

RISK MANAGEMENT FRAMEWORK

TABLE OF CONTENTS

1. Introduction
2. Purpose
3. Scope
4. Risk management principles
5. Risk management framework
 - 5.1 Risk, governance and Assurance
 - 5.1.1 Governance
 - 5.1.2 Assurance
 - 5.2 Risk management policy
 - 5.3 Risk management system
 - 5.4 Risk management process
 - 5.4.1 Establish the context
 - 5.4.2 Risk assessment
 - 5.4.2.1 Risk assessment
 - 5.4.2.2 Risk identification
 - 5.4.2.3 Risk analysis
 - 5.4.2.4 Risk evaluation
 - 5.4.3 Risk treatment
 - 5.4.4 Monitor and review
 - 5.5 Roles and Responsibilities
 - 5.6 Recording and reporting
6. Attachments
7. References



1. INTRODUCTION

The Town of Port Hedland (also referred to as 'the Town') is committed to identify, assess and manage, as an integral part of good management practice, all risks which may prevent the achievement of strategic goals and objectives. Risk management will be integrated into the Town's culture, decision-making processes, programs, practices, business planning and performance reporting activities and will establish a safe working environment for all staff.

AS/NZS ISO 31000: Risk Management – Principles and Guidelines, defines risk as "*the effect of uncertainty on objectives*". Risk Management is the responsibility of each person who is accountable for the function, service or activity that gives rise to that risk. Risk management is a continuous process to manage and mitigate threats and realise opportunities.

The strategic objective of Risk Management is to:

- Achieve organisational goals and objectives
- Ensure the ongoing health and safety of all employees at the workplace
- Ensure that public safety within the Town's jurisdiction is not compromised
- Limit the loss or damage to property and other assets
- Limit interruption to business continuity
- Foster positive public perception of the Council and the Town of Port Hedland

2. PURPOSE

This Risk Management Framework and methodology is based on **AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines**. This framework supports the Risk management policy (1/022), adopted by the Town, and focuses on encouraging a high standard of accountability at all levels in the Town in support of effective governance. The emphasis is on managing risks and maximising all opportunities as opposed to eliminating risk.

The purpose of this Framework is to:

- **Define** risk management.
- Outline the risk management **approach**.
- Outline the **process** of systematically managing risk across the Town.
- Outline **roles and responsibilities** for risk management within the Town.
- Explain the risk management **recording and reporting** requirements within the Town.

The Town will manage risks continuously using a process involving the identification, analysis, evaluation, treatment, monitoring and review of risks. It will be applied to decision making at all levels in the organisation in relation to planning or executing any function, service or activity and in particular, it will apply to:

- Strategic planning;
- New strategies and procedures;
- Management of projects, tenders and proposals;
- Introducing significant change;
- The management of sensitive areas; and
- Day to day business operations



3. SCOPE

The scope for identification of risk categories in the Risk Management Framework is broadly set as:

- **Strategic:** Risk associated with high level goals which align to the Town's strategic, business and annual plans.
- **Operational:** Risk associated with the functions and daily operations of directorates or work groups
- **Project:** Risk associated with projects, tenders and proposals
- **Compliance:** Risk associated with legislative/ regulatory requirements
- **Residual:** Risk remaining after risk treatment

Other specific items which can be associated with these categories, and included in the scope of this framework, are:

- Risk associated with introduction of **significant change**.
- The management of **sensitive areas**.
- **New** strategies and procedures.

4. RISK MANAGEMENT PRINCIPLES

The **AS/NZS ISO 31000:2009** standard explains the principles of effective risk management. These principles will be applied in this Risk Management Framework to achieve best practice outcomes.

The effective risk management principles which we will be endeavouring to achieve through best practice are:

- It will create value
- It is an integral part of the Town's processes
- It will involve decision making
- It will explicitly address uncertainty
- It will be systematic and structured
- It will be based on the best available information
- It will be tailored to suit the need and purpose
- All human factors will be accounted
- It will be inclusive and transparent
- It will be dynamic, interactive and responsive to change
- The focus will be on continued improvement and enhancement

5. RISK MANAGEMENT FRAMEWORK

The risk management framework forms the foundation of the Town's management of risk and arranges the actions for the design, implementation, monitoring, review and continuous improvement of risk management in the Town. This is demonstrated in the figure below.

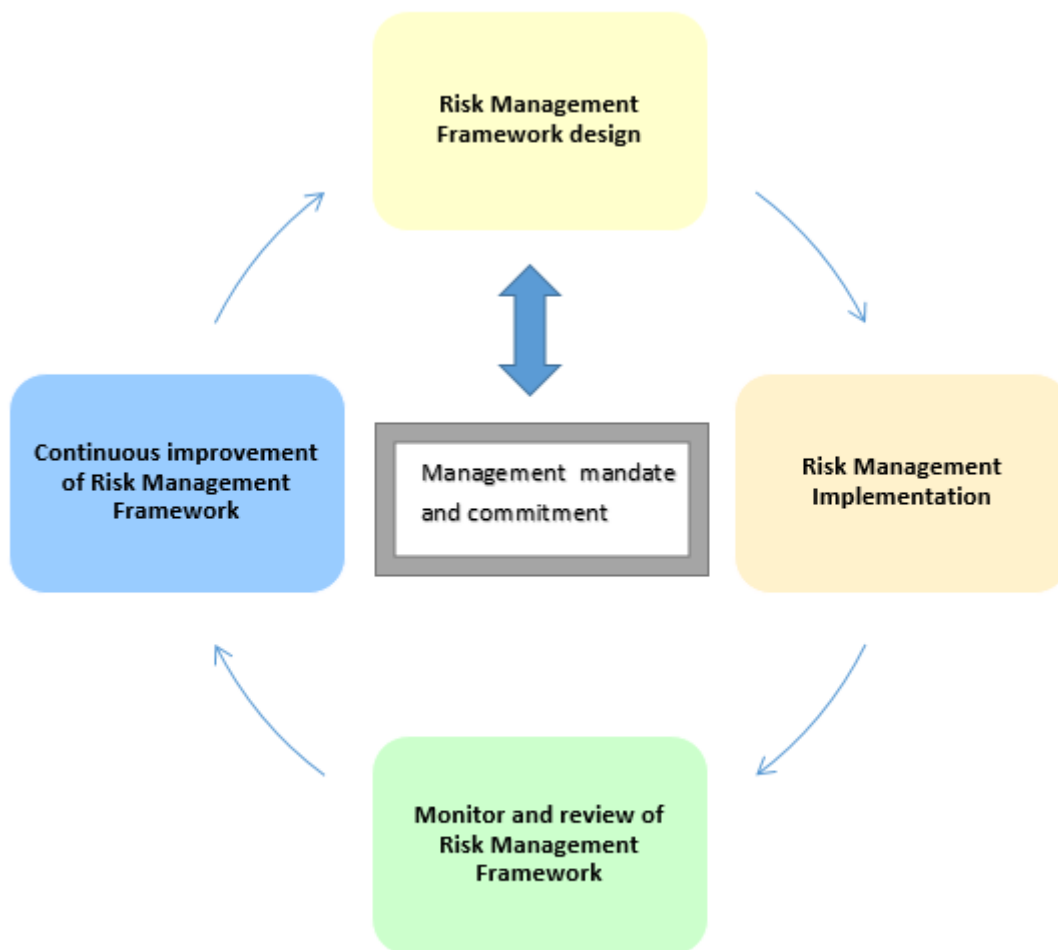


Figure 1 – Risk Management Framework

The Risk Management framework is broken down in the following key components:

- Governance and assurance and functioning of the audit, Risk and Governance Committee
- The risk management policy, it's purpose, commitment and responsibilities
- The risk management system and risk management culture, capabilities, tools templates, reporting and evaluation and review.
- The risk management process with the management of strategic, departmental and business area and program and project specific risk.



5.1 RISK, GOVERNANCE AND ASSURANCE

This component of the framework relates to the Town's governance framework and the functionality of the Audit, Risk and Governance Committee. Details of the committee's functionality, objectives and responsibilities are set out in the committee's terms of reference. Governance and assurance is broken down into two separate sections.

5.1.1 Governance

The Council provide strategic leadership in determining the risk appetite, setting the risk profile and moderating strategic Town risks. Risks identified are recorded in the Town's risk registers, which provide ELT and responsible officers with a view of the Town's risks unique and common to all departments, business areas and functionalities.

The Audit, Risk and Governance Committee is responsible for reporting to Council on the effectiveness of the risk management framework. The role of the Executive Leadership Team is to oversee and provide direction for the management of risks within the Town. Department managers provide oversight for operational, project and program risks in the relevant business area.

5.1.2 Assurance

Risk assurance is the process of providing feedback to Council that quality processes and controls are in place and are effective. This is done via internal and external audit and risk management monitoring and reporting.

Risk management monitoring and reporting - The Town's Risk management policy outlines the roles and responsibilities of key officers relating to the monitoring and reporting of risk. Reporting levels are based on the risk matrix set out in the policy. Risk management monitoring includes the assurance that risks have been assessed in accordance with the Town's risk management framework and are monitored and reported regularly. It also includes the assurance that emerging risks are escalated to the appropriate level and the assurance methods mapped to the risks that threaten objectives.

Internal Audit – Through a disciplined approach, internal audit brings objectivity and consultative attributes to evaluate and improve the effectiveness of the risk management, control and governance processes.

The Town's internal audit plan tests the internal controls around the Town's material risks. The internal audit outcomes are periodically reviewed as part of the risk management framework and its effectiveness reported.

External Audit – The purpose of the external audit is to gain reasonable assurance that accounts are free from material misstatements and can be relied upon to be presenting a true and fair view of the affairs of the Town. Tax authorities, financial institutions and management rely on the audited financial statements. Management uses the audited financial statements to re-evaluate and improve the Town's risk management processes and internal control system by considering the feedback given by the external auditors during the course of the audit.



5.2 RISK MANAGEMENT POLICY

The Risk Management Policy (1/022) is a key component of the risk management framework and states the overall purpose and direction of the Town's commitment towards risk management, emphasising the risk management principles and responsibilities for managing risk.

5.3 RISK MANAGEMENT SYSTEM

Risk management capability is a key driver for the effective management of risk. A risk capable organisation understands that:

- The role of the Executive Leadership team and operational leaders is extremely important in developing a risk conscious culture which is part of the everyday decision making process. This is achieved through leadership, communication and the integration of risk management with other business processes and systems.
- Electronic Tools and templates are important to record, track and control risks and evaluate implemented treatments. The Town embedded the risk matrix in all Council and Executive Leadership team documentation for ease of use. All reported risks are subject to a quality review process that ensures there is a consistent approach and language used across the Town. Results are recorded in the Town's risk registers.
- Risk reporting has been aligned with the Town's governance structure. Strategic and significant operational risks are reported monthly to the Executive Leadership team, relevant managers and the Audit, Risk and Governance Committee. Strategic and high operational risks are reported to the Executive Leadership team and the relevant managers and strategic, moderate and minor operational risks are reported to business area managers and coordinators.
- The Town's risk management framework will be reviewed regularly by the Audit, Risk and Governance Committee to ensure the adequacy of the framework and its application. The committee's key responsibility is to provide assurance to Council that the risk management framework remains relevant and robust.
- The Executive leadership team is responsible for the regular review of the risk management capabilities and governance system to ensure the continuous improvement of the risk management framework. This responsibility includes the review of the current; and subsequent modifications to the Town's processes, systems, resources, capabilities and skills. Operational area managers periodically evaluate the risk management practices in their unit and align it with the framework to ensure it is operating effectively with the focus on continuous improvement of risk management.



5.4 RISK MANAGEMENT PROCESS

The risk standard defines risk management as the “*Coordinated activities to direct and control an organisation with regard to risk*”. The Town aims to create a culture of risk management instilled in decision making by each employee. To achieve this a process of continuous identification, analysis, evaluation, treatment, monitoring and review is followed.

The following diagram explains the risk management process:

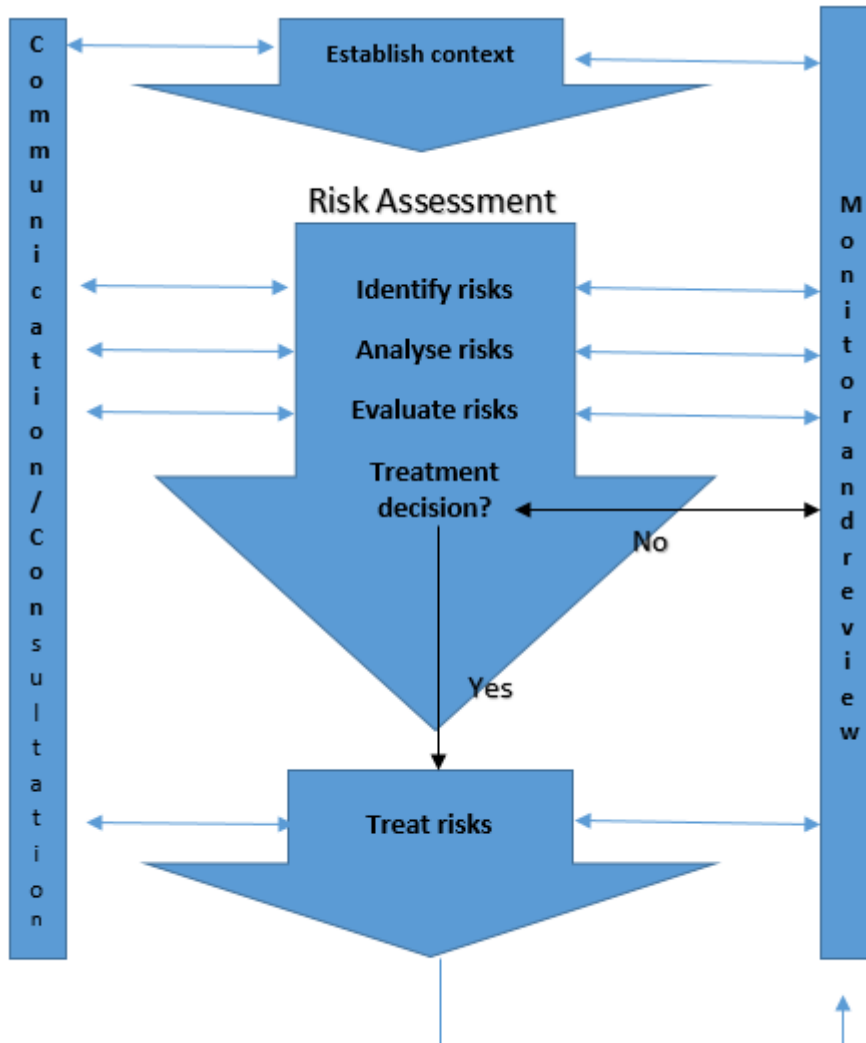


Fig 2 – Risk Management Process

Council is committed to a risk management process which:

- Establishes the context for the risk management process
- Identifies risks which could expose Council or the general community
- Identifies measures to be in place to treat and control risks
- Identifies the likelihood of certain events taking place
- Identifies the consequences of those events
- Rates the identified risks
- Identifies alternative measures to treat the identified risk

- Develops action plans, assigns responsibilities and timeframes to the implementation of those actions
- Records risks and the associated action plans within a risk register
- Measures and monitors the entire process.

5.4.1 Establish the context

To enable efficient identification of risk and achieve overall strategic and business objectives, risk management should be considered in the context of the Town's external and internal environment, its objectives and stakeholder relationships

Step 1 is to establish external environment in which the Town operates and the inputs relating to

- Business,
- Social,
- Regulatory,
- Legislative,
- Cultural,
- Competitive,
- Financial and the
- Political environment.

Further consideration is given to

- Strengths,
- Weaknesses,
- Opportunities
- Threads,
- Relationships with,
- Perceptions and values of and
- External stakeholders such as community.

Step 2 is to establish the internal context. This is the environment in which the Town functions and seeks to achieve its objected. Consideration is given to the

- Objectives and strategies in place to achieve goals
- Governance, structure, roles and accountability
- Capability of people, systems and processes
- Changes to processes or compliance obligations
- The risk tolerance and appetite of the Town.

To ensure accurate risk analysis and the successful management of risk through treatment plans implemented, it is important to establish the context first.

5.4.2 Risk assessment

5.4.2.1 Risk assessment is the systematic process of risk identification, analysis and evaluation. The principles applying to risk assessment is identification of risk, risk analysis and evaluation of the risk. It is important to include contingency planning in the risk management process. Contingency plans, is plans made to deal with unexpected disruption or harm done to the Town's expected operations, its workforce, the community or the environment it operates in.



5.4.2.2 Risk identification is the action to identify the sources of the risks, areas of impact, events, opportunities, possible failure to innovate and the causes and potential consequences. A good practice is to generate a list of risks based on the impacts or events. Risk analysis tools such as PESTLE, SWOT, Project and other analytical tools can be used, depending on the scope and type of risk.

Step one in this process is to identify what can happen, where and when it can happen. This will generate a list of potential risks that may impact the Town achieving each objective identified as part of the context. This should describe an outcome such as: “failure to...”, “inconsistent to...” or “loss off...”

A set of questions developed to identify risk, is used to identify the type of risk. These include questions such as; what, why, who, where, etc.

Step two is to identify why and how the risk can take place. The potential triggers which may result in the risk occurring is identified as well as the type of risk. The possible impact should the risk event occur is identified. A consequence may be common across multiple risk and a single risk event may have one or multiple consequences. Techniques in use include:

- Raise of risk identified by any staff member as part of the ongoing identification process or
- A process of discussion and assessment of the risk and controls with the staff involved in the day-to-day operation of the activity of process.

5.4.2.3 Risk analysis provides an understanding of the risk and guides the decision to treat the risk or not and helps in selection of the most appropriate treatment to be applied. Risk analysis also provide input in making decisions where choices need to be made between treatment options and the options involved for different types and levels of risk.

The following levels of risk can be identified, depending on the activity being assessed:

- Strategic Level Risks. These are risks associated with achieving the objectives of the Towns Strategic Community plan and the delivery of the Corporate Business Plan.
- Operational Level Risks. These risks is associated with the development and delivery of operational plans and functions or activities of the Town, including the Long Term Financial Plan, Workforce Plan and Asset Management Plan.
- Project/Event Level risks. These risks is associated with the delivery of specific projects or discrete activities and risks should be managed at each stage of the project/event by the person responsible for the project/event.

In assessing the risks, the criteria and rating to be used, is set out in the risk assessment and acceptance criteria matrix included in the Town’s Risk Management policy 1/022. This assessment criteria is measuring the likelihood and consequence of the risk and from this the risk rating is calculated. The treatment/control actions is designed according to the risk rating and action is taken according to the acceptance criteria set out in this Risk matrix.

Step 1 involves analysis of the inherent risks. The risk is assessed, considering the likelihood and impact of the risk, without taking any current controls in place in consideration.

Assessing the inherent likelihood, means determining the probability of the risk event occurring if no controls were in place.

Assessing the inherent consequence, means determining the extent of the most probable impact of the risk event occurring, if no controls were in place.

Step 2 is the actions to analyse the residual risk. Residual risk is the risk remaining after existing internal controls are taken into account. Changes from the inherent to residual ratings will be dependent on the existing controls, and whether it is addressing the likelihood of the risk, the consequence of the risk or both.

For each of the residual risks identified, the likelihood of the risk event occurring within the current control environment is determined. This is done after the effectiveness of the control has been evaluated.

The probable impact of the residual risk event is then determined in relation to the impact if it were to occur within the current control environment. The assumption should be that controls are operating at the assessed strength, and not that maximum consequence should the controls fail.

For each risk, there should be only one overall residual risk rating, based on the effectiveness of the controls in place to address the risk.

5.4.2.4 Risk evaluation is the process of deciding which risks to treat and the priority of the treatment/s to be implemented.

It involves the identification and evaluation of treatments/controls. A treatment/control is defined as any action in place that either reduces the likelihood of an event occurring or reduces the potential consequence arising from the event. For each risk identified, there may be a single or multiple treatments/controls in place to address the risk.

For each risk identified, an existing control is identified as well. This can be a process, policy, device, practice or any other action used to modify the likelihood or the consequence of the risk event occurring. The absence of an existing control, highlights a gap in the controls.

The effectiveness of the existing control is then measured in terms of the strength of its design and its operation.

Step 1 involves comparing the risk rating against the criteria/ risk appetite set out in the Risk Assessment and acceptance criteria of the Town.

Step 2 involves setting of the risk priorities. The highest rated risks are treated first. High and extremely high risks are addressed as a matter of urgency.

5.4.3 Risk Treatment

Risk treatment decisions are made according to the Town's risk matrix. Treating risks involves the selection of one or more options to modify the risk, and then the preparation and implementation of the option/s.

A treatment/action plan is put in place when current controls are either ineffective or require improvement or no controls exist. Treatment plans may be generated from various business processes, including business plans, audit reports, action plans or the risk register. The steps are:

Step 1: Identify and assess the risk treatment options.

Risk treatment involves selecting one or more options for modification of the risk and implement this option/s. It is a cyclical process involving

- Assessment of the risk treatment
- Deciding whether the residual risk levels are tolerable
- Generation of new risk treatments for risk levels which are not tolerable
- Assess of the effectiveness of the treatment

Step 2: Select risk treatment options

Treatment decisions is made based on the outcomes of the risk evaluation and the rating per the Town's risk rating matrix.

Treatment options normally include one of the following:

- Accept the risk (tolerate the risk)
- Accept the Risk in order to pursue an opportunity
- Avoid the Risk
- Remove the risk
- Changing the likelihood of the situation
- Changing the consequence of the situation
- Share the risk (with insurance companies, partners and other organisations)

Selecting the most appropriate risk treatment, means balancing the costs of implementing each activity against the benefits derived. When the decision has been made regarding treatment of the risk, a treatment plan is developed and implemented.

Treatments/controls can be linked to more than one risk, both internal and external to the organisation, making communications crucial in the treatment of the risk and normally require further treatments/controls to ensure that the original control or treatment is effective. Action plans may require more than one treatment with more than one owner.

Step 3: Prepare and implement a risk treatment plan.

A treatment/control plan is required for each level of risk. Effective risk treatment relies on committing to realistic objectives and timelines for implementation. For each risk assessment, the following will be detailed:

- The treatment option selected
- A documented treatment plan
- A risk treatment owner
- A target resolution date

To implement a treatment plan, the following initiatives should be in place:

- Structure or delegations to support the risk treatment plan
- Financing for the plan within the budget for the control
- Available resources
- Specified mechanism for monitoring



- A recorded status of the treatment plan.

Preparation of treatment plans include the preparation of contingency plans.

Step 4: Analyse and evaluate the residual level of the risk

Decision makers and other risk owners, should be aware of the nature and extent of residual risk remaining after treatment plans have been put in place.

This risk should be documented, monitored, reviewed and where applicable, further treatment applied.

All risks will be recorded in the Town's Risk register and reviewed regularly by elected members, the senior leadership team and department Managers.

5.4.4 Monitor and review

Monitoring and review is a planned part of the risk management process and involve regular checking and surveillance. Results is recorded both internally and externally, as appropriate and used as input towards the continuous improvement process of the Town's risk management framework.

Continuous checking, assessment and modification of treatment/control effectiveness is required for the purposes of:

- Ensuring effective and efficient control in both design and operation
- Provide further information to improve risk assessment
- Analysis and learning from risk events, changes, trends, successes and failures and near misses.
- Detect changes in the external and internal context, changes to the risk criteria and risks which require a revision of the risk treatments and priorities
- Facilitate the identification of emerging risks

All risk registers will be reviewed by the applicable risk owners on a regular basis.

The Risk Management Framework's purpose is to embed a risk aware culture within the Town. This will be evaluated periodically considering breaches and near misses, effective communication, corrective actions taken and lessons learned. The review process is part of the continuous improvement of the Towns risk management with the objective to ensure that the framework is still effective and applicable.

The assessment is a biannual function of the risk officer. The review include a review of the assessment criteria for relevancy to the Town's operations and practices.

5.5 ROLES AND RESPONSIBILITIES

It is important that all employees and stakeholders understand their roles and responsibilities in the risk management process. This responsibility is outlined in the Risk management policy and in particular apply to the following individuals or groups:

- The CEO is accountable to the Council for:
 - Establishing and maintaining a culture of risk management and awareness.
 - Ensuring risk management is embedded and applied throughout the Town.



- Ensuring employees receive the required support to fulfil their responsibilities.
 - Setting the standards of best practice for risk management, based on AS/NZS ISO 31000:2009.
 - Contributing to the attainment of the Town's Strategic Community plan.
 - Ensuring that formal risk assessments are undertaken as part of the annual business planning process.
 - Reporting all key risks with an extreme rating, to the Council.
 - Knowing when to escalate a risk.
- The Executive Leadership team and Senior Management are required to:
 - Demonstrate an understanding of and commitment to an integrated risk management system and culture.
 - Evaluate risks on a monthly basis including the relevance and level of risk and the effectiveness of treatments and existing controls.
 - Undertake annual/bi-annual risk workshops as part of the Strategic Community Plan, Long Term Financial plan and business planning review process.
 - Monitor the effectiveness of the risk management process through participation, recording, reporting and continuous monitor of risks.
 - Ensure treatments are implemented for all extreme and high risks.
 - Ensure the effectiveness of risk tolerances.
 - Ensure the compliance with risk management policies and processes.
 - Ensure the application of resources.
- Risk Champions and Operational Management team are responsible for:
 - Promoting risk management awareness activities in the Town.
 - Undertaking competency based training and other risk management professional development.
 - Facilitating monthly and quarterly reporting of the risk register and other responsibilities within their work area.
 - Facilitating training regarding risk management for Town employees.
 - Facilitating annual risk workshops and ensuring risk registers reflect outcomes.
 - Participating in the continuous review of the current Risk management process and its effectiveness with the view of improvement of the process.
 - Reporting monthly to the relevant director for sign off on the departmental risk register.
 - Maintaining up-to-date risk information in the departmental/ business unit Risk register.
- The Officer responsible for risk is responsible:
 - The provision of advice and recommendations on risk management.
 - The review of the Town's risk management framework and the monitor of its implementation.
 - The development, implementation and monitoring of risk management policies and strategies.
 - The monthly reporting of the risk register details to the Executive Leadership team and operational managers.



- The reporting of new and emerging risks that arise to the Executive Leadership team.
 - Liaising with all risk champions to get risk embedded in the Town and facilitating the practical day to day activities of risk management.
 - Develop internal audit plans to assess the Town's business processes and activities.
 - Conduct internal audits to provide assurance to the Executive Leadership team regarding the identification of key risks and the effectiveness of the control and management of those risks.
- Employees are required to:
 - Actively participate, support, report and contribute to the risk management process.
 - Be aware of risks and opportunities that relates to their operational areas.

5.6 RECORDING AND REPORTING

The Town's Risk Management Framework provides for the recording of all risks identified from strategic, operations, activities and projects in risk registers.

The risk registers is based on the organisational structure and incorporate strategic objectives, provide evidence of the risk being identified, analysed and treated and is a 'living' database to accurately record the risk management process, effectiveness of internal controls and progress of risk treatments. This include specified registers related to hazard management, employee health and wellbeing, assets, incident reporting, etc.

Risk responsibility and escalation is dependent on the risk rating.

Risk registers are reviewed regularly and escalated to the responsible officer, manager or Executive Leadership team according to the set rating criteria (refer Risk management policy). Low and medium risk items will remain the responsibility of each operational area manager and is reportable to the director of the unit annually. High to extreme risk items is reported to the senior leadership team and extreme risk items is reported for review to Council monthly.

The Risk Officer will review all registers regularly as part of the continuous improvement process.

6. ATTACHMENTS

1/022 Risk Management Policy vs201609

Audit, Risk and Governance Committee Terms of Reference

Risk register template

7. REFERENCES

<https://www.google.com.au/#q=dsitia+risk+management+framework>

http://www.dcsi.sa.gov.au/__data/assets/pdf_file/0008/9782/risk-management-framework.pdf

<https://www.qld.gov.au/dsiti/assets/documents/risk-management-policy.pdf>

<https://www.cooberpedy.sa.gov.au/webdata/resources/files/Risk%20Management%20Policy%20&%20Framework.pdf>

https://survey.charteredaccountants.com.au/risk_management/small-firms/identify.aspx