilities / Venues / Events

Failure to effectively manage the day to day operations of facilities, venues and / or events. 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).

Not meeting Community expectations

Failure to provide expected levels of service, events and benefit to the community. This includes where precedents have set Community perceptions or where services are generally expected. This will normally result in reputational impacts, however may have financial considerations with re-work, compensations or refunds. Examples include:

- Reducing the number or quality of events.
- Withdrawing support (or not supporting) other initiatives to provide relief/benefits to the Community.
- Loss of new or ongoing funding requirements for projects, events and other initiatives.
- Technology expectations.

Inadequate Natural Environment Management.

Inadequate prevention, identification, enforcement and management of natural 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 Financial, Accounting or Business Acumen

Inadequate identification or quantification of financial exposure or risk associated with decisions to invest in land transactions, financial derivatives or investments or poor long term forecasting / assumptions.

Examples include;

- Poor credit management (short or long term borrowing restricting capacity or flexibility).
- Ineffective market analysis (over or under estimating).
- Ineffective Business Planning (poor scope / competition analysis).
- Ineffective financial modelling, forecasting and projection techniques / processes.