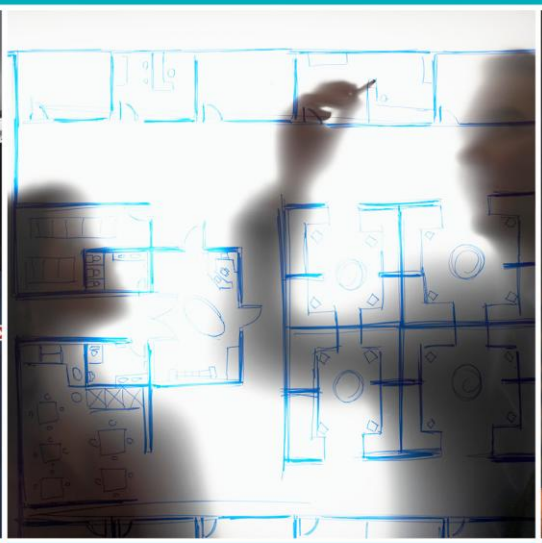



Risk Management Governance Framework

- Risk Management Policy
- Risk Management Procedures

July 2015

Version: 1.0

Town of Cottesloe

Table of Contents

Town of Cottesloe

Introduction

The Policy and Procedures form the Risk Management Framework for the Town of Cottesloe ("the Town"). It sets out the Town'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 Town adopt 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 are understood.

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

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

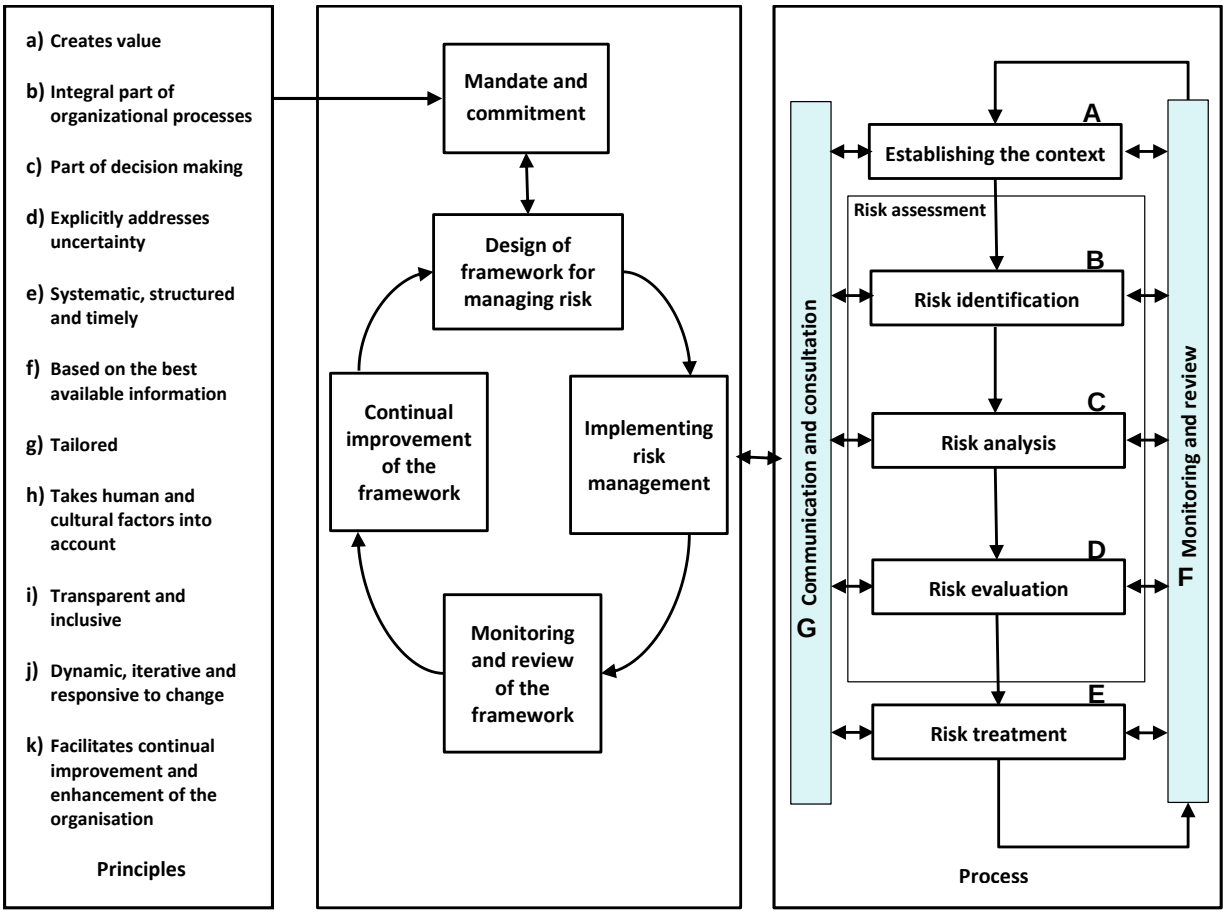


Figure 1: Risk Management Process (Source: AS/NZS 31000:2009)

Town of Cottesloe

Risk Management Policy

Purpose

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

Policy

It is the Town'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 Town, 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 Town's Integrated Planning Framework.

The Town'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, Councillor, volunteer and contractor within the Town 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.

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.

Town of Cottesloe

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 Town defined its risk appetite through the development and endorsement of the Town'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 policy.

All organisational risks to be reported at a corporate level are to be assessed according to the Town'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 Management Team.

Roles, Responsibilities & Accountabilities

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures (Operational Document).

Monitor & Review

The Town 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 kept under review by the Town's Management Team and its employees. It will be formally reviewed by the Audit & Risk Committee biennially.

Signed: ……

Mat Humfrey: Chief Executive Officer

Date: ____/____/_____

Town of Cottesloe

Risk Management Procedures

Governance

Appropriate governance of risk management within the Town of Cottesloe (the "Town") provides:

- Transparency of decision making.
- Clear identification of the roles and responsibilities of 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 annually.

Operating Model

The Town 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 Town 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.
- 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

The Manager Corporate & Community Services 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 Management Team supplement 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 Town's risk reporting for the CEO & Management Team and the Audit & Risk Committee.

Town of Cottesloe

Third Line of Defence

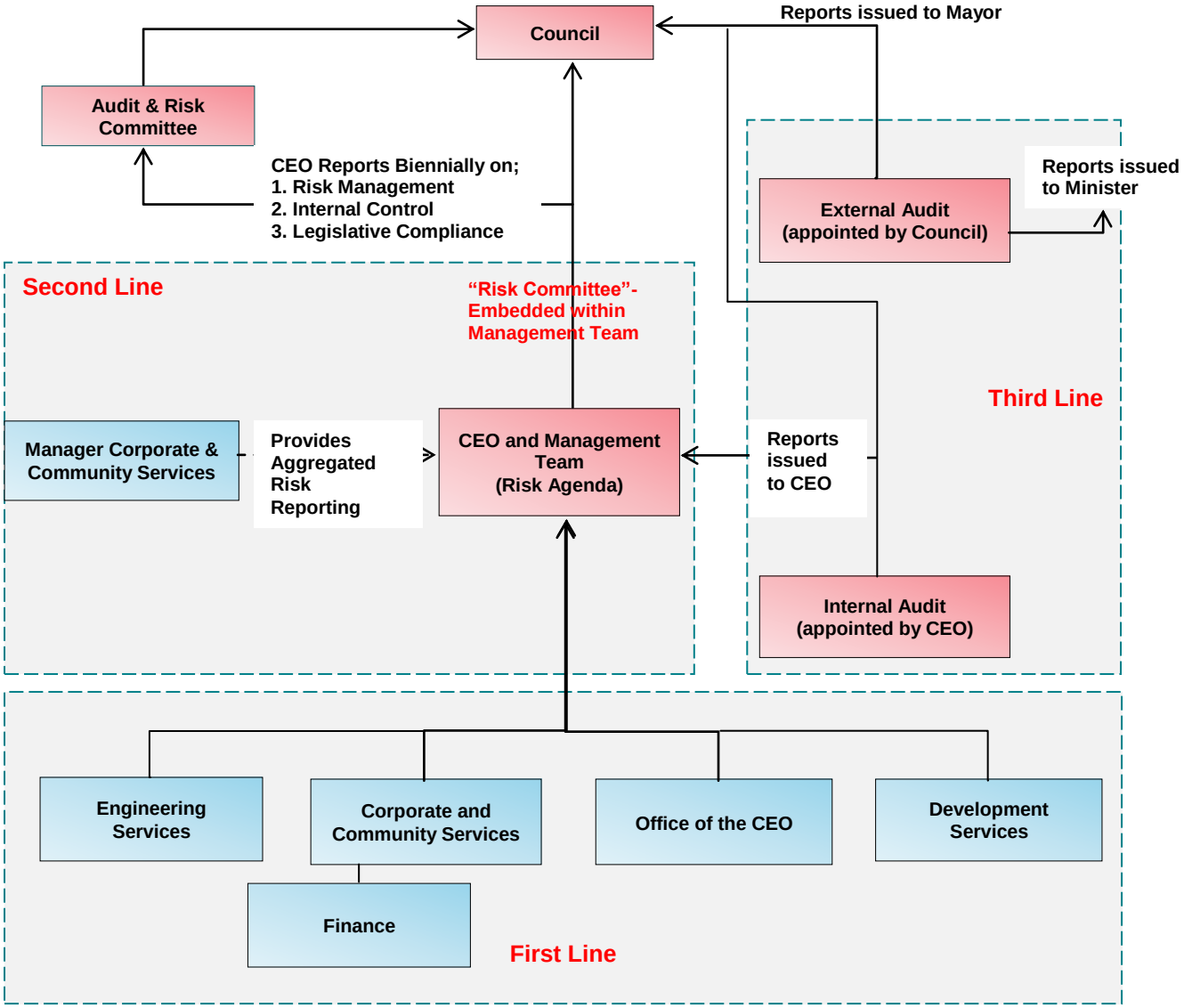
Internal & External Audit are the **'3rd Line'** of defence, providing assurance to the Council, Audit & Risk Committee and Town Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

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 with input from the Audit & Risk Committee.

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

Governance Structure

The following diagram depicts the current operating structure for risk management within the Town.



Town of Cottesloe

Roles & Responsibilities

CEO / Audit & Risk Committee / Council

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

Audit & Risk Committee

- 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 / Management Team

- Liaise with Audit & Risk Committee 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 Town Level.

Manager Corporate & Community Services

- Oversee and facilitate the Risk Management Framework.
- Support reporting requirements for risk matters.

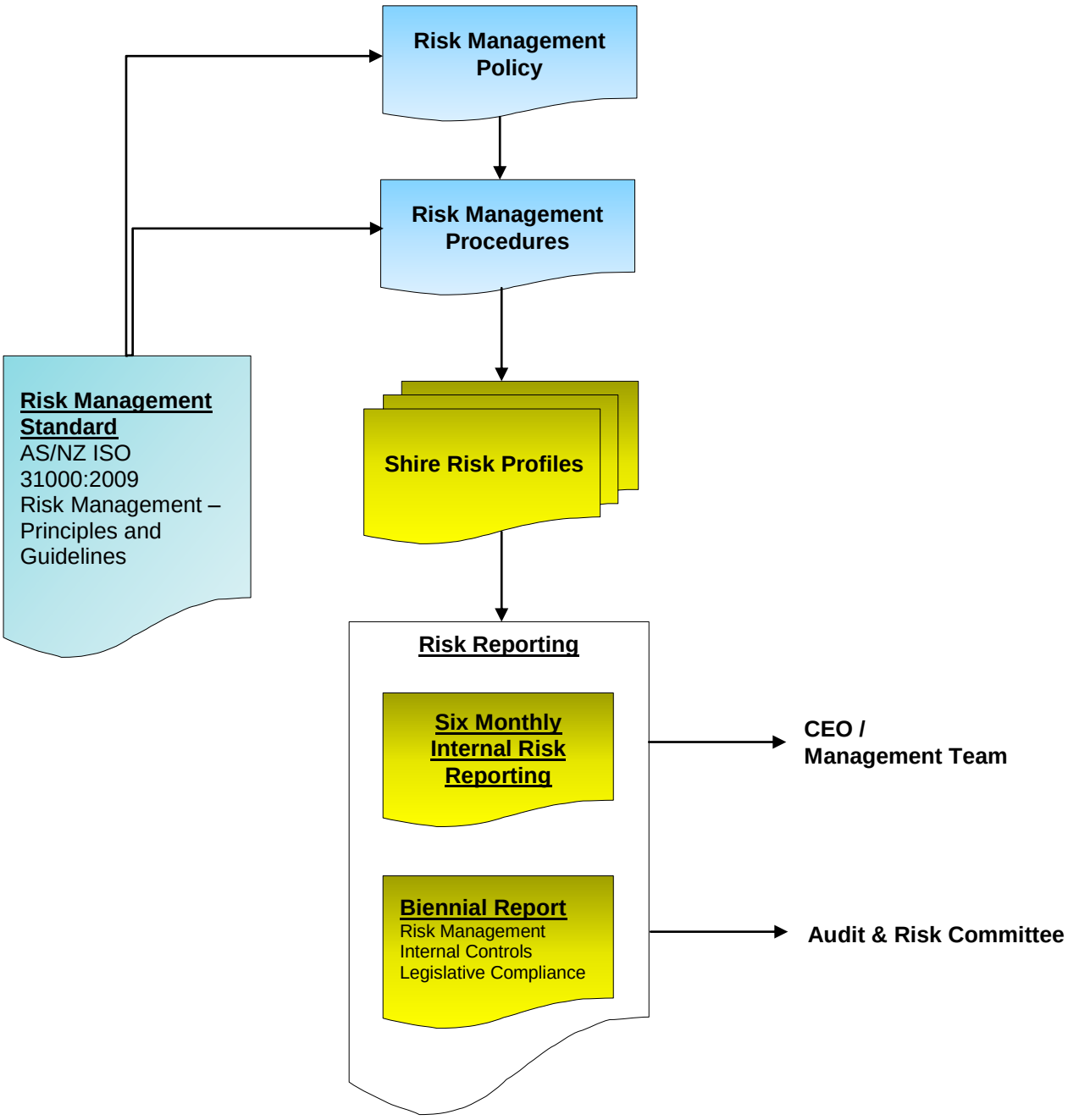
Work Areas

- 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.

Town of Cottesloe

Document Structure (Framework)

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



Risk & Control Management

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

Each Manager, in conjunction with the Manager Corporate & Community Services is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Town.
- 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 AS/NZ ISO 31000:2009 Risk Management, the following approach is to be adopted from a Risk & 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:

Organisational Context

The Town'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 must be approved by the Manager Corporate & Community Services and the 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 Town has been divided into three levels of risk assessment context:

1. Strategic Context

This constitutes the Town'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

Town of Cottesloe

2. Operational Context

The Town'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:

- **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 Town 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 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)

C: Risk Analysis

To analyse the risks, the Town'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 Town 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 systemic nature.

Town of Cottesloe

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 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 Manager Corporate & Community Services 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 Town 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 Manager Corporate & Community Services is to monitor the status of risk treatment implementation and report on, if required.

The CEO & Management Team 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 & Management Team. They will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and appropriate to the Town.

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.

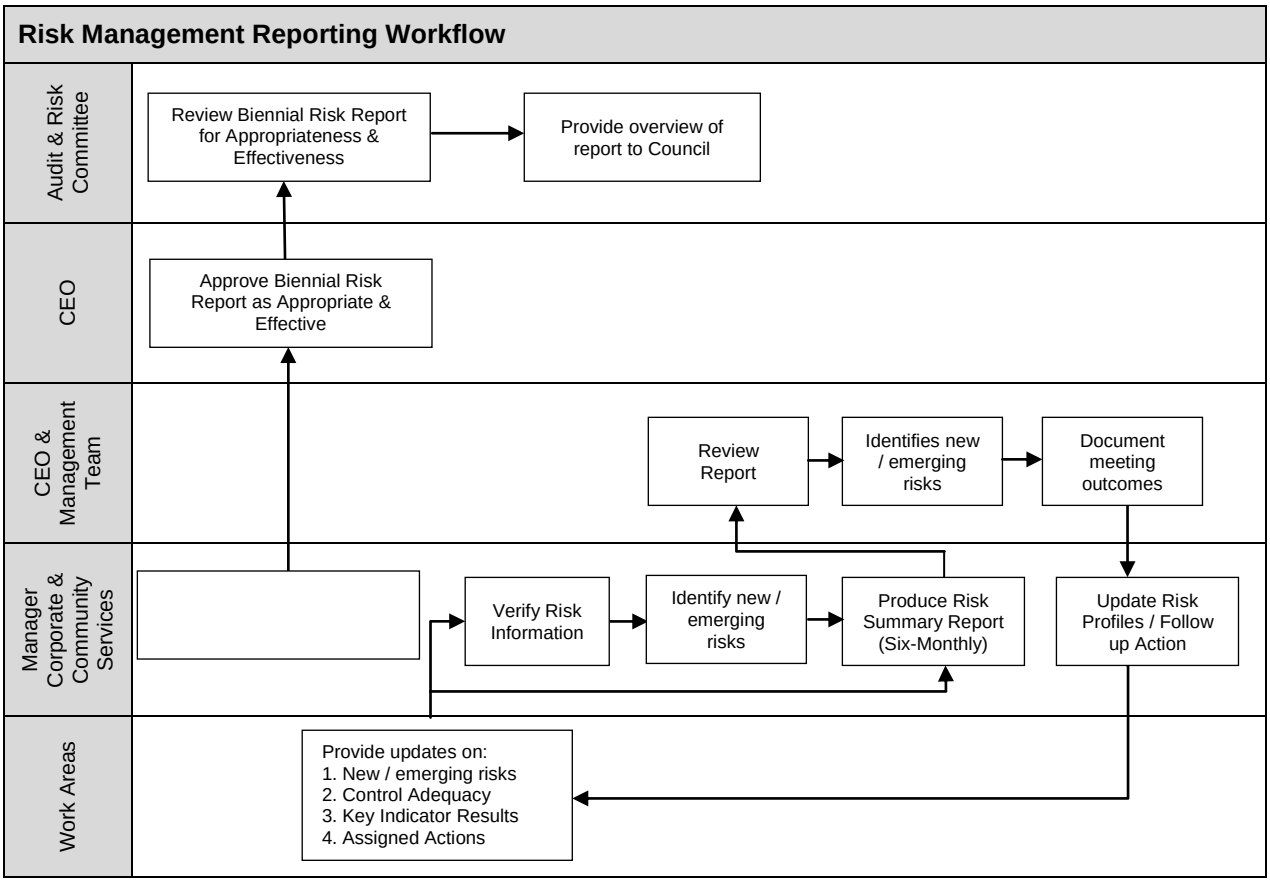
Risk management will be included within the employee induction process to ensure new employees are introduced to the Town's risk management culture.

Town of Cottesloe

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 and emerging risks, control effectiveness and key indicator performance to the Manager Corporate & Community Services.
- Work through assigned actions and provide relevant updates to the Manager Corporate & Community Services.
- Risks / Issues reported to the CEO & Management Team are reflective of the current risk and control environment.

The Manager Corporate & Community Services is responsible for:

- Ensuring Town 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.
- Producing a six-monthly Risk Report for the CEO & Management Team which contains an overview Risk Summary for the Town.
- Annual Compliance Audit Return completion and lodgement.

Town of Cottesloe

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 Control.

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 Town'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 & Management Team where appropriate management actions are to be set and implemented to bring the measure back within appetite.

Monitor & 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.

Town of Cottesloe

Risk Acceptance

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

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.

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 Control Assurance Plan

The annual assurance plan is a monitoring schedule prepared by the Executive Management Team 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 Town'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 Key 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

Town of Cottesloe Measures of Consequence							
Rating (Level)	**Health**	**Financial Impact**	**Service Interruption**	**Compliance**	**Reputational**	**Property**	**Environment**
Insignificant (1)	Near-Miss or First Aid	Less than $5,000	No material service interruption -backlog cleared < 6 hours	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	$5,001 - $15,000	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	$15,001 - $200,000	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)	Long-term disability / multiple injuries	$200,001 - $750,000	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
Extreme (5)	Fatality, permanent disability	More than $750,000	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

Town of Cottesloe 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

Town of Cottesloe Risk Matrix						
Consequence / **Likelihood**		**Insignificant**	**Minor**	**Moderate**	**Major**	**Extreme**
		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)**

Town of Cottesloe 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
MODERATE (5-9)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager
HIGH (10-16)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Director / CEO
EXTREME (17-25)	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

Town of Cottesloe 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*

Controls	Type	Date	Town Rating
List of Key Controls			

Overall Control Ratings:	

Consequence Category	Risk Ratings	Town Rating
	Consequence:	
	Likelihood:	

Overall Risk Ratings:	

Indicators	Tolerance	Date	Overall Town 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

1. **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 to Breach of Authority.

2. **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.

3. **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 (incl 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".

4. **Failure to fulfil Compliance requirements**

➢ Failures 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.

5. **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.

6. 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.

7. 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.

8. Inadequate Environment 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 / Illegal land use.

9. Errors, Omissions, 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”.

10. External theft & fraud (incl 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'.

11. 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 (e.g. cleaning / maintenance)

12. 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".

13. 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.

14. **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

15. **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.

16. **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

Report/Proposal Disclaimer

Every effort has been taken by LGIS to ensure that the commentary and recommendations contained in this communication are appropriate for consideration and implementation by the recipient. Any recommendation, advice and information contained within this report given in good faith and is based on sources believed to be reliable and accurate at the time of preparation and publication of this report. LGIS and their respective officers, employees and agents do not accept legal liability or responsibility for the content of the recommendations, advice and information; nor does LGIS accept responsibility for any consequential loss or damage arising from its application, use and reliance. A change in circumstances occurring after initial inspection, assessment, analysis, consultation, preparation or production of this report by LGIS and its respective officers, employees and agents may impact upon the accuracy and relevance of the recommendation, advice and information contained therein. Any recommendation, advice or information does not constitute legal or financial advice. Please consult your advisors before acting on any recommendation, advice or information within this report.

Proprietary Nature of Report or Proposal

This report or proposal is prepared for the sole and exclusive use of the party or organisation ('the recipient') to which it is addressed. Therefore, this document is considered proprietary to LGIS and may not be made available to anyone other than the recipient or person(s) within the recipient's organisation who are designated to assess, evaluate or implement the content of this report or proposal. LGIS publications may be made available to other persons or organisations only with permission of LGIS.

© Copyright

Echelon Australia Pty Ltd trading as LGIS Risk Management
ABN 96 085 720 056

Level 3
170 Railway Parade
WEST LEEDERVILLE WA 6007
Tel 08 9483 8888
Fax 08 9483 8898

CONTACTS

Michael Sparks BCom, Dip FS, CBCI
Senior Risk Consultant

Tel 08 9483 8820
Mob 0417 331 514
michael.sparks@jlta.com.au