WYONG SHIRE COUNCIL

Enterprise Risk Management Framework

Contents

OVERVIEW

1.1) PURPOSE

This document describes Wyong Shire Council's (WSC) Enterprise Risk Management (ERM) Framework which involves a consistent and structured approach to risk management. Its aim is to assist WSC achieve its business objectives and embed risk management in all business and operational processes.

The ERM Framework provides a basis for identifying and responding to uncertainties so that risk-informed decisions can be made for the achievement of WSC's strategic, operational and project-specific objectives.

The ERM Framework will evolve over time, together with the risk culture underpinning it to ensure:

- committed leadership, with significant risks regularly discussed at Council, executive and senior management levels
- regular reporting and discussion of high-ranked risks
- regular reviews of risk actions to ensure risks are being managed
- regular reviews of the effectiveness of risk treatments
- responsibility for risk management exists throughout WSC
- reviews of successes and failures are used for learning
- risk management is a day-to-day activity throughout WSC

1.2) DOCUMENT STRUCTURE

This document includes:

- an overview of WSC's expectations and approach for managing strategic, operational and project risks

- guidance for implementing the risk management process supporting reference documentation

A separate document describes the steps proposed for implementing the Framework.

1.3) READY REFERENCE

Readers with a good understanding of risk management terminology and concepts, and its application in a local government setting can refer to the following sections for an overview of WSC's ERM Framework:

• Risk Policy	Section 2.1, Attachment 6.5
• Roles and Responsibilities	Section 3.2
• Decision Making and Reporting	Section 3.7
• Risk assessment	Section 5.2, Attachment 6.13
• Risk Responses	Attachment 6.9

1.4) APPLICATION

This document defines a structured approach to risk management that aligns with the requirements of AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines.

It focuses on defining the context within which risk management activities will be undertaken, planning and implementing strategic, operational and project risk assessments, developing treatments, and undertaking risk monitoring and reporting activities.

The ERM Framework document should be used by:

- Directors having responsibility for planning and implementing WSC strategies
- Directors, Managers and Team Leaders responsible for planning and managing operational functions within a Service Unit or across multiple Service Units
- Employees having responsibility for identifying and evaluating project options, and for planning and implementing projects

1.5) WHAT IS RISK MANAGEMENT?

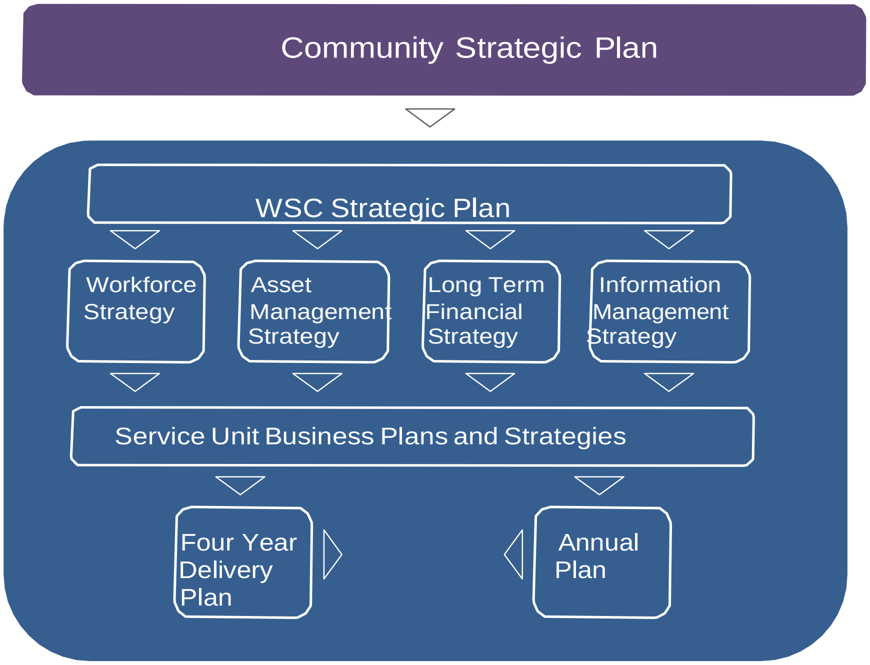
1.5.1) Risk

Risk is defined as “the effect of uncertainty on objectives” where an effect is a deviation from what is expected. Deviations can be either positive (an opportunity) or negative (a threat).

The definition of risk emphasises the need to establish objectives as the basis for risk assessment. WSC’s objectives may be expressed in terms of:

- strategic and operational objectives and key performance indicators defined in documents prepared under WSC’s Integrated Planning and Reporting Framework
- objectives defined within Service Unit Business Plans
- project-specific objectives defined within business cases and project plans
- objectives implicit within WSC’s policies

The following figure shows the hierarchy of WSC’s key strategic and planning documents. These are the sources of objectives against which to identify and manage risks.


Community Strategic Plan
WSC Strategic Plan
Workforce Strategy
Asset Management Strategy
Long Term Financial Strategy
Information Management Strategy
Service Unit Business Plans and Strategies
Four Year Delivery Plan
Annual Plan

The concept of risk has two elements: the likelihood of a risk event occurring and the consequences if it does.

1.5.2) Risk Management

Risk management is defined as “the coordinated activities to direct and control an organisation with regard to risk”.

Risk management involves a structured approach that provides consistent, timely, valuable and integrated information about risk as a basis for effective decision making.

Risks should not necessarily be avoided. Managed effectively, risks enable WSC to pursue opportunities for improving its services, business practices and project outcomes.

Good risk management is based on a logical, comprehensive, documented strategy. By itself, a risk management strategy does not manage risks. Leadership, effort by all levels of management and staff, and monitoring of its application and effectiveness are needed to make the strategy a success.

Communication and consultation about risks and risk management are important at each stage of the risk management process.

A consultative approach involving relevant stakeholders should be used to define the context for and inputs into a risk assessment. Such involvement gives confidence that all relevant risks will be identified (promoting ownership of the risk assessment outcomes), and an understanding of the risk assessment plan and support for the risk controls.

Effective risk communication ensures that those responsible for implementing risk management and those with an interest in the outcomes understand the basis on which risk management decisions are made and why particular actions are required.

The focus of this document and the accompanying implementation plan is on embedding a risk management philosophy into organisational planning activities and decision making, and providing tools to support the process.

1.5.3) Enterprise Risk Management

Enterprise risk management involves embedding risk thinking and risk actions into WSC's everyday activities.

A risk management framework is defined as the "set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation".

1.6) WHY IMPLEMENT RISK MANAGEMENT?

The Local Government Act 1993 was enacted before enterprise risk management was a widely accepted element of good governance. While there is no specific reference to risk management in the Act, it is implicitly required for efficiency, effectiveness and oversight.

The Division of Local Government, in some of its publications, identifies enterprise risk management as ... an essential part of effective corporate governance.

Effective risk management results in fewer surprises and unanticipated negative events.

Whilst there is no such thing as a risk-free environment, many risks can be avoided, modified or shared through good risk management practices.

Within a whole-of-government risk context, councils often face risks that influence other risks. These links between risks are important – a risk may not look significant in isolation, but could be significant when its flow-on effect is considered.

As whole-of-government approaches become more common, state-sector risks – in other words, risks that affect the state as a whole – are becoming better understood and can therefore be better managed in a local context.

Councils will increasingly need to understand state-sector risks, and work with other levels of government to manage them. There are three types of state-sector risk, each of which calls for a different response:

- council-level risks can become risks to the state because of their size or significance, because of the wider impact of measures to manage them, or because of poor management by councils

- inter-agency risks which, if unmitigated by one agency, become risks for other agencies (such as the link between meeting the educational and social needs of teenagers and anti-social behaviour)
- state wide risks which are beyond the boundaries of any one council and call for responses across councils, often coordinated by a central agency (such as bushfires, floods and other emergencies)

Within the Wyong Shire Council context, this ERM Framework supports WSC's vision to be an organisation of excellence in local government in Australia.

The benefits that can be expected from the effective implementation and application of an enterprise risk management approach include:

- understanding risks that might affect goals and objectives
- understanding WSC's risk exposure
- identifying and managing threats and opportunities
- moving to more proactive risk responses
- improving the basis for decision-making
- achieving an organisational culture where people understand risks associated with their roles, and their responsibilities in relation to them

1.7) TYPICAL LOCAL GOVERNMENT RISKS

There are a number of risks that are common to the local government sector. These include risks relating to governance, planning and regulation, assets and finance, community, consultation, and workforce.

WSC's significant capital works program also exposes it to project risks, including program (time), cost, safety, scope, fitness for purpose, and environmental.

See Attachments 6.2 and 6.3 for some common local government and project risks.

1.8) RISK MANAGEMENT PRINCIPLES

AS/NZS ISO 31000:2009 Risk management - principles and guidelines identifies 11 principles that underpin effective risk management, emphasising the need for risk management to:

a) create and protect value

b) be an integral part of all organisational processes

c) be a part of decision making

d) explicitly address uncertainty

e) be implemented in a systematic, structured and timely manner

f) use the best available information

g) be tailored to meet WSC's specific needs

h) take human and cultural factors into account

i) be transparent and inclusive

j) be dynamic, iterative and responsive to change

k) facilitate continual improvement

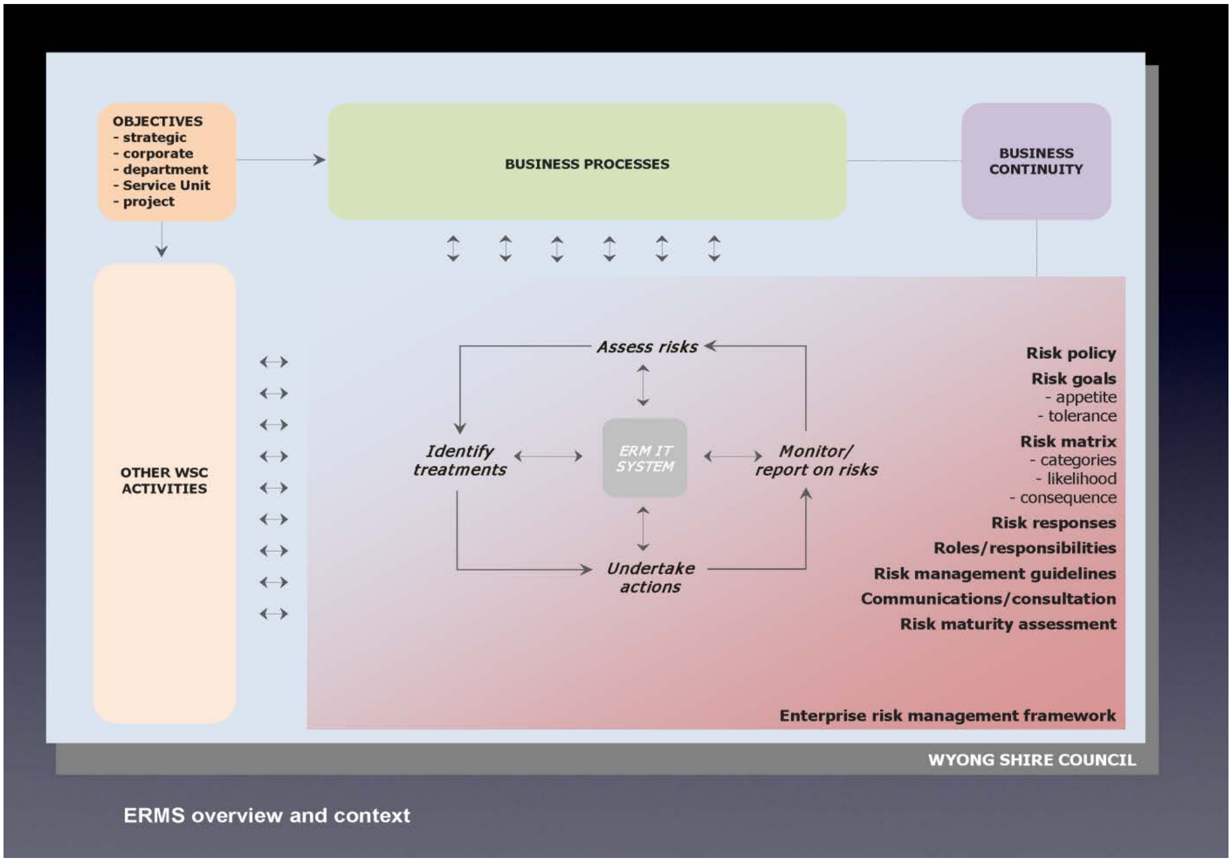
WSC's ERM Framework responds to each of these principles (refer to Attachment 6.4 for details of the responses).

1.9) WSC's STRATEGIC CONTEXT

ERM is not a stand-alone system or process or series of activities.

Whilst ERM involves a number of activities to develop and implement, the goal is to fully integrate risk management into everyday planning and everyday activities throughout the organisation.

The following diagram illustrates the context within which the ERM Framework elements operate relative to WSC's business.



OBJECTIVES
- strategic
- corporate
- department
- Service Unit
- project

BUSINESS PROCESSES

BUSINESS CONTINUITY

OTHER WSC ACTIVITIES

Assess risks

Identify treatments

ERM IT SYSTEM

Monitor/ report on risks

Undertake actions

Risk policy

Risk goals
- appetite
- tolerance

Risk matrix
- categories
- likelihood
- consequence

Risk responses

Roles/responsibilities

Risk management guidelines

Communications/consultation

Risk maturity assessment

Enterprise risk management framework

WYONG SHIRE COUNCIL

ERMS overview and context

1) WSC'S RISK POLICY

2.1) COMMITMENT

WSC is committed to effectively and systematically managing risks in order to maximise opportunities and limit adverse effects, and will achieve this by (amongst other things):

- assigning clear responsibilities to staff at all levels for managing risk
- embedding risk management controls into business processes

2.2) RISK POLICY

WSC's risk policy underpins the ERM Framework (see Attachment 6.5). All WSC staff are

expected to have knowledge of and to comply with the WSC risk policy.

2.3) ALIGNMENT WITH OTHER POLICIES AND SYSTEMS

The ERM Framework interfaces with and, in some instances, complements the following elements of WSC's control framework.

2.3.1) WSC's Internal Audit Program

Strategic, operational and project risk assessments will provide inputs to inform planning of WSC's internal audit program.

WSC's internal audit function will conduct independent reviews of the ERM Framework's performance and operation.

2.3.2) Audit and Risk Committee

Information regarding WSC's risk exposure and the operation of the ERM Framework will be provided annually to the Audit and Risk Committee for review.

2.3.3) Work Health and Safety Risks

WSC has developed its WHS system to manage WHS risks and includes separate policy, procedures and reporting mechanisms to those outlined in this document.

2.3.4) Environmental Management System

WSC is currently developing an Environmental Management System. It will provide a set of tools (including training) to help staff make informed decisions on minimising impacts on the natural environment from WSC activities and facilities, and those activities undertaken on behalf of WSC.

2.3.5) Business Continuity Risks

An element of WSC's risk management strategy is the maintenance of an effective Business Continuity Plan (BCP).

WSC has developed a BCP to:

- identify critical aspects of WSC services exposed to risk from business interruption

- define preparatory actions which will minimise loss or damage should an interruption occur

- define response strategies to maintain or reinstate critical WSC services through periods of disruption

- minimise adverse effects on the public, employees and WSC

2.3.6) WSC’s Insurance Program

WSC has an obligation under section 382 of the Local Government Act 1993 (NSW) to hold adequate public liability and professional indemnity insurance coverage.

WSC has a suite of insurances in place to mitigate direct pecuniary loss. Its purpose is to reduce WSC’s business exposure against risks which cannot otherwise be effectively mitigated, and are normally accidental in nature or involve an unexpected calamity or incident.

2.4) INTEGRATED PLANNING AND REPORTING FRAMEWORK

WSC has a tiered structure of externally and internally focused strategies that align with the NSW Division of Local Government’s Integrated Planning and Reporting framework.

These documents identify strategic objectives and community outcomes, operational objectives, and key performance indicators that establish the primary basis for strategic and operational risk assessment across WSC.

2) ENTERPRISE RISK MANAGEMENT

3.1) SCOPE

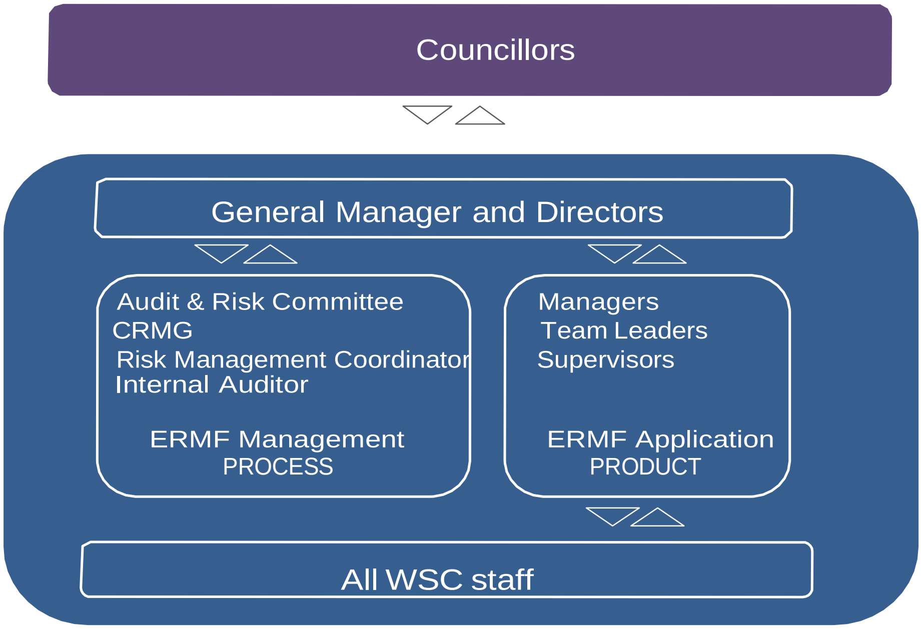
Risk management can and should be applied to all decision points and at all levels of planning and operations including the following:

- strategic planning
- policy formulation
- financial planning
- asset management
- procurement processes
- ethics, fraud and probity issues
- project management
- professional advice
- conducting physical works
- workforce planning

- organisational change
- business interruption preparedness
- health and safety activities
- audit
- information technology planning

3.2) ROLES AND RESPONSIBILITIES

The following diagram illustrates the different roles involved in risk management in WSC, and the table provides details of risk management responsibilities. Relevant sections can be used in new and revised position descriptions to incorporate ERM roles, responsibilities and expectations.



Column A of the below table contains the Role and Column B contains the responsibilities for that role.

Role	Responsibilities
Council	• Adopt WSC's ERM Framework, comprising the ERM Strategy and Policy. • Set priorities for the implementation of the ERM Framework to maximise value to WSC. • Provide direction regarding responses to strategic, operational and project risks, as required.
General Manager, Directors	• Lead the development of an ERM culture across WSC. • Promote a culture that encourages the open and transparent discussion of risk. • Ensure the effective implementation and operation of WSC's ERM Framework and provide direction to the ERM Committee. • Define and communicate WSC's risk appetite and tolerance. • Assess and manage strategic risks (in other words, those with a whole-of-organisation impact). • Monitor high-ranked risks associated with strategic projects. • Monitor high-ranked operational risks. • Monitor high-ranked project risks. • Nominate risk owners for all high-ranked risks. • Provide direction regarding responses to strategic, operational and project risks. • Provide responses/direction in response to reports and recommendations provided by the ERM Committee. • Provide information to the Audit and Risk Committee regarding WSC's risk exposure and the operation of the ERM Framework. • Resolve urgent, sensitive, complex or council-wide risk management issues that cannot be resolved by staff. • Approve Service Unit Business Plans, Business Cases and Project Plans – defining planned strategies for managing service and project risks.
Managers	• Promote risk culture. • Ensure that the ERM Framework is being effectively implemented and operated within their areas of responsibility. • Participate in operational and project risk assessments. • Manage risks within Service Units. • Develop strategies to manage operational risks. • Report high-ranked and changed operational risks monthly to the Director. • Escalate risks to a Director for resolution (as appropriate).
Project Managers	• Assess and manage project risks. • Develop strategies to manage project risks. • Ensure the effective management of risks within the project team to support the achievement of project objectives. • Escalate risks to the Project Control Group, the Project Sponsor, Director or General Manager (where required).
Team Leaders, Supervisors	• Promote risk culture. • Manage risks within functional areas. • Contribute to the development of Service Unit Business Plans (where required). • Escalate risks to Managers or Directors to support the achievement of operational objectives (where required).
Audit and Risk Committee	• Provide independent assurance and advice to Council on risk management, control, governance, and external accountability responsibilities as defined in the Committee's terms of reference.

Role	Responsibilities
Risk Management Coordinator	• Provide specialist risk management support and training to staff to ensure a consistent risk management approach across WSC. • Facilitate the progressive implementation of the ERM Framework and the development of a risk-aware culture. • Promote the communication of risks within and between WSC's various Service Units and Departments. Coordinate day-to-day risk management activities across WSC. • Maintain WSC's risk database in a consistent and accessible form – providing consistent information as a basis for effective risk management across WSC. Identify opportunities for improvement of the ERM Framework. • Review ERM implementation and operational effectiveness and provide associated reports and recommendations to the ERM Committee. • Ensure the ERM Framework is being effectively implemented and operated within their areas of responsibility. • Undertake or arrange a periodical risk maturity assessment. • Plan further ERM training, development etc based on the results of the maturity assessments.
CRMG	• Plan and facilitate the progressive implementation of the ERM Framework and the development of a risk-aware culture. • Establish and monitor key performance indicators for the implementation and operation of the ERM Framework. • Report quarterly to the General Manager and Directors regarding the performance of the ERM Framework. • Identify training and development needs to achieve the required risk management competencies across WSC. • Coordinate resources to support the implementation of the ERM Framework. • Facilitate the formal review and update of the ERM Framework. • Promote the ERM Framework across WSC.
Internal Audit	• Consider the risk management framework in planning and conducting audits. • Provide advice and assurance over WSC's risk management and internal control frameworks.
All staff	• Act at all times in a manner consistent with WSC's ERM Framework. • Take practical steps to manage WSC's risk exposure within their area of activity and responsibility, including the identification of emerging risks and opportunities. • Notify or escalate information about risks and opportunities to ensure effective and timely responses. • Identify emerging risks requiring attention. • As risk owners, take responsibility for the effective management of specific risks as nominated in WSC's risk IT system.

3.3) RISK TYPES

There are two fundamental types of risk:

- the first, which the balance of this document addresses, are those risk events that are capable of analysis using a reasonably known or predictable likelihood and consequence to give a risk score that represents the organisation's exposure

- the second are those events that may have catastrophic consequences but for which no reliable likelihood estimates are available

There are two subsets to the second group:

- a risk event for which the consequences can be contemplated but for which not enough information exists to make predictions about likelihood

- an "unknown" risk event is one that has not been considered previously and probably not even thought about (sometimes referred to as black swan events because, like the discovery of black swans in Australia by European explorers, they had never before been contemplated but were entirely reasonable in hindsight)

The only counter to the second category of risks – those with unknown or unknowable likelihoods – is to have comprehensive contingency and emergency response plans.

3.3.1) Strategic and Corporate Risks

There are two types of risks that fall into this category.

Strategic risks and corporate vulnerabilities inform strategic decision making, and provide an input for WSC's risk-based internal audit program.

Strategic risk and corporate vulnerability assessments will require review and updating at regular intervals to take into account changes to WSC's external and internal environments or when significant changes occur e.g.

- significant organisational change (e.g. restructuring, council elections, or appointment of a new General Manager or Director)

- significant changes to WSC's strategic commitments (e.g. significant revisions to the Community Strategic Plan)

3.3.1.1) Corporate Risks

These risks relate to the organisation as a whole, and the vulnerability of its functions and activities to internal and external risk events. They include not only whole-of-organisation risks but also:

- high-ranked operational risks that are escalated because of their potential for impact beyond a service or business unit

- high-ranked project risks that are escalated because of significance (e.g. reputation), value (e.g. financial exposure) or other potential impact.

A Strategic Risk Profile was developed that assessed the impacts of a range of risk events on day-to-day council activities. The assessment was undertaken in the absence of any existing risk controls being applied, to give a “total vulnerability” picture of WSC’s risk exposures (a similar approach would normally be taken when assessing levels of insurance coverage to ensure that total capability could be reinstated).

WSC’s initial Strategic Risk Profile is included in Attachment 6.7.

3.3.1.1) Strategic Risks

Strategic risks are those risks having a potential impact on the achievement of WSC’s strategic objectives which are defined in:

- Community Strategic Plan
- WSC Strategic Plan
- Four Year Delivery Plan
- Annual Plan
- related plans and strategies

3.3.1) Operational Risks

Operational risks are associated with WSC’s core operational functions, whether customer-focused functions or internal supporting functions. They can relate to a single service unit, such as library services or enabling activities, such as ICT or Learning and Development.

Operational risks derive from service objectives defined in:

- Workforce Strategy
- Asset Management Strategy
- Long Term Financial Strategy
- Information Management Strategy
- Service Unit Business Plans

Directors are responsible for ensuring that operational risk assessments are planned and completed to align with the annual planning and reporting cycle.
Monitoring and review of operational risks should be undertaken by Managers on a monthly basis and discussed with their Directors.

Where high-ranked operational risks are identified that have a potential impact beyond the business unit, they should be referred to the Service Unit Manager of the affected business unit in the first instance, and only escalated to the General Manager and Directors if the matter cannot be resolved between Managers and/or Directors.

Example operational risks include:

- failure to plan and/or maintain council assets
- non-compliance with safety standards resulting in injury, loss of critical plant, fines or business delays
- loss of a major asset
- system interruption
- industrial action
- financial failure of a council contractor
- financial
  - ➢ risks associated with financial controls, systems and procedures, including but not limited to procurement, fraud and corruption
  - ➢ risks related to funding (rates/charges/grants and other revenue), liquidity and credit exposures
- environmental
  - ➢ climate change risks to WSC’s operations and service delivery
  - ➢ environmental hazards affecting human health or the environment
  - ➢ disasters affecting the natural environment (beyond human control/intervention)
- legal, regulatory and compliance
  - ➢ risks associated with meeting compliance and governance frameworks
  - ➢ liability risks associated with harm or damage incurred in the course of undertaking WSC’s business
  - ➢ risks associated with the damage to or loss of property or an impact on its use
  - ➢ injury risks to third parties
- Reputation
  - ➢ risks associated with negative publicity regarding WSC's business practices or service delivery
  - ➢ risks such as civil disruption or community dissatisfaction

3.3.1) Project Risks

Project risk assessment should be undertaken during each phase of the project investment life cycle to inform procurement, stakeholder consultation, communication strategies, project resourcing, and cost and time contingency provisions.

Each project plan should include the objectives, scope and timing of risk assessments to be completed at the different project phases.

Comparative risk assessment can assist in the evaluation of alternatives where more than one option or alternative exists.

Project risk management activities include:

- high level risk assessments at concept and options development
- identification of high-ranked project risks within business cases to inform the investment decision
- risk assessment reviews coinciding with project milestones
- project-specific risk monitoring and treatment plans
- monthly reports by the Project Manager providing details of the status of project risks (stable, changing, etc) and treatment actions

3.4) RISK APPETITE

Risk appetite is a critical component of an effective ERM Framework.

Risk appetite defines the type and how much risk that WSC is prepared to take or to retain in pursuit of its objectives. Expressed differently, it describes where WSC “wants to be most of the time” in relation to its risk exposure.

By making risk appetite explicit, the expected or business as usual operating parameters for risk management established by the General Manager and Directors are available to guide staff (see Attachment 6.8 for details of the WSC risk appetite).

WSC’s risk appetite (and any tolerance statements developed in the future) should be reviewed at least annually, and updated as required.

Risks can be categorised according to the goals, objectives and outcomes defined in WSC’s strategic, management and business plans or, more usually, according to a series of generic groupings that apply to one or more objectives and outcomes.

3.5) RISK CATEGORIES AND RISK TABLES

WSC’s current risk categories are:

- Work Health and Safety

- Socio-economic
- Regulatory/compliance (including Environment, Cultural Heritage)
- Reputation
- Financial
- Business Continuity

See Attachment 6.9 for WSC's current Risk Tables which includes various degrees of severity against each risk category to assist in judging the impact of the risk event.

3.6) RISK RESPONSES

Risk responses are those actions to be taken once risk assessment is complete. They represent the "business rules" for the management of risk following risk assessment.

Risk responses include:

- mandatory or optional development of risk treatments
- mandatory or optional assessment of post-treatment residual risk
- level of escalation for decision making about the acceptability or otherwise for high-ranked risks, and what subsequent actions are required
- mandatory or optional assignment of a risk owner

See Attachment 6.10 for WSC's current risk responses table

Risk treatment options are actions over and above existing controls and can include:

- avoiding the risk by deciding not to undertake the activity giving rise to the risk
- taking or increasing the risk in order to pursue an opportunity
- removing the risk source
- changing the likelihood
- changing the consequences
- sharing the risk with another party or parties (including contracts, insurance and risk financing)
- retaining the risk by informed decision and conscious acceptance

3.7) RISK-BASED DECISION MAKING AND REPORTING

Risk-related decisions should be made at the lowest appropriate level within the organisation. Column A lists the action, Column B describes the action, Column C the responsibility and Column D the timing.

Action	Description	Responsibility	Timing
Operational risk assessments	Undertake comprehensive risk assessment based on Service Unit objectives; record results in WSC's risk database; escalate high-ranked risks for decision (based on Risk Responses table)	Service Unit Managers	Annual (for SUBPs); significant change
Project risk assessments	Undertake comprehensive risk assessment based on project objectives; record results in WSC's risk database; escalate high-ranked risks for decision (based on Risk Responses table)	Project Managers	Business Case (preliminary); project commencement; significant change
Strategic risk assessments	Undertake comprehensive risk assessment based on WSC's community and strategic objectives; record results in WSC's risk database; escalate high-ranked risks for decision (based on Risk Responses table)	General Manager and Directors or delegate	New CSP or Strategic Plan; significant change
Operational risk reviews	Review current risks and update for any changes; update treatment actions; identify/assess any new or emergent risks; record changes in WSC's risk database; report/discuss new, changed and high-ranked risks and any proposed new treatments with Director; escalate further if warranted	SUMs	Monthly; significant change
Project risk reviews	Review current risks and update for any changes; update treatment actions; identify/assess any new or emergent risks; record changes in WSC's risk database; report/discuss new, changed and high-ranked risks and any proposed new treatments with Director; escalate further if warranted	Project Managers	Monthly; significant change
Strategic Risk Profile review	Review WSC's vulnerability; record results in updated WSC Strategic Risk Profile	General Manager and Directors or delegate	Annual; significant change

Only where such decision making is beyond the authority of an individual or the risks require escalation for other reasons (see Risk Responses above) should they be passed up the line, and they should only go as far as needed for an authoritative decision.

The progression is most likely to be (remembering that it can start anywhere along the sequence): team member -7 supervisor -7 team leader -7 Service Unit Manager -7 Director -7 General Manager and Directors -7 Council.

Consistent, comprehensive and timely risk reporting is essential to provide management with the details of risks that need to be managed, monitored or require decisions.
The following table summarises the key ERM Framework actions, reports and reviews required for strategic, operational and project risks.
Column A lists the action, Column B the description, Column C the responsibility and Column D the timing.

Action	Description	Responsibility	Timing
Review of escalated operational or project risks	Review high-ranked risks referred from operations or projects; monitor the status of risk treatments already agreed; decide and advise treatment or other actions to be taken for newly referred risks; update WSC’’s risk database	General Manager and Directors or delegate	Monthly (or when received for high priority risks)
Plan internal audit program	Review strategic, operational and project risks as an input to planning WSC’s internal audit program	General Manager and Directors or delegate	Annual
ERM Framework review	Review ERMF use, operation, application, documentation, systems, etc; identify improvement opportunities (changes, additions, training, etc); report to General Manager and Directors	ERM Committee	Quarterly

3.8) ORGANISATIONAL RISK ENVIRONMENT

3.8.1) Risk Communication and Culture

Embedding risk management into WSC’s everyday work culture is fundamental to achieving the benefits and outcomes of integrated risk management. This will be accomplished by (amongst other things):

- Directors and Managers championing risk management behaviours and actions
- promoting and reinforcing the view that all staff are managers of risk
- encouraging staff to develop knowledge and skills in risk management
- including risk management in WSC’s induction program and ongoing learning and development program
- providing targeted training and support to staff so that risk management practices are effectively incorporated into their everyday roles and responsibilities

WSC recognises that a proactive risk management culture is desirable in order to be able to respond to unexpected events (and hence the involvement of all staff).

An organisational culture that supports effective risk management is one where:

- a “no surprises” rather than “no risks” philosophy is encouraged
- individuals can identify and respond to risks without fear of retribution
- individuals can challenge and debate risk responses in a constructive manner
- there is a common risk language that facilitates clear and consistent discussion of risks affecting the entire organisation

3.8.1) Potential ERM Pitfalls

There are many articles and forums that describe pitfalls that can undermine the effective implementation and operation of an ERM framework.

The following examples are provided as a checklist of things to avoid:

- risk management should not have a “tick the box” focus
- risk management occurs in silos, without consideration of the organisational context or impacts elsewhere in the organisation
- risk management activities are not clearly linked to strategic, operational and project goals and objectives
- risk events are not well described, limiting or precluding proper likelihood and consequence analysis
- risk events that overly focus at the micro level (often missing significant “higher-order” risks)
- risk events that overly focus at the macro level (often missing detail for which meaningful risk treatments should be developed)
- poor visibility and integration of risk policies and procedures
- poor internal communication about risk

3.9) CONTINUOUS IMPROVEMENT

3.9.1) Risk Maturity

One way of monitoring an ERM Framework is via a risk maturity assessment tool that provides a snapshot of current skills, knowledge, culture, processes and systems for risk management, measured around the following attributes:

- management of change
- organisational learning
- control environment
- management accountability
- core organisational process
- strategic alignment
- risk and control management performance
- contingency management

The results of the initial WSC maturity assessment provided an important foundation for the development of the ERM Framework because they:

- identified gaps in risk management processes, capacity and culture
- identified relative strengths and weaknesses in risk management performance across different functions within WSC
- identified variations in perceptions between different groups within WSC
- established a baseline for assessing changes over time

See Attachment 6.6 for WSC's current risk maturity assessment report.

3.9.2) Continual Improvement

The ERM Committee will set ERM Framework performance goals and measures. It will review the Framework against them, and may recommend modifications to processes, systems, resources, capabilities and skills that will enhance its operation and/or outcomes.

Improvement will be achieved through the following (and shared on the intranet):

- responses to internal and external audit findings and recommendations
- responses to advice and directions from the Audit and Risk Committee and General Manager and Directors
- responses to opportunities for improvement identified as a result of risk maturity assessments
- through the ongoing review of successes and failures

3) KNOWLEDGE MANAGEMENT

4.1) REFERENCES AND FURTHER INFORMATION

Sources used in developing this document are included in Attachment 6.10 and cover risk principles and practices relevant to councils. It also includes a number of references recommended by the Division of Local Government for those seeking a deeper understanding of risk management principles and practice (see Attachment 6.11).

4.2) TRAINING

Three levels of risk training have been defined to support WSC's ERM Framework, as follows:

- Level 1 – risk management overview, basic terminology and concepts, expectations around roles (basically for anyone that does not fall into any of the subsequent categories and as part of the induction package for new starters)

- Level 2 – for regular users and participants in risk management activities, risk managers, risk owners and treatment owners

- Level 3 – practitioners, risk champions, and ERM subject matter experts.

Each of the above levels assumes knowledge and understanding of the preceding levels.

The broad topical coverage for each level of training includes:

- Level 1 – overview/familiarisation
    - understand basic risk management terminology
    - understand basic risk responsibilities, including reporting, alerts and escalation
    - understand WSC's ERMS goals
    - understand WSC's risk management context and risk appetite
    - understand the benefits of good risk management
    - understand objectives (as the basis for risk assessment)
    - understand risk assessment techniques
    - understand WSC's risk tables – risk categories, use of likelihood and consequence to determine risk rating, responses to risk rating
    - understand changes in risk environment over time

- Level 2 – risk user/risk manager/risk and treatment owners
    - risk perception and analysis
    - risk management principles
    - risk identification processes
    - risk analysis techniques
    - development, selection and implementation of treatments
    - risk communication

- Level 3 – practitioner, subject management expert
    - manage strategic and organisational risk
    - manage enterprise risk management system
    - engage stakeholders
    - facilitation techniques
    - risk assessment techniques
    - establish risk context
    - team effectiveness
    - facilitate development of risk organisation culture
    - identify changing risk management requirements across the organisation
    - contribute to risk management education and training
    - identify risk solutions, and communicate outcomes
    - develop quality organisation risk management systems and processes
    - facilitate implementation and monitoring of continuous
    - improvement in all aspects of risk management across the organisation.

Levels 1 and 2 training are available within WSC, whilst Level 3 training will be undertaken externally.

4) RISK MANAGEMENT PROCESSES

5.1) GENERAL APPROACH

This document describes WSC’s ERM Framework as it applies to strategic, operational and project risks, and must be used by everyone having responsibility for or an involvement in risk management including:

- Directors having responsibility for planning, implementing and monitoring WSC strategies
- Directors, Managers and Team Leaders responsible for planning and managing products and services within a Service Unit or across multiple Service Units
- personnel contributing to or having responsibility for planning and implementing projects

The process map included at Attachment 6.12 outlines the people, processes and outcomes for managing strategic, operational and project risks.

5.2) RISK IDENTIFICATION, ASSESSMENT AND ACTION

Attachment 6.13 describes the complete risk management process for strategic, operational and project risks.

Related documents include:

- Attachments 6.2 and 6.3 – common council and project risks
- Attachment 6.1 – risk terminology
- Attachment 6.13 – the risk register template (database) in which details of risk events, scores, treatments and actions are recorded
- Attachment 6.8 – the risk tables used to determine likelihood and consequence scores and an overall risk score
- Attachment 6.9 – risk responses based on overall risk score

5) ATTACHMENTS

The intention is that the following attachments will be excised from this document and for stand-alone references on the WSC intranet. They are included here to give the reader the ERM Framework in a single document.

6.1) GLOSSARY

Column A contains the Term, Column B the definition and comments and Column C the source

Term	Definitions/Comments	Source
Council	Wyong Shire Council's elected representative	
council	Wyong Shire Council	
consequence	Outcome of an event affecting objectives Note: An event can lead to a range of consequences. A consequence can be certain or uncertain and can have positive or negative effects on objectives. Consequences can be expressed qualitatively or quantitatively. Initial consequences can escalate through knock-on effects.	ISO Guide 73:2009 Risk management - Vocabulary
enterprise risk management	A process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.	Committee of Sponsoring Organizations of the Treadway Commission
likelihood	Chance of something happening Note: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).	ISO Guide 73:2009 Risk management - Vocabulary
potential exposure	The total plausible maximum impact on an organisation arising from a risk without regard to controls Note: The term "inherent risk" is sometimes used as an alternative to risk exposure.	HB 158 - 2010, Delivering assurance based on ISO 31000:2009 Risk management - Principles and
residual risk	Risk remaining after risk treatment	AS/NZS ISO31000:2009

Term	Definitions/Comments	Source
risk	Effect of uncertainty on objectives Note: An effect is a deviation from the expected, whether positive or negative. Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, operational and project objectives).	AS/NZS ISO31000:2009 Risk management - Principles and Guidelines
risk appetite	The amount and type of risk an organisation is prepared to pursue or take Note: Risk appetite is about the pursuit of risk and what the organisation does (or does not) want to do, and how it goes about it.	ISO Guide 73:2009 Risk management - Vocabulary
risk assessment	The overall process of risk identification , risk analysis and risk evaluation	ISO Guide 73:2009 Risk management - Vocabulary
risk category	A class or group of risk events based on their risk consequence. Note: Risk categories are used by WSC to classify risk events as a basis for risk management (including risk reporting, and risk management decision making)	
risk event	an occurrence or change of a particular set of circumstances Note: An event can be one or more occurrences, and can have several causes. An event can involve something not happening. An event can sometimes be referred to as an “incident” or	ISO Guide 73:2009 Risk management - Vocabulary
risk management	Coordinated activities to direct and control an organisation with regard to risk	ISO Guide 73:2009 Risk
risk owner	Person or entity with the accountability and authority to manage a risk	ISO Guide 73:2009 Risk management - Vocabulary

Term	Definitions/Comments	Source
risk source	An element which alone or in combination has the intrinsic potential to give rise to risk Note: The term 'risk source' means a tangible or intangible element that alone or in combination has the intrinsic potential to give rise to risk. It is thus an encompassing term that includes the terms 'hazard' (a source of potential harm) and 'environmental aspect'. An activity may be a source of risk. A source of risk may also be a change in circumstance, for example, an increase in the average temperature that may cause damage to some species but enhance the habitat of others.	ISO Guide 73:2009 Risk management – Vocabulary HB 203:2012 Managing environment-related risk
risk treatment	A process to modify risk Risk treatment can involve: avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk taking or increasing risk in order to pursue an opportunity removing the risk source changing the likelihood changing the consequences sharing the risk with another party or parties (including contracts and risk financing) retaining the risk by informed decision. Note: Sometimes referred to as "risk mitigation" or "risk reduction".	AS/NZS ISO31000:2009
risk tolerance	A series of limits which, depending on the organisation, may either be: in the nature of absolute limits, beyond which the organisation does not wish to proceed (i.e. the organisation cannot deal with risks beyond these limits), or in the nature of alarms that alert the organisation to an impending breach of tolerable risks. Risk tolerance can be expressed in terms of absolutes, for example "we will not expose more than x% of our capital to losses in a certain line of business" or "we will not deal with certain types of customer ".	IRM Risk Appetite and Tolerance Guidance Paper

6.2) EXAMPLE RISKS IN WSC

- Contractor in financial difficulty leading to project delay, public inconvenience and possible additional costs to Council (3 consequences).

- Breach of licence requirements or POEO Act leading to (i) EPA investigation and (ii) potential fines (2 events and 2 consequences = 4 risks).

- Inadequate emergency response to calamitous events (e.g. natural disaster - flood, bushfire, swine flu, foreshore degradation, terrorist action – leading to loss of life and/or property and potential litigation claims (multiple consequences).

- Increased waste disposal costs/levies combined with changing regulations reducing the capacity to reuse materials leading to increased operational/project costs and reducing available budget in real terms (3 events and 2 consequences = 6 risks).

- Budget allocations not keeping pace with an expanding asset base leading to deterioration of the assets, earlier replacement than otherwise necessary, and reduction in service capacity.

- Increasing cost of energy leading to significant unbudgeted increases in operational costs.

- Major failure of electricity supply over an extended period (say greater than 8 hours) affecting the delivery of water and sewer services.

- Staff complacency on the worksite leading to lost time injuries rising and increased workers compensation costs.

- Inability to attract and retain appropriately skilled staff leading to a reduced capability of the organisation and a reduced capacity to plan and deliver services.

- Environmental incident from WSC activity on land owned or controlled by WSC leading to legal action, financial penalty and reduced Council reputation.

- Increasing sport participation rate leading to increased demand on assets, potential over-usage and risk of injury to players.

- A person drowns at a WSC beach leading to litigation.

- WHS incident (e.g. slip or trip) at Community Centres leading to injury/litigation.

- Accident occurs to a child, staff member or the public whilst at the child care centre, leading to serious injury or death.

- Customer Service Standards are not met leading to poor publicity and damage to WSC's reputation.

- Aggressive or threatening customers at the customer contact counter or on the phone threatening violence, verbal or written threats, harassment, verbal abuse and physical attacks leading to staff stress, stress leave and payments or loss of staff.

- Insufficient staff resources leading to a reduction in the ability to deliver sustainability, climate change and carbon management programs as outlined in the 2012-13 Strategic Plan.

- Information systems across WSC are not aligned leading to a high volume of manual reporting, low productivity, double handling, inefficiency and increased error rate.

- Field staff are assaulted leading to lost time injury, worker's compensation claims and loss of reputation as an employer.

- Loss of income due to a decline in development applications leading to a loss in forecast income.

- Poor communication across WSC resulting in uncoordinated work practices causing duplications and omissions leading to unnecessary expenditure, potential litigation and damage to reputation.

- Failing to keep abreast of changes to relevant legislation leading to potential litigation and reputation damage.

- Inappropriate financial delegations leading to extra administration burdens placed on Service Unit Managers.

6.3) EXAMPLE PROJECT RISKS

- Definition and certainty of project scope and functional requirements.
- No/insufficient testing, evaluation and acceptance processes.
- Development and maintenance of project documentation.
- Adequacy of funding including planning, construction and project support activities.
- Maturity of the processes, tools and training to support them.
- Skills and experience of the project management team.
- Changes n technologies or equipment.
- Ill-defined areas of technical specification, discrepancies between acceptance tests and the operating environment.
- Safety critical and security aspects.
- Sustainability, affordability, operation and maintenance of the solution throughout its expected operational life.
- Restructuring consequences for requirements and resources, and changes in work practices.
- Legislative changes affecting requirements and operating rules.
- Skills, tools, training and development required to provide competent users and support staff throughout the expected operational life of the solution
- Contractors' resourcing, financial sustainability, legal matters.
- Management stability of contractors and sub-contractors.
- Maturity of customer and contractor organisations in the process dimensions of process management, project management, engineering and support.

6.4) RESPONSE TO RISK MANAGEMENT PRINCIPLES

The following table summarises the AS/NZS ISO 31000:2009 ERM principles and identifies WSC's ERM Framework response to each.
Column A describes the principles and Column B identifies WSC's response

	WSC Response
(a) Risk management creates and protects value	
Risk management contributes to the demonstrable achievement of objectives and improvement of performance.	This ERM Framework identifies and focuses on WSC's strategic, operational and project objectives and supports their achievement. Risk management processes clearly establish objectives as the basis for risk assessment, and the subsequent implementation of risk management activities and the pursuit of opportunities.
(b) Risk management is an integral part of all organisational processes	
Risk management is part of the responsibilities of management and an integral part of WSC processes, including strategic planning and all project and change management processes.	The ERM Framework identifies the range of WSC functions where risk management will be applied, including strategic, operational and project risks. The ERM Framework will be integrated into WSC's induction process and training program. A common risk methodology will be applied across WSC, with records maintained in a common risk database.
(c) Risk management is part of decision making	
Risk management helps decision makers make informed choices, prioritise actions and distinguish among alternative courses of action.	The ERM Framework identifies WSC processes where risk management will inform more effective decision making. These include a range of strategic, operational and project reporting functions. Risk appetite statements and metrics are defined to inform decision making, and business rules define expected actions in response to various risk ratings.
(d) Risk management explicitly addresses uncertainty	
Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.	WSC's Risk Policy recognises and accepts that uncertainties will always exist in WSC's operating environment. The ERM Framework explicitly addresses uncertainty as part of the process of risk assessment and risk management.
(e) Risk management is systematic, structured and timely	
A systematic, timely and structured approach contributes to efficiency and to consistent, comparable and reliable results.	The ERM Framework document defines a structured approach to risk management that includes timeframes for risk assessments, risk responses, risk treatment actions, risk reporting, and for reviewing and updating the ERM Framework.

	WSC Response
f) Risk management is based on the best available information	
Inputs are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement.	This ERM Framework document highlights the importance of stakeholder involvement in risk assessments, and embedding risk management practices, processes and awareness in the day-to- day activities of all staff. Risk management processes embedded within the ERM Framework encourage the use of cross- functional teams. Improvement processes will include an assessment of the adequacy of risk information and the effectiveness of risk management processes. Risk treatment actions can include further investigations to improve the basis on which risk decisions will be made.
(g) Risk management is tailored	
Risk management is aligned with the organisation's external and internal context and risk profile.	The ERM Framework has been developed to reflect the particular circumstances of WSC's internal and external environment, including risk appetite statements, Strategic Risk Profile, Risk Tables, and its organisational structure, roles and responsibilities.
(h) Risk management takes human and cultural factors into account	
Risk management recognises the capabilities, perceptions and intentions of external and internal stakeholders that can facilitate or hinder achievement of WSC's objectives.	The ERM Framework recognises WSC's current resourcing levels and governance structures – particularly the role and responsibilities of the General Manager and Directors. Implementation of the ERM Framework will develop staff and stakeholder skills and capabilities that will, over time, explicitly address human and cultural factors in risk assessment and risk management practice generally.
(i) Risk management is transparent and inclusive	
Appropriate and timely involvement of stakeholders at all levels ensures that risk management remains relevant and up-to-date.	ERM processes recognise the need for stakeholder involvement and contributions. Risk registers will be accessible to and permit actions upon by those with defined risk responsibilities e.g. raise risks, update treatment status, and extract reports.
(j) Risk management is dynamic, iterative and responsive to change	
Risk management continually identifies and responds to change.	Risk assessment requirements are integrated into all organisational processes.
(k) Risk management facilitates continual improvement of the organisation	
Organisations should develop and implement strategies to improve risk management maturity alongside all other aspects of their organisation.	Assurance and improvement processes are explicitly defined in the ERM Framework and include mechanisms for regular reviews of WSC's risk maturity and the adoption of continuous improvement based on lessons learnt.

6.5) WSC RISK MANAGEMENT POLICY

Wyong
Shire
Council
CENTRAL COAST

POLICY FOR ENTERPRISE RISK MANAGEMENT

POLICY SUMMARY

A.1. The purpose of this Enterprise Risk Management (ERM) Policy is to communicate Council's commitment to managing enterprise-wide risks and to establish clear expectations to ensure that all staff are aware of their responsibilities for identifying and managing risk.

POLICY BACKGROUND

A.2. Wyong Shire Council acknowledges that significant risk events – should they occur – have the potential to adversely impact the achievement of its strategic, operational, financial, regulatory and other objectives.

A.3. Risk management explicitly addresses uncertainty but can never eliminate all risks.

A.4. Risk management thinking, principles and practices will support the achievement of objectives, helping Council deliver quality services, improving decision-making, establishing priorities, promoting safety, minimising the impact of loss, and ensuring regulatory compliance.

DEFINITIONS

A.5. Council means the elected representatives, Councillors, who form the governing body of Wyong Shire Council.

A.6. WSC means Wyong Shire Council, being the organisation responsible for the administration of Council affairs and operations and the implementation of Council policy and strategies.

A.7. Risk is the effect of uncertainty on objectives

A.8. Risk Management is a systematic process that involves establishing the context for risk management, identifying and analysing risks, treating and controlling risks, periodically monitoring and reporting on risks and treatments, communicating and consulting about new and emergent risks, and sharing experiences so that the overall process improves.

A.9. Enterprise Risk Management is the holistic management of all risks within council, not just insurable risks or occupational health and safety (DLG Internal Audit Guidelines, September 2010).

A.10. Enterprise Risk Management Framework is a set of components that provides the foundations and organisational arrangements for designing, implementing, undertaking, monitoring, reviewing and continually improving risk management throughout the organisation.

A.11. Risk Appetite is the amount and type of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time. It is expressed in the form of a risk appetite statement that covers Council’s critical risk categories.

POLICY STATEMENTS

Jurisdiction

A.12. This Policy covers all elected members of Council, all personnel employed by WSC, any person or organisation contracted to or acting on behalf of WSC, any person or organisation employed to work on WSC premises or facilities and all activities of the WSC.

A.13. This policy does not confer any delegated authority upon any person. All delegations to staff are issued by the General Manager.

General

A.14. Amendment to this policy will occur in accordance with the procedure for Organisational Policy establishment contained in the WSC Policy for the Establishment of Policies.

A.15. It is the personal responsibility of all WSC employees and agents thereof to have knowledge of, and to ensure compliance with this policy

A.16. WSC is committed to the formal, systematic, structured and proactive management of risks across the organisation.

A.17. Whilst risk is inherent in all WSC's activities, the management of risk is good business practice, creates value, is integral to good corporate governance and, in some instances, a mandatory legal requirement.

A.18. Effective risk management:

- supports decision-making and planning
- increases the likelihood of achieving objectives
- identifies opportunities

POLICY IMPLEMENTATION - PROCEDURES

A.19. WSC is committed to maintaining an effective, efficient and tailored risk management framework that consists of this policy, an enterprise risk management strategy, and supporting policies that complement risk management such as fraud prevention, internal audit, business continuity, environmental and WHS management systems and the Code of Conduct.

A.20. The ERM framework will enable:

- a formal, structured approach to risk management that is appropriate to WSC's activities and operating environment

- a risk management approach consistent with the principles of AS/NZS ISO31000:2009

A.21. WSC's current risk appetite statement is contained in a separate document and is broadly based on a low tolerance to risk, particularly where it may affect the safety of staff and/or the community, financial viability and regulatory compliance.

A.22. WSC is committed to ensuring that a strong risk management framework is in place that:

- integrates risk management with existing planning and operational activities
- allocates sufficient funding and resources to risk management activities
- provides staff with appropriate training in risk management principles and processes
- assigns clear responsibilities to staff at all levels for managing risk
- embeds controls to manage risks into business processes
- establishes mechanisms for measuring and reporting risk management performance
- communicates risk management policies, plans and issues to staff and other stakeholders
- is dynamic, iterative and facilitates continual improvement

A.23. Council is ultimately responsible for adopting and committing to this risk management policy and fully considering risk management issues contained in Council reports.

E.6 The ERM Committee is responsible for periodically reviewing the ERM Framework and for monitoring:

- plan and facilitate the progressive implementation of the ERM Framework and the development of a risk-aware culture
- establish and monitor key performance indicators for the implementation and operation of the ERM Framework
- report quarterly to the Executive Team regarding the performance of the ERM Framework, including recommendations to achieve performance targets
- identify training and development needs to achieve the required risk management competencies across WSC
- coordinate resources to support the implementation of the ERM Framework
- facilitate the formal review and update of the ERM Framework

E.7. The General Manager is responsible for leading the development of an enterprise risk management culture across the organisation and ensuring that this Policy and the enterprise risk management strategy are being effectively implemented.

E.8. The Executive Team is responsible for considering urgent, sensitive and/or complex risk management issues that cannot be resolved by staff.

E.9. The Risk Management Coordinator is responsible for ensuring that all requirements necessary for the implementation and operation of the risk management strategy across Council are in place, including:

- reporting to Executive Team on business and financial risks, risk plans for major projects and undertakings, and new and emerging risks relevant to Council
- reporting to the ERM Committee on ERM Framework development needs
- implementing directions of Executive Team relating to the ERM Framework
- contributing to Council’s risk policy, risk appetite, and strategic, operational and project risk planning
- assisting managers in understanding the interrelationships between various types and sources of risk
- creating a risk-aware culture
- ensuring a consistent approach to ERM throughout Council

E.10. Directors are responsible for ensuring that this Policy and the risk management strategy are being effectively implemented within their areas of responsibility.

E.11. Managers are required to create an environment where the management of risk is accepted as the personal responsibility of all staff, volunteers and contractors. Managers are accountable for the implementation and maintenance of sound risk management processes, structures and outcomes within their areas of responsibility in accordance with Council's risk management framework.

E.12. Staff are required to act at all times in a manner which does not place at risk the health and safety of themselves or any other person in the workplace. Staff are responsible and accountable for taking practical steps to minimise Council's exposure to risks including financial, legal, environmental, reputation and conduct insofar as it is practicable within their area of activity and responsibility, and for notifying potential hazards and opportunities.

E.13 This policy will be reviewed within 12 months of the election of each new Council and two years thereafter, or more frequently in the event of a material change in circumstances.

Associated documents

E.14. WSC Enterprise Risk Management Framework WSC Risk Appetite Statement

6.6) RISK MATURITY ASSESSMENT – JUNE 2012

WYONG SHIRE COUNCIL

Enterprise Risk Management Strategy

Risk Management Maturity Assessment Report

May 2012

Contents

Revision History

Issue	Date	Description	By
1	12 Jun 12	Draft for internal review	CD
2	14 Jun 12	Draft for WSC review	CD
3	25 June 12	Final	CD

INTRODUCTION

BACKGROUND

Capital Insight is appointed to assist Wyong Shire Council (WSC) with the development of an Enterprise Risk Management Strategy (ERMS).

A risk maturity assessment is part of the early phase of development of the ERMS and provides WSC with a snapshot of current skills, knowledge, culture, processes and systems for risk management.

The results of the risk maturity assessment provide an important foundation for the development of the ERMS because they:

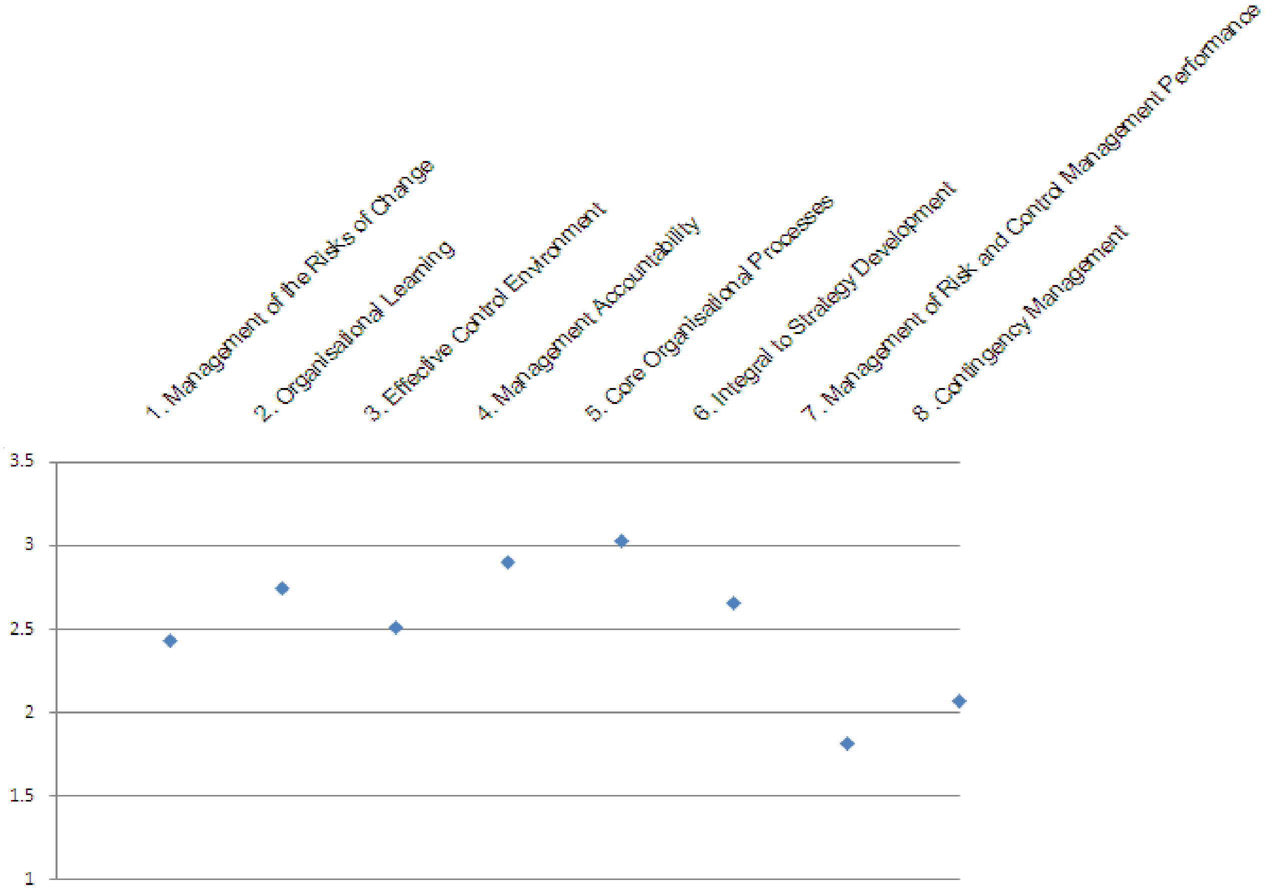
- identify gaps in risk management processes, capacity and culture
- identify relative strengths and weaknesses in risk management performance across different functions within WSC
- identify variations in perceptions between different groups within WSC
- provide an input for subsequent phases which involve agreement and articulation of WSC's risk appetite
- inform prioritisation for WSC's ERMS development
- establish a baseline for assessing improvement over time
- provide a basis for benchmarking with other organisations if WSC opts to do so.

SUMMARY OF FINDINGS

The following graph summarises WSC's risk maturity scores showing the average overall rating for each attribute measured across five departments.

Ratings indicate the extent to which assessment participants believe that WSC risk management practices align with a series of best practice statements (from 0 = not at all to 4 = almost always).

Note that qualitative feedback and commentary for each of the attributes provides important context for these findings and is detailed in the body of this report.



In summary, findings of the assessment are:

- the majority of risk maturity ratings were in a range between 2 and 3, indicating the interviewees' view that there is some but inconsistent alignment of WSC's risk management practices with best practice indicators at the lower level, and trending to a measure of consistency of approach at the upper level
- the lowest risk maturity ratings were associated with attributes for risk and control performance – requiring WSC to have implemented (among other things) a documented risk management framework, a risk management plan, risk management KPIs, risk management performance reporting, and professional development initiatives. These tasks will be addressed as part of WSC's ERMS implementation
- of the remaining attributes, the next lowest ratings were associated with contingency management where feedback indicated that WSC had some processes in place to respond to crises and business interruptions, but acknowledging that a draft business continuity plan is currently under review within WSC and that a regular testing program has not been implemented
- core organisational processes had the highest ratings, where many participants believed that WSC's decision-making processes – particularly for large projects and significant changes to the organisation – involved careful considerations of risks, although risk processes are not uniformly embedded in all day-to-day activities

- management accountability rated almost as high as organisational processes with senior staff taking responsibility for risk management, with good oversight/monitoring processes in place.

Overall, WSC has opportunities for improving risk management maturity across all eight attributes.

It is Capital Insight's view that improvements with respect to attributes such as managing risks of change and risk and control management will be closely tied to the implementation of the ERMS, and should result in significant improvements in risk maturity ratings within 12 months of ERMS implementation.

The organisational learning attribute will be partly addressed in the training component of the ERMS engagement which will, in turn, be informed by the outcomes of this maturity assessment.

Attributes such as effective control environment will require significant changes with respect to the allocation of accountabilities, individual attitudes and organisation culture changes that are longer term goals of the ERMS. Characteristics of a good risk-aware organisational culture will be included in the ERMS documentation.

MATURITY ASSESSMENT METHODOLOGY

RISK MATURITY MODEL SELECTION

Risk management maturity measures the level of skills, knowledge and attitudes of people in an organisation, combined with the level of sophistication of processes and systems applied to managing risk.

Determining where WSC is at the moment is a necessary first step in developing and articulating Council's risk appetite and for developing elements of the ERMS.

A number of recognised risk maturity models exist. These were summarised and discussed with the PCG to determine the model most appropriate and practical for this risk maturity assessment.

Each model has a different focus and/or assessment method. None aligns directly with ISO31000, although all have some commonality with its principles and structure[1].

Considerations for selection of a preferred maturity model included:

- alignment of the model with ISO31000 and WSC's needs
- the extent of industry recognition and adoption of the model
- ability to derive reliable and relevant results as a driver for improvement
- accessibility and ease of use (including licensing restrictions and costs)
- potential to replicate the assessment as a basis for measuring changes over time
- opportunities to use the model for benchmarking with other organisations.

The maturity model adopted is included in Attachment B. It is structured around the following attributes:

- management of change
- organisational learning
- control environment
- management accountability
- core organisational process
- strategic alignment
- risk and control management performance
- contingency management.

[1] ISO31000:2009 is the international risk standard

INTERVIEW METHOD AND PARTICIPATION

Interviews were conducted on a Department-by-Department basis with the Director and Service Unit Managers. A list of participants is provided at Attachment A. In total, the risk maturity assessment process involved discussions with 31 WSC staff.

All assessments were conducted through group interviews, with the Capital Insight assessor and the WSC Project Manager attending each session.

QUANTITATIVE ASSESSMENT

Assessment Rating Scale

Ratings indicate the extent to which WSC risk management practices align with a series of best practice statements. The best practice statements are included in Attachment B.

Participants rated each statement as a group and were asked to what extent they considered that WSC operates in accordance with each best practice statement, with a focus on Departmental functions and activities.

There were some exceptions that required a whole-of-organisation response.

RatingDescription	Score	%
Not at all	0	<1%
Very little	1	1-19%
Sometimes	2	20-49%
Mostly	3	50-84%
Almost always	4	>85%

It should be noted with respect to the overall ratings shown on page 1 that a number of participants opted for a rating of 3 however noting that WSC's current performance probably was at the lower end of the 50-84% range.

QUALITATIVE FEEDBACK

The comments recorded during each interview provide important context for understanding the quantitative results which, by themselves, present a somewhat over-simplified view of current risk management practices. Discussions often identified scenarios in which participants felt that either:

- practices were generally lacking, but there were examples of good practice, or
- practices were often good, but with obvious examples where risk practices had been lacking.

Therefore, use of the ratings as a management and planning tool should always occur with consideration of the associated commentary.

DETAILED FINDINGS

MANAGING RISKS OF CHANGE

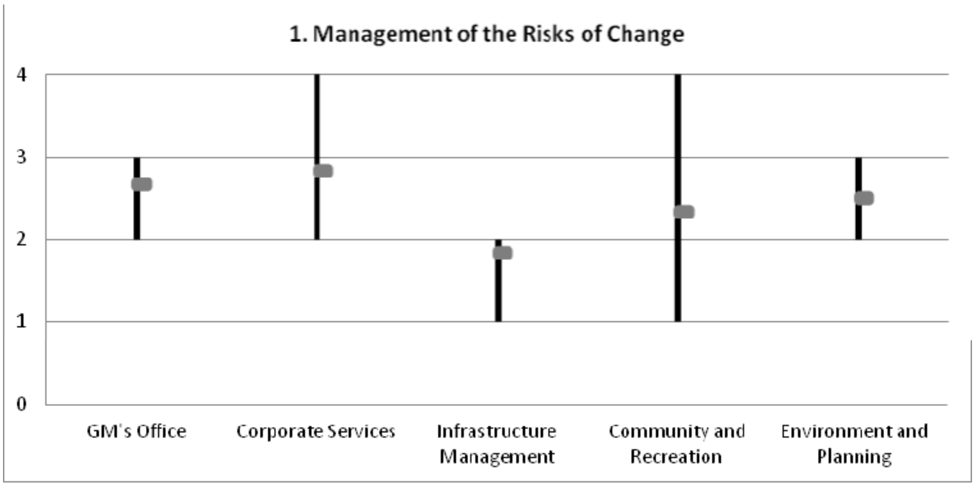
Attribute Overview

This attribute recognises the potential impacts of change on the effective management of corporate risk, and aims to ensure that risks generated by both internal and external changes and events are effectively and efficiently managed.

Best practice includes requirements for:

- documented and effective approaches for the management of change
- risk assessments that consider relevant categories of risk and apply them for assessment of:
  - internally initiated change
  - externally imposed change
  - changes to critical processes or procedures
  - structural or organisational change.

Rating Results



- Average rating for this attribute = 2.4 (sometimes/mostly)
- Weakest rating (1): Feedback indicated that WSC had not yet established documented and effective approaches for the management of change.
- Strongest rating (4): Feedback indicated that risk assessments were applied to risks associated with changes, with many of those originating externally having prescribed processes associated with them.

Feedback

Comments included:

- There is a perception that a documented approach for the management of change does not exist.
- Externally initiated or oriented changes are generally better managed than internal ones because the external changes tend to be better defined (e.g. change in legislation or regulation, new guidelines, fees/charges, finance, governance) with correspondingly clearer opportunities to allocate responsibilities for change management.
- There are several notable exceptions to the above comment, with detailed risk considerations applied to IT system and WHS changes.
- There is a "follow the bouncing ball" perception in the use of templates and checklists, with a number of participants suggesting that these tools need to change so that people are forced to think and not just fill out the form or tick the box.
- Some SWOT analyses have been undertaken within Service Units, outside of the template structure for Service Unit Business Plans to better inform service planning and delivery.
- Consideration of change risks is inconsistent and ad hoc across Service Units and Departments. When change is considered, outcomes are not shared consistently or communicated particularly well.
- Risk assessments tend to focus on risk categories that have impacted WSC before – instead of a broader, more balanced approach across all risk categories.
- Risk assessments are carried out as part of the management processes for the design and delivery of major projects, for major events, and for critical processes. These are generally acknowledged across WSC as the leading exemplars of risk management in the organisation at the moment.

ORGANISATIONAL LEARNING

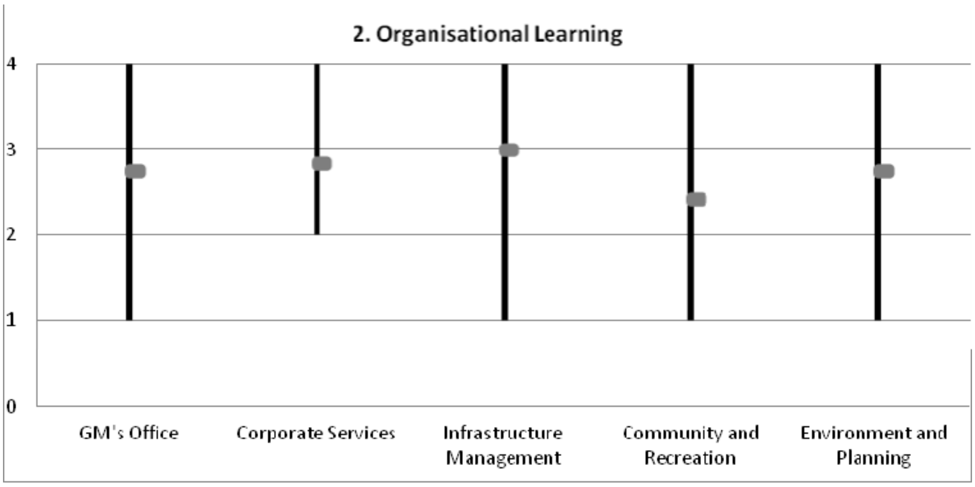
Attribute Overview

This attribute aims to ensure that there are structured processes for improvement whereby WSC can learn from both successes and failures.

Best practice includes requirements for:

- systems to capture lessons learnt following significant changes, activities or events
- ensuring that root cause analysis techniques are adopted where appropriate
- mechanisms to capture, record and communicate lessons learnt
- review of prior risk assessments to establish their effectiveness and to drive improvement in future risk assessment
- forums to discuss opportunities for improvement
- identifying and sharing better practice risk management practices.

Rating Results



- Average rating for this attribute = 2.8 (sometimes/mostly). Organisational learning was one of the strongest of the eight attributes reviewed as part of the interview process, with fairly consistent ratings across all departments.
- Weakest Rating (1): Feedback indicated that WSC had not yet established effective mechanisms for sharing lessons learned across the organisation, or for reviewing the effectiveness of prior risk assessments.
- Strongest Rating (4): Opportunities are provided in management meetings to discuss opportunities for improvement, and review and internal audit processes provide a good capture mechanism for lessons learnt

Feedback

Comments included:

- Good risk practices are starting to be discussed at management and supervisor meetings, but less consistently between Departments.
- Although there is no formal structure for the capture and dissemination of lessons learnt, there are newsletter, briefing and update mechanisms used that can lead to better practice approaches.
- Good risk and business practices are also available through legislation (e.g. WHS) and DLG guidelines.
- There are over 20 audit and review processes that have occurred or are occurring, all directed towards improving the organisation's performance e.g. Service Delivery Review, internal audits, the ERMS project, asset management review.
- WSC also has a number of processes that identify/incorporate lessons learnt e.g. audits, WHS investigations, post-completion assessments, Safe Work Method Statements, Service Delivery Review.
- The investigation into the Link Road project included root cause analysis (although the only example of root cause analysis cited by participants). Other reviews mentioned included the 2007 storm event and contracts, although they did not use root cause analysis.
- When analysis occurs, there are problems in communicating to the community that the problem has been rectified.
- There are risks in having risk issues concentrated in one person and not recorded in some form that is accessible to others.
- There are risks in the numbers of emails that people receive, in terms of the time taken to deal with them or – more importantly – possibly missing an important one.
- Retrospective reviews of project risks occur but inconsistently.
- Time is specifically allocated in monthly Infrastructure Management meetings to consider risk, when the risk register is reviewed.
- WSC is better at reviewing projects and operational-level risks, than corporate/strategic risks.
- Templates help to ensure that business is undertaken consistently, however there may be a need to review some templates. The comment was made several times that the previous version of the Service Unit Business Plans had a better section on risk management than the current one.
- Generally, post-implementation reviews are not conducted at WSC.
- There is a need to improve knowledge sharing to leverage the expertise within WSC (and not repeat the mistakes of the past).
- Opportunities are normally available to raise continuous improvement opportunities as part of management meetings.
- There needs to be a cultural change to facilitate continual improvement.

CONTROL ENVIRONMENT

Attribute Overview

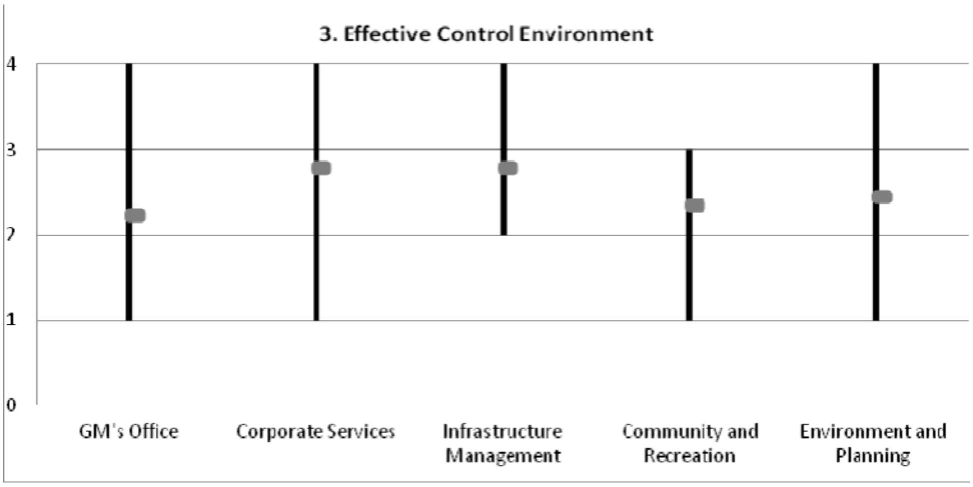
This attribute aims to ensure that risk is effectively and consistently managed within an explicit, established and efficient internal control environment.

WSC's control environment can include procedures, checklists, approval protocols, formal reviews, delegations, reporting requirements, staff training and expertise, communications protocols, monitoring, audits, incident response, etc.

Best practice includes requirements for:

- identifying and documenting risk controls
- readily accessible risk controls/procedures
- ensuring that staff are aware of risk controls relevant to their areas of responsibility
- controls that are designed and matched to the causes of the risks
- ensuring that key controls are tested
- clear identification of control owners
- ensuring that self-assessments are conducted by control owners
- application of cost-benefit analysis for the selection of risk treatments for significant/material risks.

Rating Results



- Average rating for this attribute = 2.5 (sometimes/mostly).
- Weakest Rating 1: Structured processes and staff competencies have not been established to ensure that risk controls are designed and matched to the operational risks requiring management.
- Strongest Rating 4: Senior staff are aware of risk controls relevant to their areas of responsibility.

Feedback

Comments included:

- There are a variety of control mechanisms at WSC and they are well defined – SharePoint, TRIM, alerts, intranet, legislation, delegations, training, Code of Conduct – but not very well integrated.
- The current internal audit plan reflects WSC's perceived risk profile.
- Controls for project management are generally well defined.
- Control testing is not formalised or structured, and not undertaken consistently across WSC.
- Operational level staff have very high levels of understanding of the risk context of their jobs, but possibly less so for office-based staff.
- Life-cycle cost analysis is a commonly used tool as part of decision making, and not just for deciding between risk treatment options e.g. life cycle costs of vehicles and buildings, new systems.
- There is no consolidated high-level definition of WSC's internal control framework, and a risk software package has not yet been implemented that could potentially provide a consolidated overview of organisation-wide risk controls.
- Some of the control documentation is not particularly clear ("impenetrable" was mentioned), and the sheer volume represents another barrier to access, understanding and use ("documented to death").
- The strictures of the way local government operates places a greater emphasis on what individuals do, rather than how they do it.

MANAGEMENT ACCOUNTABILITY

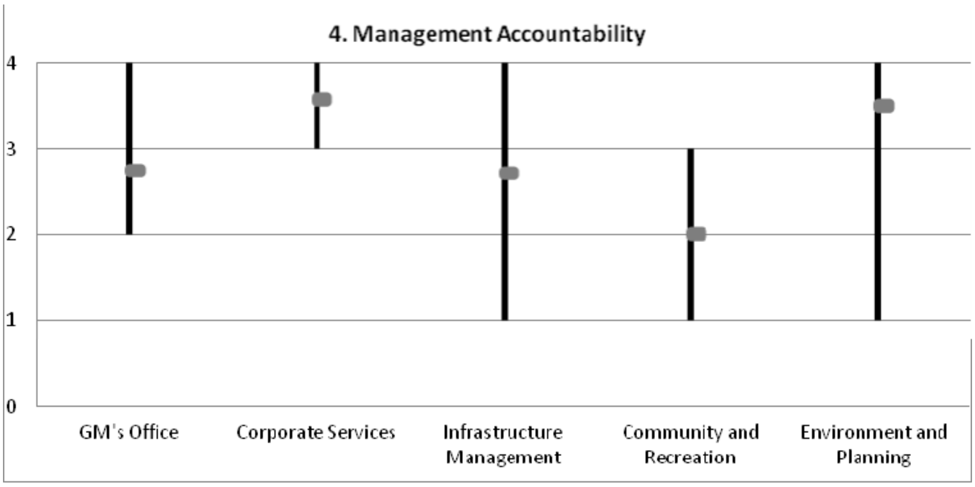
Attribute Overview

This attribute aims to ensure that there is comprehensive, defined and accepted accountability for risks, controls and risk treatment tasks. This includes compliance activities.

Best practice includes requirements for:

- allocation of controls to control owners
- allocation of significant risks to risk owners
- an appropriately skilled person to be allocated formal responsibility for overseeing enterprise risk management processes
- Council's Governance Committee to oversight the effectiveness of Council's ERM Framework
- delegations of authority to be based on risk exposure
- position descriptions to clearly define accountabilities for the management of risk
- accountabilities to be defined so that staff know expectations.

Rating Results



- Average rating for this attribute = 2.9 (mostly).
- Weakest Rating 1: Feedback indicated that lower level position descriptions do not clearly define accountabilities for the management of risk.
- Strongest Rating 4: Controls are allocated to control owners for significant risks, and these are accepted and known.

Feedback

Comments included:

- Risks in risk registers are not communicated very well. Staff do not see risk registers in other Departments, hence there is little cross-flow of information, and lessons learnt.
- There are instances of unclear and duplicated responsibilities e.g. at Service Unit Manager level for reputation risk, yet impacts can arise across the organisation.
- Risk owners are identified for significant risks in the Corporate and IM registers, with the concept of control owner not differentiated from risk owner.
- ERM processes within WSC do not yet have an effective oversighting role or function identified, or an individual with accountability for the ERM Framework.
- Many controls are externally defined (e.g. Local Government Act), with some staff relying on the controls for decision-making (tick the box mentality.
- Some position descriptions are not explicit with respect to risk accountabilities beyond safety and financial, and some participants indicated they did not understand the accountability for risk implicit in their position descriptions.
- Delegations below Service Unit Managers are reportedly only a couple of lines and probably not sufficient for the accountabilities/ controls they seek to define e.g. Responsible Officer in child care centres.
- Some staff reportedly avoid accountability by escalation (see also the comment relating to email volumes in an earlier section), with some comments suggesting that this could be because of unclear risk responsibility or an inclination to avoid accountability.
- High turnover in some Departments has impacted on staff understanding of their roles/responsibilities.
- Delegated authorities have a good alignment with WSC's risk exposure, but this alignment is not explicit.
- WHS controls and accountabilities are well defined.
- Problems with accountability can arise when responsibility and authority are allocated to a person, not a position.
- Accountabilities are not sufficiently well defined for staff who need to manage operational threats at a lower level in the organisation (i.e. below manager level),

CORE ORGANISATIONAL PROCESS

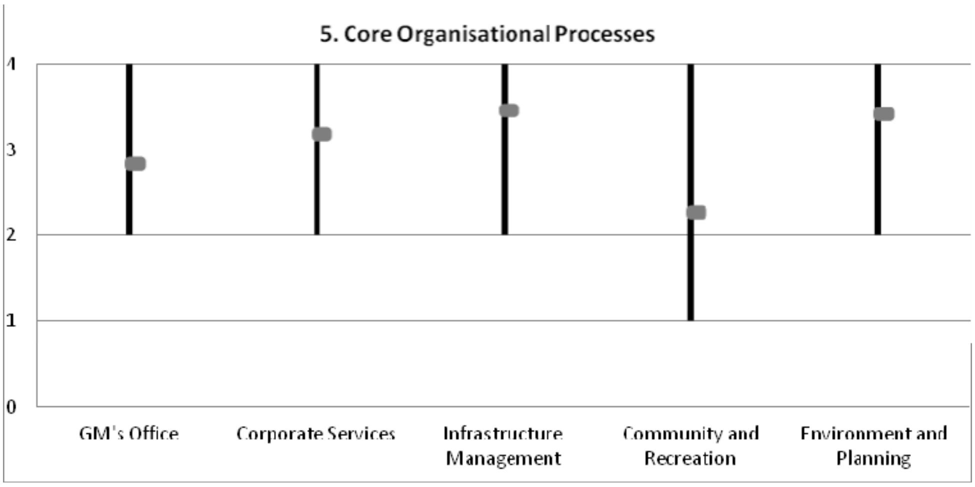
Attribute Overview

This attribute considers the management and control of risk as central to the achievement of the organisations' objectives.

Best practice includes requirements for:

- the effective consideration of risks in decision making
- consideration of positive (opportunity) and negative (threat) risks
- management of risk in accordance with Council's risk appetite
- identification and effective communication of objectives as a basis for risk identification
- embedding risk management within key organisational processes
- ensuring that decisions regarding major investments or potential liabilities involve consideration of risk
- engaging with internal and external stakeholders (as appropriate) during all stages of the risk management process.

Rating Results



- Average rating for this attribute = 3.0 (mostly). This was the highest rated attribute.
- Weakest rating 1: There is little effective communication about risks between Service Units/Departments.
- Strongest rating 4: Directors and Service Unit Managers manage risks within the boundaries of WSC's implicit risk appetite and existing controls, with good decision-making processes for large projects and significant organisational changes.

Feedback

Comments included:

- WSC's strategic direction is clearly articulated and clearly understood, however not all lower level plans are fully aligned to those directions. The Service Unit Business Plans currently under finalisation are one response that will achieve greater alignment and consistency.
- There is consideration of both risks and opportunities in some Departments.
- Risk communication is good within Departments, but less so between Departments.
- Some of the language in strategic documents is too high level for clearly communicating with individuals e.g. roles, impacts, expectations.
- Not much consultation occurs between Service Units in other Departments to know/understand what they are doing. Where it happens, it is perhaps viewed as a form of risk mitigation.
- WSC takes a relatively conservative approach to risk appetite (risk appetite will be defined as a part of the current ERMS project).
- Processes are usually followed where critical and/or material subjects are being considered, often involving discussion with Councillors to develop proposals prior to going for decision.
- There are instances where a "get it done" attitude prevails at the expense of giving risk due consideration as part of a process.
- Directors and Service Unit Managers are aware of and manage risks within the (perceived) boundaries of WSC's risk appetite and existing controls.
- Risk is considered as an input to decision making within the ELT.
- The approach taken to risk and opportunity identification (and their pursuit) varies by discipline and is influenced by the individual's experience and attitude.
- Corporate objectives are not yet reflected in KPIs.
- WHS risk management is embedded within WSC's key organisational processes, but a similar outcome has not been achieved for other business risks.
- External communication and consultation requires a trusting environment which is often lacking when WSC actions might negatively impact on individuals or groups

STRATEGIC ALIGNMENT

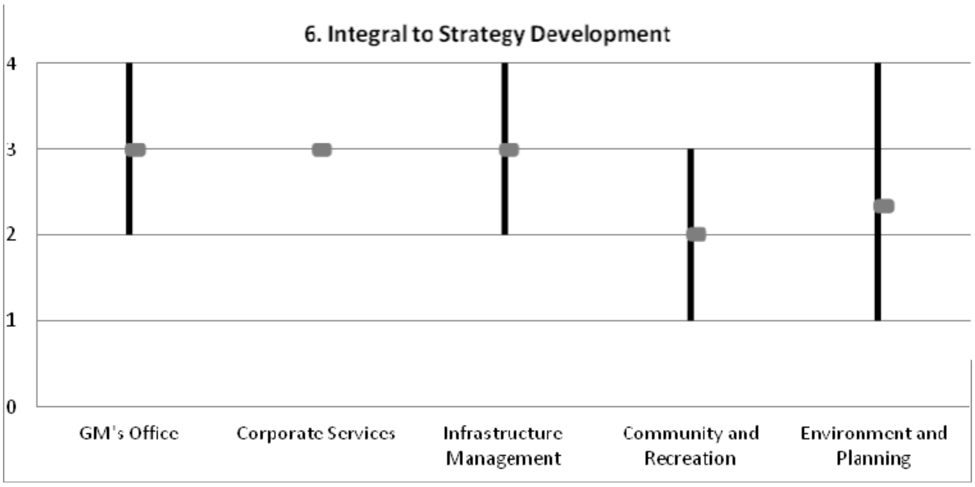
Attribute Overview

This attribute aims to ensure that there is a clear and explicit linking of risk and control management to WSC's strategic planning and implementation.

Best practice includes requirements for:

- WSC's strategic planning documents to contain information identifying risks and opportunities
- WSC policy setting and KPIs to be informed by WSC's risks and opportunities
- WSC's strategies to be established with reference to Council's risk appetite
- Management decision making has a long term, strategic focus.

Rating Results



- Average rating for this attribute = 2.7 (sometimes/mostly). Note that Corporate Services scored this attribute as 3 throughout, hence no range is shown.
- Weakest rating 1: Risks and opportunities are not applied consistently across the organisation.
- Strongest rating 4: WSC has a well-developed vision and a well- articulated strategic direction.

Feedback

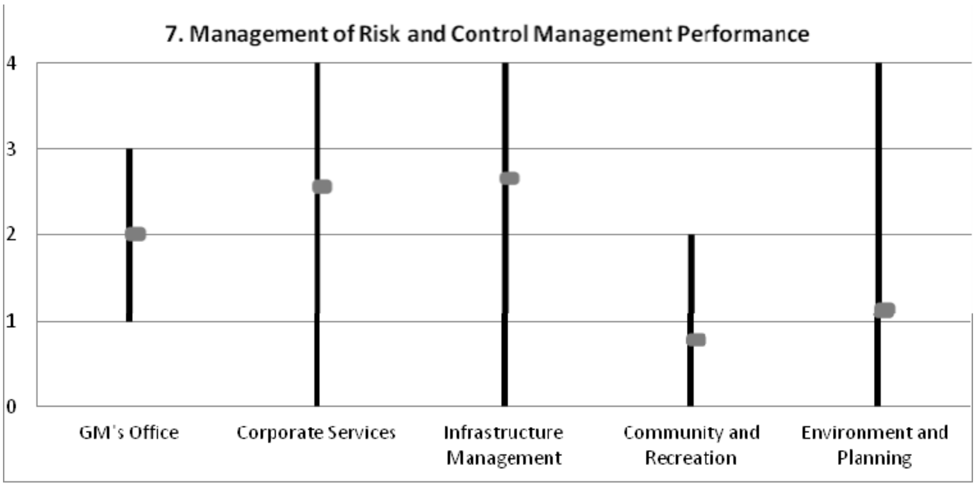
Comments included:

- WSC has a well-developed vision.
- Risk appetite was stated to be implicitly understood by staff, possibly erring on the side of caution when uncertainty about appetite arises.
- Service Unit Business Plans include operational risks and these are included in risk registers, although to varying levels of detail and consistency.
- WSC’s strategic plan uses the term “challenges” in lieu of “risks”. The ERMS project will seek to establish consistent terminology when referring to risk-related issues.
- The risks and opportunities relating to strategies are not applied consistently across the organisation.
- Short-term gains are sacrificed in order to pursue longer-term gains.
  An example is the life-cycle cost approach taken to asset management planning where higher costs now lead to lower operating and maintenance costs later.
- Participants indicated that the balance is “pretty good” between expedient versus value generating decisions. Most Service Units and Departments have a medium to long-term view, although there can be political pressure for short-term wins/gains.
- KPIs that are externally imposed generally relate well to the relevant requirement, with internally established KPIs less well done.
- Policy development can occur without consideration of risks.

RISK AND CONTROL PERFORMANCE

Attribute Overview

This attribute aims to ensure that continuous improvement in risk management is achieved through the setting of WSC's risk management performance goals, measurement, review and the subsequent enhancement of processes, systems, resources and capability/skills.



- Average rating for this attribute = 1.8 (sometimes). This attribute has the lowest overall rating, with quite divergent views across departments.
- Weakest rating 0: A risk management plan does not yet exist for WSC. Other formal ERM components are being developed but are not yet in place.
- Strongest rating 4: There are KPIs for senior staff, recognised risk expertise within WSC, and a growing awareness of risk as an integral component of day-to-day activities.

Feedback

Comments included:

- WSC has commenced its risk maturity assessment journey, and the findings of this assessment will inform further planning for the ERMS project.
- Specific risk-related KPIs for the GM are explicit, whilst some exist for senior executives. KPIs relating to WHS are explicit, as are those included in contracts.
- Risk performance is measured and reported in monthly reports and the Green Book.
- Risk management content in reports that go to Councillors is perceived to be for guidance and to report possible impacts.
- To date there has not been a program of formal risk training (although this will alter once the training component of the ERMS project commences later in 2012).
- Councillor decision-making can be politically driven, with an inclination to avoid seeking advice where such advice might be contrary to the desired direction/outcome.
- There is a developing knowledge, expertise and experience throughout WSC through the ERMS project (amongst other things). One participant indicated that they had realised there were some things they could be implementing even now, just by having read the maturity assessment statements.

CONTINGENCY MANAGEMENT

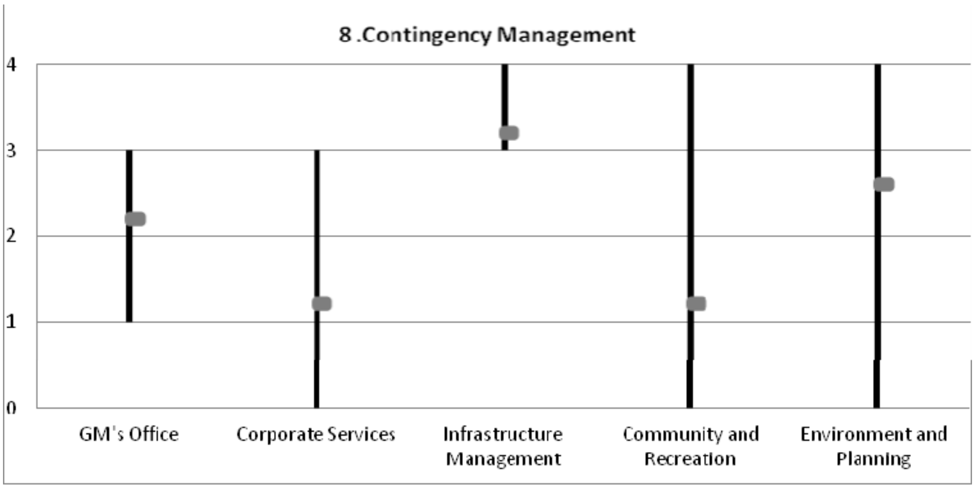
Attribute Overview

This attribute aims to ensure that WSC has a viable and effective plan to ensure business continuity in the event of a major incident.

Best practice includes requirements for:

- establishing crisis/emergency management plans
- ensuring that plans deal with all of the types of events that can impact WSC
- testing these plans in accordance with an agreed testing program
- ensuring that plans are kept up to date
- ensuring that all staff having a role in the implementation of plans are fully aware of their roles.

Rating Results



- Average rating for this attribute = 2.1 (sometimes)
- Weakest rating 0: There is uncertainty about any testing of existing plans, and consensus that there is not a regular testing program.
- Strongest rating 4: Staff indicated an awareness of business continuity plans and roles.

Feedback

Comments included:

- WSC has various crisis/emergency response/business continuity plans, the latter currently in draft for review.
- The assessor mentioned that the current draft business continuity plan omitted several important topics including key personnel and alternates, critical information/documentation, training in the application of the plan, scenario testing, the circumstances under which the plan would be activated, and communications protocols with staff in the event that the plan is activated.
- There was considerable uncertainty about whether plans had been tested, although all those with an emergency response role had all been trained in the last two years.
- A number of staff indicated that they were aware of the business continuity plan and understood their role.
- No testing has been done on existing plans, and there is not a program for regular testing.

ATTACHMENT A: LIST OF PARTICIPANTS

The following WSC staff contributed to the risk maturity assessment. The left hand column lists staff names and the right hand column lists their titles.

Name	Title
Corporate Services	
David Jack	Director Corporate Services
Stephen Bignill	Senior Project Executive
Melisa McKee	Corporate Planning Executive
Kathleen Morris	Manager Integrated Planning
Brett Phillips	Manager Economic and Property Development
Bob Platt	Chief Information Officer
Infrastructure Management	
Greg McDonald	Director Infrastructure Services
John Barnard	Manager Plant Fleet Depots
Stefan Botha	Manager Waste
Darryl Mann	Manager Water and Sewerage
David Norbury	Senior Assets Engineer
Andrew Pearce	Manager Roads and Stormwater
David Witherdin	Manager Contract and Project Management
Community and Recreation	
Maxine Kenyon	Director Community and Recreation
Ian Clarke	Manager Community Buildings
Adam Holland	Manager Life Long Learning
Sue Ledingham	Manager Customer and Community Relations
Tara Mills	Manager Sport Leisure and Recreation
Brett Sherar	Manager Open Space
Julie Vaughan	Manager Community and Cultural Development
Environment and Planning	
Gina Vereker	Director Environment and Planning
Paul Bowditch	Manager Place Management
Peter Fryar	Manager Development Assessment
Martin Johnson	Manager Land Use Policy and Development
Jamie Loader	Manager Building Certification and Health
David Ryan	Manager Estuary Management
Rob Van Hese	Manager Compliance and Regulation
Greg White	Manager Environment and Natural Resources
General Manager's Office	
MichaelWhittaker	General Manager
Brian Glendenning	General Counsel
Stefano Laface	Executive Manager to the GM

ATTACHMENT B: RISK MATURITY EVALUATION TABLES

1. Management of the Risks of Change

All risks created by both internal and external changes and events are effectively and efficiently managed.

Column A lists the requirement and Column B provides guidance on the evaluation

Requirement	Guidance on evaluation
1.1 WSC has an effective documented approach for the management of changes.	Normally this would be a change of management system or procedure. The form of risk assessment should be specified within it. The change management system or process should cover all those significant changes which we propose to undertake internally together with those changes which might occur externally which would be significant for WSC.
1.2 WSC effectively uses a documented approach for the management of changes	This is about the effectiveness of the utilisation of the documented approach
1.3 Risk assessments that consider all relevant categories of risk are conducted whenever significant internally created changes occur or are planned.	This means a properly conducted systematic risk assessment with the rigour of the assessment in keeping with the severity of the potential consequences. The risk assessment covers all relevant categories of risks and is not, for example, just for workplace health and safety or financial risks.
1.4 Risk assessments that consider relevant categories of risk are conducted whenever significant external changes and events are detected	Normally, the risk assessments would cover all relevant categories of risks. A risk assessment that deals only with workplace health and safety or financial risks is not adequate.
1.5 Risk assessments that consider relevant categories of risks are conducted whenever important or critical processes or procedures are changed.	Normally, the risk assessments would cover all relevant categories of risks. A risk assessment that deals only with workplace health and safety or financial risks is not adequate.
1.6 Risk assessments that consider relevant categories of risk are conducted before structural or organisational changes occur.	Organisational changes may involve just one or a small number of people (for example the restructure of a section) or may affect the whole WSC (for example an organisational restructure).

.

2) Organisational Learning

There is a structured process of improvement whereby WSC can learn from both successes and failures.

Column A lists the requirement and Column B provides guidance on the evaluation

Requirement	Guidance on Evaluation
2.1) WSC has a system to capture significant lessons learnt after significant changes, activities or events, whether planned or not.	This may be part of a change management system. This must be for more than just Workplace Health and Safety incidents and asset failures. It should deal with successes and 'positive outcomes' as well as losses, accidents and breakdowns.
2.2) Systems of root cause analysis are used as appropriate to derive lessons learnt and generate actions after changes, activities, and events, whether positive or negative. (Root cause analysis is finding the real cause of the problem and dealing with it rather than simply continuing to deal with the symptoms)	This implies the adoption of a proper system for root cause analysis. Just writing down the root causes is not sufficient. Importantly, the analysis must lead to actions to codify and communicate actions.
2.3) There is a formal mechanism to efficiently capture and disseminate significant lessons learnt and actions arising from root cause analysis within WSC.	Software can be used for this. It can also be through regular meetings and briefings.
2.4) Reviews of prior risk assessments are undertaken to consider their effectiveness.	This is about the degree to which we assess the effectiveness of risk management in completed or in progress activities (and apply that knowledge to current or planned activities).
6.7) Time is specifically allocated in management meetings to discuss opportunities for improvement, based on lessons learnt from post activity analysis, decisions or events.	This should be a standing item in the agenda of management meetings. For projects, this should be on the agenda of project management meetings. Both successes and failures should be discussed.
6.8) When things go wrong we're mostly concerned with preventing this from recurring	Lessons learned approach is taken rather than looking to someone to blame when things go wrong.
6.9) Good practices in risk processes are identified and shared across the organisation	There should be processes in place to share good risk practice across the organisation, whether sourced internally or externally
6.10) Organised efforts are made to implement improvements and good practice risk processes	There should be processes in place to identify and capture risk management improvement opportunities by all levels of the organisation
6.11) Good practices in business processes are identified and shared across the organisation	There should be processes in place to identify and share good practice business processes across the organisation, whether sourced internally or externally

6.12) Staff are encouraged to speak up and say what they think	There is an acceptance of alternative views in the organisation - staff feel that it does pay to voice concerns. Without this, suggestions for improvement will be stifled whether they are for risk management or other key processes or activities.

Requirement	Guidance on Evaluation
6.13) Organised efforts are made to implement improvements and good practice business processes	There should be processes in place to identify and capture business improvement opportunities by all levels of the organisation. We invest time and effort to improving the way we work rather than often making the same mistake over again.
6.14) Processes and systems help us to undertake business in a consistent way	There should be good processes and systems in place which are easy to understand and are followed. If there are poor processes and systems then consistency will be difficult to achieve.

3) Effective Control Environment

Risk is effectively and consistently managed within an explicit established and efficient internal control environment.

Column A lists the requirement and Column B provides guidance on the evaluation

Requirement	Guidance on Evaluation
3.1) Key controls are identified, documented and available in an accessible system or procedure documentation.	Normally a risk software package will capture critical controls in a multi-functional organisation. Procedural documentation should also clearly identify them.
3.2) The intent of each key control is included in the system information or procedure documentation.	Normally a risk software package is used. The point of this requirement is that unless it is documented what the control is supposed to achieve and how, then it is not possible to effectively assure and maintain it.
3.3) Key controls are known and used appropriately when required.	It is important that there is an awareness of the key controls and that they are applied in the appropriate manner at the right time in a process.
3.4) A systematic process is used for the design of controls using the results from risk assessment.	A procedure or standard that applies to all controls - not just those that apply to financial reporting and Workplace Health and Safety matters. Generally, the process will involve matching the controls to the causes of the risks. Also the controls should, in preference, control the likelihood of the consequences. Controls that mitigate the consequences once an event occurs are of secondary preference. For greatest efficiency, one control can treat a number or risks.
3.5) Staff have appropriate levels of understanding of the key controls relevant to their responsibilities.	Staff need to have a good understanding of the key controls which are relevant to their responsibilities so that they can undertake their roles in a competent manner.
3.6) Key controls are subject to planned testing by 'control owners'.	This process needs to be documented – in terms of what tests, when and by whom. Risk software packages can be used for this.

Requirement	Guidance on Evaluation
3.7) "Control self-assessments" by control owners are undertaken as planned activities.	This is a specific form of line management review conducted by designated control owners. It is a systematic process for evaluating controls against design intent and the current risk profile to ensure that the controls are adequate, effective and cost effective.
3.8) Cost/benefit analysis is normally applied as appropriate to risk treatment action selection.	The cost/benefits of risk mitigation actions are considered in a manner appropriate for the required action.
3.9) Both the what (performance) and the how (behaviour) counts in our organisation.	The manner in which we achieve outcomes is just as important as achieving outcomes. Our actions need to consider both.

4. Management Accountability

There is comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. This includes compliance activities

Column A lists the requirement and Column B provides guidance on the evaluation

Requirement	Guidance on Evaluation
4.1) Key controls are allocated to 'control owners' for monitoring and assurance	This allocation is accepted and known to the person. The allocation can be noted in the risk system or a position/job description or a procedure. The allocation should be to a named individual and not to a position. Risk should not be allocated to departments or to more than one named individual.
4.2) Significant risks in risk registers are allocated to 'risk owners' for monitoring and review.	This allocation is accepted and known to the person. The allocation can be noted in the risk register system or a position/job description or a procedure. The allocation should be to a named individual and not to a position. Risk should not be allocated to departments or to more than one named individual.
4.3) Tasks within risk treatment plans are allocated to risk owners or other designated staff.	This allocation is accepted and known to the person. The allocation can be noted in the risk system or other task or action tracking system.
4.4) An appropriately skilled professional has accountability for overseeing the effective operation of enterprise risk management processes	This should be a formal appointment recognised in a position description. Skill levels should be maintained by on-going professional development in risk management.
4.5) There is consideration of the effectiveness of the enterprise risk management framework by the Governance Committee	The Governance Committee's charter requires it to review whether management has in place a current and comprehensive risk management framework, and associated procedures for effective identification and management of WSC's financial and business risks, including fraud and corruption. The Committee also is required to consider processes around developing strategic risk management plans, the impact of the risk management framework on the organisation's control environment and the effectiveness of business continuity planning arrangements.
4.6) Position descriptions clearly define the level of risk accountability for the management of risk within the respective roles	A key element of success for effective risk management is that staff accountabilities in respect of risk management are well understood

Requirement	Guidance on Evaluation
4.7) "Delegation of authority" rules within WSC are based on 'risk exposure' not just dollar value where discretion is allowed under legislation.	This will be by using a measure of 'potential exposure' as well as residual risk.
4.8) Accountabilities are well managed	Staff should be held to account to meet their responsibilities. Clear guidance is given where improvement is required.

5) Core Organisational Process

The management and control of risk is viewed as central to the achievement of the organisations' objectives.

Requirement	Guidance on Evaluation
5.1) Decision making within WSC which involves significant consequences includes the consideration of relevant risks and the application of risk management processes.	Normally this would be required by policy and procedures. This may be covered by the change management system and/or an Enterprise Risk Management Framework.
5.2) Executive Team members consider risk from a positive (opportunity) and negative (consequence) perspective.	This is a crucial for effective and beneficial enterprise risk management. This is evident by the way risk is referred to in policies, procedures and in management-level discussions and papers.
5.3) Service Unit Managers consider risk from a positive (opportunity) and negative (consequence) perspective.	This is a crucial for effective and beneficial enterprise risk management. This is evident by the way risk is referred to in policies, procedures and in management-level discussions and papers.
5.4) WSC embraces risk where it can achieve a community benefit through effective management.	WSC will normally have regard to its risk appetite in seeking to take on greater risk to gain more beneficial outcomes for the community
5.5) Management identify risks to the organisation's success and communicate these to staff	Key risks and success factors are communicated regularly to staff
5.6) Decisions about major investments and incurring of liability involve the consideration of relevant risks.	Normally a "gateway" process is required where potential major investment opportunities go through a staged approval process before funding is made available. This should apply equally to liability incurring decisions such as supply contracts as it does to capital expenditure.
5.7) The objectives of the organisation are identified from a longer term strategic level through to a Service Unit service and product level.	An objective is an outcome to be achieved with available resources, to a defined timeframe and to required levels of performance and quality. These should be clearly identified in all key strategic documents such as WSC's Strategic Plan and the 26 Service Unit business plans.
5.8) The objectives of the organisation are clearly aligned across WSC, from longer-term strategic to service and product level.	There should be a clear alignment of objectives cascading down from the higher level Strategic Plan and through the organisation.
5.9) Risk management processes are embedded in all key organisational processes and are not stand alone or separate from the activities and processes of WSC.	This implies that WSC has mapped and risk assessed its most important processes in terms of the achievement of its objectives. All risk management processes, not just risk assessment, should be embedded.
5.10) Generally management does what it says it will do.	There is environment of "walk the talk" - there is a backing up of words with actions.

Requirement	Guidance on Evaluation
5.11) Management and staff generally work well together.	Inhibitors to effective integration such as silos, internal competitiveness and conflict needs to be largely absent from the organisation to enable effective integration of strategy and risk and control management so as to achieve the organisation's objectives.
5.12) Communication and consultation with external and internal stakeholders takes place (as appropriate) during all stages of the risk management process	There is effective engagement with relevant internal and external stakeholders when undertaking risk management processes.

6) Integral to Strategy Development

There is a clear and explicit linking of Risk and Control Management to Business strategy and plan development and achievement.

Column A lists the requirement and Column B provides guidance on the evaluation

Requirement	Guidance on Evaluation
6.1) WSC's strategic and business planning documents include a risk section that identifies risks and opportunities.	Systematic risk assessment is required. The control gaps revealed by the risk assessment should either lead to changes in the plan or to supplementary tasks to increase the likelihood that the objectives will be achieved.
6.2) WSC policy setting considers risks and opportunities.	This could be as part of a change management system. No policies are made or changed without the implications being assessed through risk assessment. The actual policy wordings can also be assessed.
6.3) The process of establishing KPIs considers risks and opportunities.	The setting of KPI's should take into account the level of risk to WSC if performance is outside specified performance levels.
6.4) When strategies are acted upon, there is a clear understanding of the risks and opportunities involved and associated actions	It is particularly important that where the business is 'taking on risk' the persons concerned should be aware of the risk, its magnitude and potential consequences. Normally there would be explicit limits or tolerances within a set risk appetite.
) WSC strategies are set with due reference to its level of risk appetite. (Risk appetite is the amount and type of risk that an organisation will pursue or retain.)	This implies that WSC has a clear understanding of its risk appetite – in keeping with its business model, vision and stakeholder expectations. Risk is treated as providing an opportunity for advantage and enterprise, not just as a source of loss. WSC should be able to engage in appropriate risk- taking activity knowing the risks involved the potential consequences and associated likelihoods and the controls required to be in place to manage the risk.
) Management make decisions for the long term, sometimes sacrificing short term gain	Decisions should reflect a more strategic approach rather than a focus on short term performance.

7) Management of Risk and Control Management Performance

Continuous improvement in risk management is achieved through the setting of WSC risk management performance goals, measurement, review and the subsequent modification of processes, systems, resources and capability/skills.

Column A lists the requirement and Column B provides guidance on the evaluation

Requirement	Guidance on Evaluation
7.1) There is an documented and up to date Risk Management plan for WSC	This should have been reviewed and revised in the last 6 months. The risk management plan should deal with improving the maturity of risk management in WSC. It should cover embedding risk management processes in key business processes, the improvement of risk and control management performance, the take up and improvement of control checking and assurance. It may also include training in risk management processes and any actions that are required to satisfy the requirements within this evaluation protocol. It should cover both the positive and negative aspects of risk management.
7.2) There is a documented Risk Management Framework for WSC which reflects good risk management practice	This should outline the key approaches and processes around risk management across the organisation and include the risk management policy and the key principles and processes of risk management. The framework should be supported by detailed guidelines in key areas such as risk assessment, appetite setting and risk culture.
7.3) A risk management maturity evaluation designed to identify improvement opportunities is undertaken at appropriate intervals	Normally as part of reporting to senior management and annually to the Governance Committee. It provides a benchmark for measurement of the maturity of risk management across the organisation.
7.4) There are appropriate risk management KPIs for Senior Executives and Service Unit Managers.	These should be explicit and recorded as part of personal performance goals. The KPIs should be measured against 'lead indicators' and should drive good risk and control management practice. They should not just be related to losses and accidents or other lag measures.
7.5) There are role models and leaders for risk management within WSC.	WSC should have in place a range of staff with risk and personal capabilities able to meet the evolving business needs of the organisation and effectively communicate the cultural change that is required to have enterprise risk management effectively in place across the organisation.
7.6) Requisite knowledge, expertise and experience in risk management are in place across the organisation.	Risk management knowledge needs to extend beyond management to all levels of the organisation. While staff do not have to be risk management experts, they do need to ensure that they are familiar with key risk management processes and are able to apply risk and innovative thinking in every day decision making.
7.7) Executive and Service Unit Managers undertake regular risk-related professional development	While managers do not have to be risk management experts, they do need to ensure that they are fully familiar with current risk management knowledge. This must extend beyond traditional risk knowledge such as financial and safety related risks or knowledge of risks in their own area of specific accountability. It needs to extend into innovative thinking around helping achieve strategic and operational objectives within their area and across WSC.
7.8) Risk management performance is measured and reported within Units and Departments	This should be part of normal business reporting within the WSC. Quarterly reporting to a Committee is not enough. The performance has to be communicated to all relevant stakeholders in WSC in a timely and informative manner.

Requirement	Guidance on Evaluation
7.9) Councillors apply risk management principles and processes to decision making	While councillors do not have to be risk management experts, they do need to ensure that they are familiar with current risk management standards and processes generally. They need to know how to bring risk thinking into the decision making process especially around strategic planning, policy setting, meeting their statutory obligations and understanding the organisation's capacity to deliver outcomes.

8) Contingency Management

If an event occurs that threatens WSC, employees, assets and/or services we have a viable and effective plan as to how we will act to minimise negative consequences

Column A lists the requirement and Column B provides guidance on the evaluation

Requirement	Guidance on Evaluation
8.1) There is a crisis/emergency plan or plans.	These must be written plans – not just based on thoughts or conversations.
8.2) The plans deal with types of events that can significantly affect the continuity of the WSC's operations and revenue stream.	All types of events must be covered, both internal and external to WSC. This includes transport/logistics failures, weather events, bushfire, industrial disputes, failure of critical equipment and systems, loss of access to premises, failure of contracting and partner companies etc.
8.3) The plans are tested in accordance with the planned testing program	At least by table top exercises that were rigorously conducted and necessary improvements made to the plan.
8.4) The plans are up to date. If it were initiated now, all the information is current and reliable. This implies that there is specific activity to keep the plan up to date. All named individuals and roles are current.	At this moment, they could all access a copy of the plan – even if they were away from the premises. They must be fully aware of their roles and be capable of fulfilling them.
8.5) All persons that have a specific role in the plans have a copy of the plan and have been trained in their roles within the last 2 years.	At this moment, they could all access a copy of the plan –even if they were away from the premises. They must be fully aware of their roles and be capable of fulfilling them.

6.7) RISK APPETITE

WYONG SHIRE COUNCIL

Enterprise Risk Management Strategy

Column A states the risk and Column B shows the metric

RISK APPETITE

RISK APPETITE – the amount and type of risk that WSC is prepared to pursue, retain or take in order to achieve its objectives

Statement	Metric
Compliance / Reputation	
WSC has an appetite for maintaining levels of satisfaction in the community	75% customer satisfaction with the service provided by Customer Contact Reducing year-on-year number of upheld complaints
WSC will develop and maintain a reputation for providing value for money services, and friendly customer service	75% customer satisfaction with the service provided by Customer Contact
WSC has an appetite for doing the right thing and being seen to do the right thing	Number of annual positive citations (local or state level)
WSC has an appetite for acting and responding consistently and appropriately in all its dealings with stakeholders and constituents	Zero upheld complaints of bias or partiality
WSC will comply with its legal, professional and regulatory compliance obligations – avoiding litigation, fines, or the imposition of restrictions that affect its ability to operate	Reducing year-on-year number and severity of breaches
Financial Management	
WSC will meet agreed financial targets to support our long term financial sustainability	Achievement of financial sustainability targets as defined in the Long Term Financial Strategy.
WSC has an appetite for maximising revenue to fund existing services, including opportunities for: full cost recovery user pays new revenue streams	Achieve 100% of target revenue budget
WSC will maximise opportunities for successfully obtaining grant applications and special rate increases to help redress recurrent funding shortfalls	
WSC has an appetite for pursuing operational efficiencies by increasing shared service activities and working relationships with other councils or partners	Achieve program targets for CCWC and Joint Services

RISK APPETITE – the amount and type of risk that WSC is prepared to pursue, retain or take in order to achieve its objectives	
Statement	**Metric**

Asset Management

WSC will provide and maintain “fit for purpose” assets in a timely manner to meet community expectations WSC will manage its infrastructure and assets in a systematic and sustainable manner, ensuring that life cycle costs are optimised (for both existing and new assets) Asset renewals will be prioritised to align with priority objectives of the WSC Strategic Plan WSC will prioritise capital expenditure to optimise alignment with strategic objectives and produce optimal outcomes for the investments made	Achievement of objectives and targets defined in the WSC Asset Management Policy

Development and Environment

WSC has an appetite for pursuing opportunities to utilise and capitalise on cultural and environmental heritage	
WSC has an appetite for encouraging cooperative approaches to feasible and realistic development proposals	
WSC has an appetite for pursuing initiatives that result in net gains in Wyong’s environmental heritage	
WSC has an appetite for improving the existing natural environment including wetlands, bushland, beaches, dunes, stream banks, and foreshores	Year-on-year improvements using a standardised measure

Service Performance / Community Outcomes

WSC will fulfil priority objectives as defined in the Community Strategic Plan in a manner that reflects the priorities and expectations of the community	
WSC will seek to avoid commitments that cannot be fulfilled WSC has an appetite for substantially delivering upon its commitments	< 5% variance from expected operations, performance or outcomes
WSC has an appetite for achieving best value outcomes for the Wyong community WSC has an appetite for consistently delivering its services to the Wyong community WSC has an appetite for developing and applying controls that contribute to a liveable and amenable	>90% KPI achievement
WSC will prioritise projects based on Project Assessment Criteria WSC has an appetite for managing projects within budget (including contingency provisions) and on time WSC will engage the community in all key projects	All major projects (designated in the Annual Plan) are delivered in accordance with their approved work program. At least 80% of all projects are completed on time and on budget

RISK APPETITE – the amount and type of risk that WSC is prepared to pursue, retain or take in order to achieve its objectives	
Statement	**Metric**

Workforce Management

WSC is committed to implementing policy and systems, leadership, accountability, and consultation in order to maintain a safe and healthy work environment The safety of our Workers will take priority over competing interests WSC will pursue opportunities to minimise WHS risks to our Workers, and to achieve WHS performance objectives	Lost Time Injury Frequency < 28
WSC has an appetite for maintaining its self-insured status	Ongoing unqualified 3-year licence renewals
WSC will seek to optimise resources, to have the right people in the right job at the right time within budget	
WSC will develop and sustain a skilled and knowledgeable workforce to support its ability to deliver future programs and services	Achieve 100% of HR targets as defined in the WSC Workforce Management Strategy
WSC has an appetite for supporting and retaining committed, experienced and talented staff	Permanent staff turnover <10%

6.8) WSC RISK TABLES

Wyong Council Risk Tables Stage 2 Revision 1.1: May 2013

Consequence Table

		Work, Health &Safety	Socio-economic	Regulatory/ Compliance (including Environment, Cultural & Heritage Protection)	Reputation	Financial	Business Continuity
A	**Catastrophic**	1 or more deaths, serious disability	✗	Significant breach of legal, regulatory requirement or duty; prosecution; custodial sentence; Council dismissed.	✗	>$10,000,000	✗
B	**Major**	Serious injury (Major surgery > 2 months admission)	✗ .	Substantial breach of legal, regulatory requirement or duty; likely fines, prosecution and/ or litigation	✗	$1,000,000 to $10,000,000	✗
C	**Moderate**	Significant injury 1 – 2 months absence	Moderate adverse impact on community specifically affected by the activity.	Breach of legal, regulatory requirement or duty; enforcement action or prohibition notices imposed	Significant Community dissatisfaction State coverage. Reputation recoverable in the long term.	$500,000 to $1,000,000	Unable to undertake business for (1) one week
D	**Minor**	First aid or medical attention required no long lasting effects	Minor adverse impact on community specifically affected by the activity.	Non-compliance of legal, regulatory requirement or duty; monitoring by external regulator	Expressed community dissatisfaction local coverage. Reputation recoverable in the medium term.	$10,000 to $500,000	Unable to undertake business for two to three (3) days.
E	**Insignificant**	No absence	Little adverse impact on community specifically affected by the activity. .	Minor non-compliance of legal, regulatory requirement or duty; investigation, not reportable.	May cause minor public concern	$1,000 to $10,000	Unable to undertake business for twenty four(24) hours

Likelihood Table

	Descriptor (Project)	Indicative frequency (Whole of Life)	Probability
Almost certain	Almost certain to occur	Once a year or more frequently	> 85%
Likely	More than an even chance of occurring	Once every 2 years	50 - 85%
Possible	Could occur quite often	Once every 5 years	21 - 49%
Unlikely	It is possible for the event to occur, but it is unlikely to happen.	Once every 10 years	5 - 20%
Rare	Event that may occur very seldom and the chances of it happening are considered exceptionally remote	Once every 20 years	< 5%

Level of Risk Table

	A	B	C	D	E
			Consequence		
Likelihood	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost certain	**1**	**3**	**6**	**10**	**15**
Likely	**2**	**5**	**9**	**14**	**19**
Possible	**4**	**8**	**13**	**18**	22
Unlikely	**7**	**12**	**17**	21	24
Rare	**11**	**16**	20	23	25

6.9) RISK RESPONSE BUSINESS RULES

Column A in the table contains the risk and following columns explains the rating from low, medium, high and extreme.

	Business Rules for Various Risk Ratings			
	Low	Medium	High	Extreme
General Characteristics	This risk lies within the bounds of Council's current risk appetite. Council will accept this risk and manage the risk using existing processes and controls.	This risk lies within the bounds of Council's current risk appetite. Council will tolerate this risk, however cost effective risk treatments for reducing threats or optimising benefits should be identified.	This risk lies beyond the bounds of Council's current risk appetite. Council will only accept this risk if it is not cost-effective to implement controls to reduce the level of risk exposure. Action is required reduce this risk to Tolerable or better. Proactive management by Service Unit Managers is required to ensure that this risk does not escalate to Intolerable.	This risk lies beyond the bounds of Council's current risk tolerance and Council will not tolerate this risk. Action is required to reduce the risk to Unacceptable or better. If the risk cannot be reduced, then continuation of the activities leading to the risk exposure must be subject to the highest level of review, considering potential benefits to Council. There must be explicit acceptance of the risk and implementation of
Risk Treatment This identifies Council expectations for identification of risk treatments.	Proposed risk treatments may be identified to reduce the risk consequence, likelihood or both.	Cost effective risk treatments for reducing threats or optimising benefits should be identified.	Proposed risk treatments must be identified to reduce the risk consequence, likelihood or both.	Proposed risk treatments must be identified to reduce the risk consequence, likelihood or both.
Residual Risk This identifies Council expectations for estimating post-treatment residual risk.	Residual risk need not be estimated	Residual risk need not be estimated	Anticipated post-treatment residual risk must be estimated.	Anticipated post-treatment residual risk must be estimated.

	Residual Risk			
	Low	Medium	High	Extreme
Decision Making This characteristic identifies Council expectations for decision-making including whether to proceed with the proposed action or strategy given Council's risk exposure, and whether the proposed risk treatments are considered adequate.	Decisions to be made within existing delegated authorities and processes.	Risk assessment and proposed risk treatments to be reviewed by the Service Unit Manager or higher.	Risk assessment and proposed risk treatments to be reviewed by the ELT. Decision to proceed subject to endorsement by the ELT.	Risk assessment and proposed risk treatments to be reviewed by the ELT or higher. Decision to proceed subject to endorsement by the ELT and elected Council
Risk Ownership A Risk Owner is the person (or position) with accountability and authority to manage a risk.	No requirement to identify Risk Owners	No requirement to identify Risk Owners	Risk Owner must be nominated (Service Unit Manager or above)	Risk Owner must be nominated (Director or above)

6.10) REFERENCES

Column A in the Table identifies the Title and Publisher and Column B is the description of the title.

Title and Publisher	Description
AS/NZS ISO 31000:2009 Risk management – principles and guidelines, Standards Australia	This International Standard provides principles and generic guidelines on risk management. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences. It can also be applied throughout an organisation, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.
HB 158:2010 Delivering assurance based on ISO 31000:2009 Risk management—Principles and guidelines	HB 158:2010 draws on the Institute of Internal Auditors' International Professional Practices Framework with respect to using and assuring the ISO 31000:2009 risk management process. In particular, it describes how to use the risk management process to: • develop a risk-based assurance strategy and program • plan an assurance engagement • report the assurance program • design controls. The Handbook also provides a guide to assessing the adequacy of risk management framework and process.
HB 203:2012 Managing environment-related risk	Handbook HB 203:2012 discusses how AS/NZS ISO 31000:2009 can be used to help an organisation manage environment-related risks, including risks to the environment and from the environment.
Internal Audit Guidelines (2010), Division of Local Government, NSW Department of Premier and Cabinet	These Guidelines are Director General's Guidelines for the purposes of section 23A of the Local Government Act 1993, issued by the Chief Executive, Local Government under delegated authority. The Guidelines are designed to provide councils with assistance to implement internal audit and risk management. The Guidelines also include appropriate structures, functions, charter, and membership of audit and risk management committees.
ISO Guide 73:2009 Risk management - Vocabulary	The Guide provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.
ISO/IEC 31010:2009 Risk management - Risk assessment techniques	This International Standard is a supporting standard for AS/NZS ISO 31000:2009 and provides guidance on selection and application of systematic techniques for risk assessment. The application of a range of techniques is introduced, with specific references to other international standards where the concept and application of techniques are described in greater detail.

Title and Publisher	Description
Project Risk Management Guideline (2011), NSW Department of Finance and Services	The objective of this guideline is to provide guidance to project teams and project stakeholders on the application of the standard risk management process to Information and Communications Technology Governance (ICT) projects and programs in the NSW Government. It is applicable to ICT projects and programs of all sizes and its principles and techniques are applicable to risk management for other programs, projects, plans and activities.
PMBoK Practice Standard for Project Risk Management (2009), The Project Management Institute Inc.	The Practice Standard for Project Risk Management provides a standard for project management practitioners that aligns with the PMBoK Guide. The document also provides a source of tools, techniques and templates for project risk management.

Black Swans – https://www.thenbs.com/topics/practicemanagement/articles/riskAssessmentAndBlackSwans.asp (access 16 Oct 12)

AS8000:2003 Corporate Governance

Corporate Governance – Strategic Early Warning System NSW Auditor- General's Report Volume Two (2011)

Enterprise Risk Management Manual (Coffs Harbour City Council, Nov 2011) Risk culture –

http://www.insurancebusinessonline.com.au/cri/article/risk-culture-all-talk-and-no-action-126516.aspx

Risk culture – http://www.insurancebusinessonline.com.au/cri/article/5- essential-findings-for-risk-professionals-142846.aspx (access 25 Aug 12)

Risk culture – http://www.audit.nsw.gov.au/ArticleDocuments/234/01_Volume_One_2012_Full_Report_v3.pdf.aspx?Embed=Y (access13 Apr 12)

Bias and group-think – http://www.iia.org.au/Libraries/SOPAC_-_Previous_ Confs/5F.sflb.ashx

Commonwealth Guidelines for Managing Risk in the Australian Public Service (refer www.apsc.gov.au/mac/index.htm)

Public Sector Governance Volume 16 which describes the key components of effective risk management, as well as the importance of developing a risk management culture (see www.anao.gov.au)

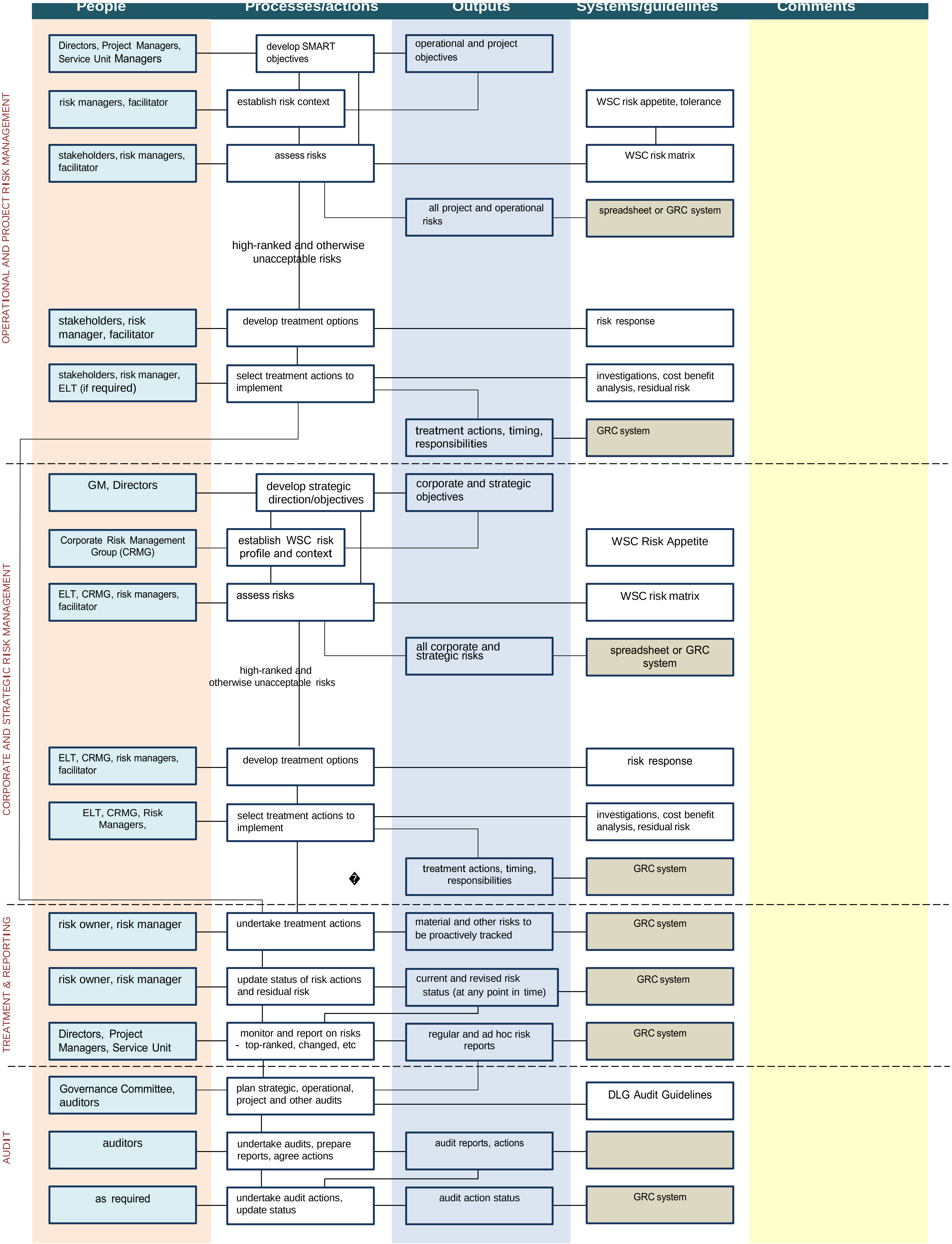
Public sector risk management (see www.cpaaustralia.com.au/ 20_cpastore):

6.10)1. Case Studies in Public Sector Risk Management: Better Practice Guide
6.10)2. Enterprise-wide Risk Management: Better Practice Guide
6.10)3. Public Sector Risk Management: A State of Play
6.10)4. Research Report on Public Sector Risk Management.

6.11) RISK MANAGEMENT PROCESS MAP

WYONG SHIRE COUNCIL
Enterprise Risk Management Strategy

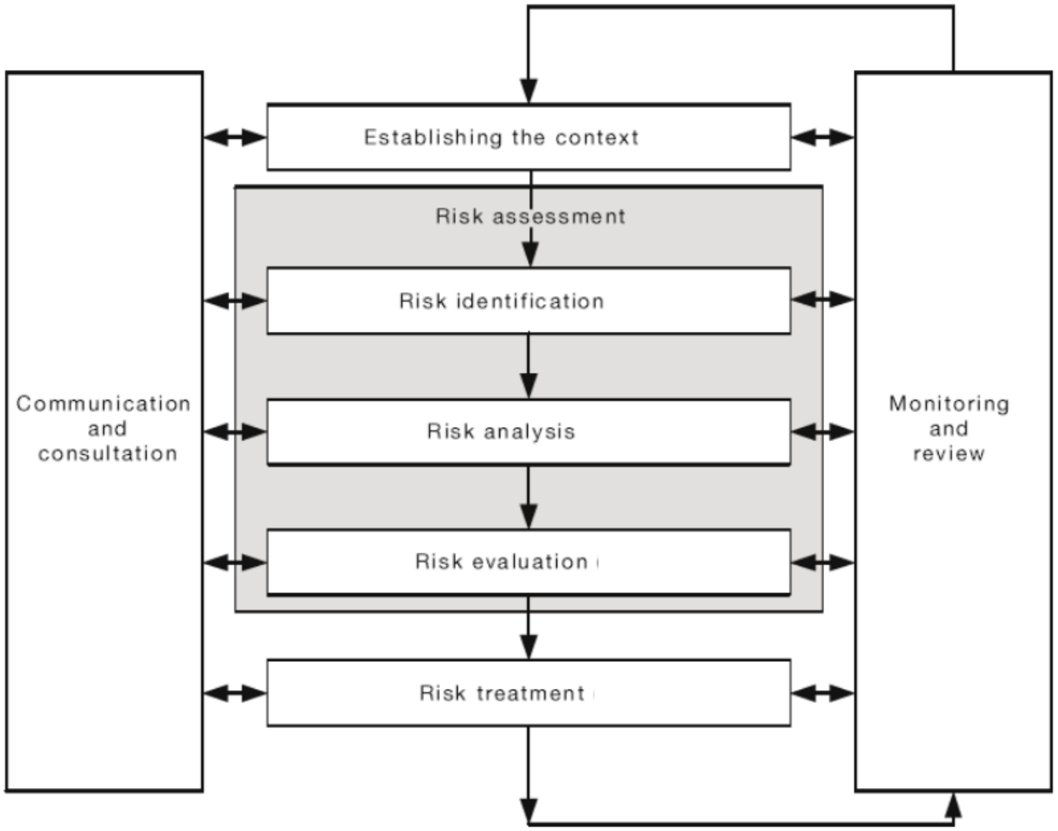
DRAFT ERM FRAMEWORK OPERATION



	People	Processes/actions	Outputs	Systems/guidelines	Comments
OPERATIONAL AND PROJECT RISK MANAGEMENT	Directors, Project Managers, Service Unit Managers	develop SMART objectives	operational and project objectives		
	risk managers, facilitator	establish risk context		WSC risk appetite, tolerance	
	stakeholders, risk managers, facilitator	assess risks		WSC risk matrix	
			all project and operational risks	spreadsheet or GRC system	
		high-ranked and otherwise unacceptable risks			
	stakeholders, risk manager, facilitator	develop treatment options		risk response	
	stakeholders, risk manager, ELT (if required)	select treatment actions to implement		investigations, cost benefit analysis, residual risk	
			treatment actions, timing, responsibilities	GRC system	
CORPORATE AND STRATEGIC RISK MANAGEMENT	GM, Directors	develop strategic direction/objectives	corporate and strategic objectives		
	Corporate Risk Management Group (CRMG)	establish WSC risk profile and context		WSC Risk Appetite	
	ELT, CRMG, risk managers, facilitator	assess risks		WSC risk matrix	
			all corporate and strategic risks	spreadsheet or GRC system	
		high-ranked and otherwise unacceptable risks			
	ELT, CRMG, risk managers, facilitator	develop treatment options		risk response	
	ELT, CRMG, Risk Managers,	select treatment actions to implement		investigations, cost benefit analysis, residual risk	
		�	treatment actions, timing, responsibilities	GRC system	
TREATMENT & REPORTING	risk owner, risk manager	undertake treatment actions	material and other risks to be proactively tracked	GRC system	
	risk owner, risk manager	update status of risk actions and residual risk	current and revised risk status (at any point in time)	GRC system	
	Directors, Project Managers, Service Unit	monitor and report on risks - top-ranked, changed, etc	regular and ad hoc risk reports	GRC system	
AUDIT	Governance Committee, auditors	plan strategic, operational, project and other audits		DLG Audit Guidelines	
	auditors	undertake audits, prepare reports, agree actions	audit reports, actions		
	as required	undertake audit actions, update status	audit action status	GRC system	

6.12) RISK ASSESSMENT

The risk management process defined in AS/NZS ISO 31000:2009 Risk management – principles and guidelines comprises seven elements, as represented in the diagram below.



The elements of the risk management process are:

- Communication and consultation – communication and consultation with external and internal stakeholders should occur during all stages of the risk management process. This ensures that stakeholders as well as those accountable for implementing the risk management process understand the basis on which decisions are made, and the reasons why particular actions are required.

- Establishing the context – establish the external, internal, and risk management context in which the risk management process will take place. In establishing context, WSC articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope for the remaining processes.

- Risk assessment – risk assessment is the overall process of risk identification, risk analysis and risk evaluation.
    - Risk identification – the aim is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate, delay or otherwise impact on the achievement of objectives.
    - Risk analysis – risk is analysed by determining the consequences of risk events, the likelihood of their occurrence, and other attributes of the risk. It informs risk evaluation and potential risk treatment.
    - Risk evaluation – involves comparing the level of risk with pre-established risk criteria and making decisions about which risks need treatment and the priority for treatment implementation.
- Risk treatment – risk treatment involves selecting one or more options for modifying risks, and implementing those options.
- Monitoring and review – monitoring the implementation and effectiveness of risk treatments, and reviewing, updating and reporting on the entire risk environment to detect, assess and respond to changes.

The following sections provide guidance for implementing each element of the risk management process.

6.12.01) Communication and consultation

Communication and consultation are important considerations at each stage of the risk management process (and which itself does not have a finite timeframe).

A consultative approach involving all relevant stakeholders must be utilised to define the context for and inputs into a risk assessment and provide confidence that all reasonably foreseeable risks are identified. This promotes ownership of the risk assessment outcomes, an appreciation of the benefits of the risk controls, and support for the risk assessment plan.

Effective risk communication ensures that those responsible for implementing risk management and those with an interest in the outcomes understand the basis on which risk management decisions are made and why particular actions are required.

6.12.02) Establish the context

Establishing the context articulates the relevant strategic, operational or project objectives, defines the parameters within which risks must be considered and managed, and sets the scope for the remainder of the risk management process.

Questions to inform the risk management context include:

- have objectives been defined and agreed/approved?
- are the objectives well defined (are they SMART objectives – specific, measurable, achievable, relevant and timely)?
- what is to be achieved from the risk management process?

- what outcomes are being sought?
- what opportunities or benefits might be achieved?
- what decisions will need to be made?
- who will be involved in or affected by the activities and objectives under consideration?
- who are the significant stakeholders (both internal and external)?
- should they be involved in the risk assessment?
- what is the internal context – including strategic direction, recent or proposed organisational change, budget constraints, resource capacity and capability, performance expectations, governance arrangements, information availability, target timeframes, policies and procedures?
- what is the external context – including the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment?
- are there benefits to be gained by involving subject matter experts in the risk assessment, or independent personnel who can provide a "fresh set of eyes"?
- are there lessons from previous risk assessments and comparable projects that might assist the risk assessment?
- what background information and data is needed to inform the risk assessment e.g. information regarding current and projected resourcing levels, budget, cashflow, program, assumptions, current budget and program contingencies, performance data, regulatory or contractual obligations?

6.12.02.01) Strategic risk context

Context for assessment of WSC's strategic risks should be informed by:

- WSC strategies prepared in response to the NSW Division of Local Government Integrated Planning and Reporting framework (including the Community Strategic Plan, Delivery Program, Operational Plan, and Strategic Plan)
- other WSC strategic planning documents
- WSC's strategic risk profile
- WSC's defined risk appetite.

6.12.02.02) Operational risk context

Context for assessment of WSC's operational risks should be informed by:

- operational objectives, key performance indicators, and performance targets as defined in WSC strategies and Service Unit Business Plans
- requirements defined in WSC's operating policies and procedures
- WSC's strategic risk profile
- WSC's defined risk appetite

6.12.02.03) Project risk context

Context for assessment of project risks should include reference to the business case and project plan, and be informed by:

- the purpose and objectives of the project
- the outcomes and benefits to be derived from the project
- operational and strategic risks impacting on the project
- WSC's defined risk appetite.

6.12.02.04 Determine potential exposure

In establishing context, consideration should be given to whether WSC's potential exposure needs to be determined. Potential exposure (also known as inherent risk) deliberately assumes the absence of any existing risk controls.

It introduces a different context for risk assessment that should be applied:

- when determining maximum potential exposures as a basis for prioritising further risk assessment (for example, when developing WSC's high-level strategic risk profile)
- when determining maximum potential exposures as a basis for assessing the adequacy of WSC's insurance coverage
- to identify maximum potential exposure in the event of critical control failure (for example, non-availability of key staff, business disruption, fraud and corruption, or IT system control failure)
- for new services or projects where there is an absence of established risk controls
- where there is a lack of confidence in the reliability or effectiveness of existing risk controls.

6.12.03 Identify the risks

Risk identification is the process of identifying risks having an effect on the achievement of objectives. It involves the identification of risk sources, risk events, their causes and potential consequences.

Risk identification involves thinking about what, when, where, why and how events can occur that may prevent WSC from achieving its strategic, operational or project objectives.

6.12.03.01 Apply a structured approach

Identifying the effect of risk events on the achievement of objectives is fundamental to effective risk management. Risk assessment should work through the list of relevant objectives one by one, identifying the full range of risk events across all risk categories that potentially impact each objective.

Risk events include threats that objectives will not be achieved, as well as opportunities that exceed current objectives.

Risk identification should include risks whether or not they are under the control or influence of WSC.

Should an identical risk event be identified for more than one objective, rationalise identified risk events to remove duplicates.

Risks that are not identified cannot be assessed, and remain a source of unknown, unquantified and unexpected exposure for the organisation.

6.12.03.02) Risk event statements

Document risk event descriptions in the risk register in sufficient detail so that they can be understood by a variety of stakeholders, particularly those who were not part of the risk assessment process.

For clarity and consistency, risk event descriptions should be expressed in the form “x leads to y”, where x is a specific event and y is a specific description of the resulting consequences. For example:

- failure to secure grant funding leads to a significant reduction in the annual operating budget (> $50,000)

- difficulty in recruiting experienced supervisory resources leads to poor quality frontline service delivery

- a significant increase in project scope leads to a major project cost increase (>10% of project budget).

6.12.03.03) Risk identification methods

There are a number of different methods to identify risk events, which can be applied individually or in combination:

- brainstorming sessions with stakeholders
- an examination of previous comparable events/projects/activities
- fault tree or event tree analysis
- checklists developed for similar events/projects/activities.

Note that risk management requires participants to think, and the use of past risk events and checklists should never be a substitute for detailed, structured analysis.

Questions to be asked when identifying risks include:

- what can happen?
- where can it happen?
- when can it happen?
- why would it happen?
- how can it happen?
- what would cause it to happen?
- what else happens?

The following may assist the identification of risks:

- Attachment 6.2 includes a sample of risks relevant to local government
- Attachment 6.3 includes a sample of project delivery risks.

Note that these resources should be used as prompts to assist risk identification brainstorming by individuals and stakeholder groups, and should never be adopted verbatim, or considered to be comprehensive.

6.12.03.04) Select risk events

When identifying risk events there are typically a range of similar risk events along a spectrum that can be identified and used as a basis for risk assessment. The following table provides some examples of similar risk events at opposite extremes of the spectrum (representing worst case and most likely risk events).
The left column identifies the worst case risk event and the right column identifies the most likely risk event.

Worst case risk event	Most likely risk event
Fire or spill: Major fire or chemical spill requiring emergency response that prevents access to WSC's administration building for an extended period, with major disruption to services	Fire or spill: Multiple minor fires or chemical spills occurring in the field throughout the year requiring local response and resulting in minor injuries and temporary, localised operational disruption
ICT failure: ICT system failure that results in loss of business-critical information for an extended period (>1 week)	ICT failure: Recurring, localised IT system failures that have negligible business impact and are rectified rapidly (<2 hours)
Scope creep: Major increase in project scope (with major consequences for the project budget) due to clarification of user needs for a critical high-cost project component	Scope creep: Recurring minor increases in project scope due to poor definition of user needs and/or poor ongoing scope control processes

Risk identification can be based on:

- worst case: risk event having the worst case consequence scenario that could reasonably occur, irrespective of likelihood

- likely worst case: risk event having a worst case consequence scenario that has at least a 50% chance (say) of occurring during the timeframe being considered

- most likely: risk event having the most likely consequence.

Different risk identification approaches will lead to very different risk assessment results, and require different risk treatments.

The most common technique used is likely worst case, and this will be the default technique used for WSC risk assessments.

It is important for participants to be conscious of the technique applied for the risk identification and to apply the technique consistently throughout the risk identification process.

6.12.03.05) Root cause analysis

Root cause analysis is a structured approach to identifying the causes that can lead to the risk event. WSC's risk register template provides the opportunity to record three levels of causation – that is, to ask "why" up to three times.

Root cause analysis is valuable because it provides an opportunity to better understand and record the real causes of specific risk events, and increases the chance that:

- the likelihood of a risk event will be analysed accurately (reflecting the root cause)

- risk treatments will be identified that respond to the root cause

6.12.04) Analyse the risks

Once all risks have been identified, the next step in the risk management process is to analyse the risks. Risk analysis determines the level of risk as a basis for risk evaluation and decisions about risk treatment. WSC's preferred approach for risk analysis is a semi-quantitative approach using the WSC Risk Tables.

Should further analysis be required, a number of other quantitative and qualitative techniques are available depending upon the needs of the risk assessment and the available data.

Risks are analysed by determining their consequences and likelihoods. The effectiveness of existing controls should also be taken into account, where existing controls are in place, known and operating effectively.

WSC's risk register template will be used to record:

- all of the foregoing details e.g. project/strategy/service, risk event
- the risk consequence category selected as the primary consequence as the basis for risk analysis
- details of any existing controls that mitigate exposure and considered as part of the consequence and/or likelihood rating
- the consequence and likelihood ratings applicable to the risk event
- comments providing additional context for the risk analysis (including assumptions regarding the effectiveness of existing controls).

6.12.04.01) Analyse consequence

The Risk Tables identify a number of risk categories applicable for WSC, as follows:

- work health and safety – risk events affecting the safety and wellbeing of staff, volunteers, contractors, visitors and the public
- environment – risk events affecting environmental outcomes and the achievement of WSC's environmental objectives
- socio-economic – risk events affecting the social fabric of the Central Coast community and its economic performance and development
- cultural-heritage – risk events affecting people indicators and employee attraction and selection outcomes
- regulatory/compliance – risk events affecting legal, professional or regulatory compliance
- reputation – risk events affecting staff and community confidence in WSC operations
- financial (enterprise level) – risk events affecting WSC's financial objectives (including

short term and long term financial objectives)

- business systems – risk events affecting the continuity and delivery of WSC’s business activities
- fraud and corruption – risk events affecting the lawful and ethical discharge of WSC activities by WSC staff and those with which it interacts.

Assess the consequence using the Risk Tables to identify which consequence descriptions (A – catastrophic through E – insignificant) best align with the consequence for this risk event.

Where a risk event has multiple consequences, risk analysis should focus on the consequence having the greatest impact on WSC objectives.

6.12.04.02) Analyse likelihood

Use the likelihood ratings in the Risk Tables to identify the likelihood of the consequence occurring, ranging from almost certain to rare.

Assess likelihood based on records of past risk events, personal experience or a collective judgement, taking into account the appropriate planning horizon e.g.

- WSC’s 4 and 10 year planning cycle
- Service Unit annual planning cycle
- project duration (for project risks).

6.12.04.03) Existing controls

The effect of existing controls must be considered when analysing consequence and likelihood. Existing controls may reduce the likelihood of an event occurring, or the consequences should the event occur, or both. Existing controls may include:

- training
- policies and procedures
- defined roles, responsibilities and authority
- checking and approvals processes
- monitoring or supervision
- escalation and reporting processes
- physical and information controls.

If controls are under development or being planned but are not yet in place, their mitigating effect should not be considered as part of the risk assessment process. Only controls that are in place and working should be included.

6.12.05) Evaluate the risks

Risk evaluation assists in deciding which risks require treatment and the priority for treatment implementation.

6.12.05.01 Risk evaluation

WSC's risk evaluation is documented in its Risk Tables (Attachment 6.9) and Risk Responses (Attachment 6.10), both of which derive from WSC's risk appetite.

Use the consequence and likelihood ratings in the Corporate Risk Assessment Tables to identify a risk rating of:

- extreme (red)
- high (yellow)
- medium (light blue)
- low (white).

WSC's risk register template will automatically establish the overall risk rating based on consequence and likelihood ratings entered.

WSC's Risk Response table defines expectations for responding to risks under the above ratings including:

- the need to identify risk treatments
- the analysis of residual risk
- escalation of risks for decision making
- the nomination of risk owners.

6.12.05.02) Prioritisation

A common challenge is that too many high ranked (unacceptable) risks are identified that require treatment, with insufficient time and resources available to address all of them in a timely manner.

Therefore, WSC accepts that (in addition to the evaluation process identified above) unacceptable risks can be subject to further informed prioritisation to ensure that practical and achievable risk treatment strategies are implemented to provide the greatest value to WSC. This approach is consistent with AS/NZS ISO 31000:2009 Risk management – principles and guidelines.

The basis for prioritisation must be recorded on the risk register and can include:

- the timeframe in which the consequences will occur, or the timeframe in which associated risk treatments would need to be completed (informing the relative urgency of risk treatment)

- the possibility of foreseeable changes in the internal or external environment which are likely to increase or reduce the risk rating in the near future (for example, changes to legislation, changes to resourcing, dependencies on progress with other WSC initiatives)

- uncertainty around the accuracy of the risk analysis, where further investigation and analysis may be required to better inform the risk analysis prior to agreeing the final priority for a particular risk.

6.12.06) Identify risk treatments

Risk treatment involves:

- identifying one or more options for modifying risks
- evaluating risk treatment options to identify the preferred option(s)
- implementing the preferred risk treatment options.

Risk treatment options are additional to existing controls and can include:

- avoiding the risk by deciding not to undertake the activity giving rise to the risk
- taking or increasing the risk in order to pursue an opportunity
- removing the risk source
- changing the likelihood
- changing the consequences
- sharing the risk with another party or parties e.g. contract conditions, insurances, risk financing
- retaining the risk by informed decision and conscious acceptance.

Risk treatment is about managing risk not necessarily eliminating it.

6.12.06.01) Business rules for risk response

WSC's Risk Response Business Rules (refer Attachment 6.10) identify what to do under various risk ratings, including the development of risk treatments for all risks rated as unacceptable and intolerable.

6.12.06.02) Select preferred risk treatments

Risk treatment is about managing risk, but not necessarily eliminating it. The key is to strike the right balance to be in a position where WSC knowingly take on reasonable risk, rather than being unwittingly exposed to it.

Selecting the most appropriate risk treatment option involves balancing the costs of implementing each option against the benefits to be derived from it. It is important to consider all direct and indirect costs and benefits, both tangible and intangible.

Monitoring and review activities are a particular type of risk treatment that may be appropriate where further information needs to be obtained to properly understand the risk.

Questions to confirm whether proposed risk treatments will be effective include:

- is there an understanding of how the risk treatments will modify the risk?

- does cost/benefit analysis favour the proposed risk treatment?

- is it likely that the risk treatment will be implemented in a timely and effective manner (if not, consider alternatives)?

- if the risk treatment is implemented effectively, is there confidence that the level of risk will be reduced to an acceptable level?

- how can the effects of the risk treatment be measured to confirm its effectiveness?

- will there be clear accountability for implementing the risk treatments?

- where applicable, what ongoing monitoring and review might be needed to confirm that the risk treatments remain effective?

6.12.06.03) Record preferred risk treatments

When defining existing controls and considering new ones, be specific about how the risk controls mitigate the risks. For example, in a purchasing process 'segregation' may be a control but a more specific and informative description would be 'introduce procurement processes that ensure separation between those responsible for raising a payment order and those authorising payment'.

WSC's risk register template should be used to record:

- the risk owner (the role having overall responsibility for management of the risk and implementation of risk treatments)

- a description of each agreed risk treatment

- the target timeframe for implementation of each risk treatment.

6.12.06.04) Determine residual risk

Residual risk is the risk remaining after risk treatment. The assessment of residual risk assists management to demonstrate due diligence by providing confidence that unacceptable and intolerable risks can be reduced to more acceptable levels, subject to the effective implementation of the proposed risk treatments.

The assessment of residual risk is not required for all risks. WSC's Risk Response table (see Attachment 6.10) identifies requirements for the assessment of residual risk which should be recorded in the risk register.

Residual risk are assessed assuming that the nominated risk treatments have been effectively implemented.

6.12.07) Monitor and review

The risk management process is an ongoing one. It is essential to consider appropriate ongoing monitoring and review proce3sses and timing so that all risks having nominated risk treatments are monitored on a regular basis for the purposes of:

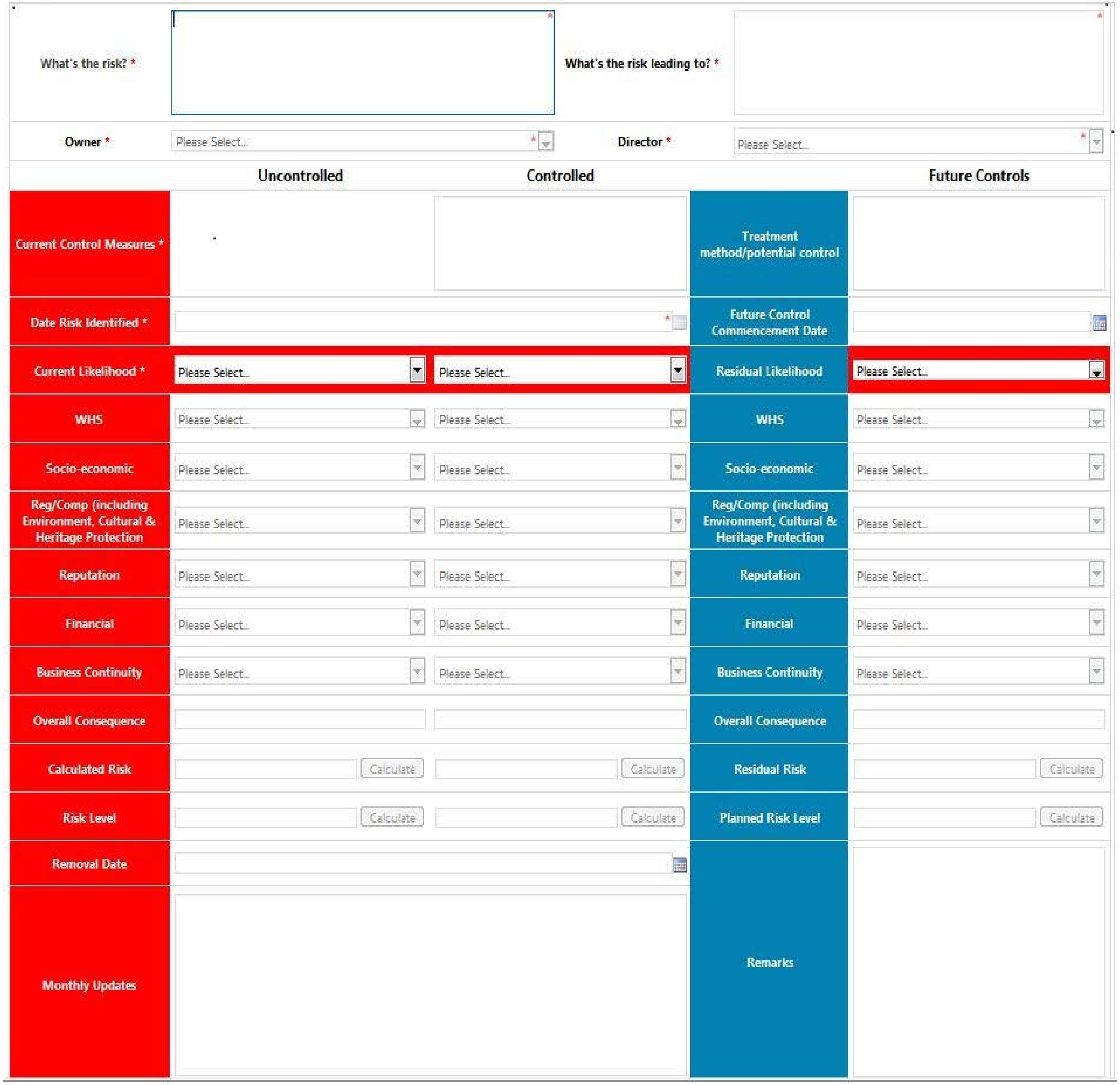
- ensuring that controls are effective and efficient in both design and operation
- obtaining further information to improve risk assessment
- analysing and learning lessons from events (including near-misses), changes, trends, successes and failures
- detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk assessments, treatments and priorities
- identifying emerging risks.

Agreed monitoring and review activities must be recorded using WSC’s risk register.

Questions to consider when planning risk monitoring and review activities include:

- what are the benefits of monitoring and review (how will it help optimise outcomes)?
- what information should monitoring and review identify?
- how often should monitoring and review occur?
- what monitoring or review activities would be most effective (for example, audits, customer survey, media reports, etc.)?
- who should be responsible for monitoring and review activities?
- how should the results of monitoring and review be reported to facilitate timely and effective decision making?

6.13) RISK REGISTER FORM



What's the risk? *			What's the risk leading to? *	
Owner *	Please Select..		Director *	Please Select..
	Uncontrolled	Controlled		Future Controls
Current Control Measures *			Treatment method/potential control	
Date Risk Identified *			Future Control Commencement Date	
Current Likelihood *	Please Select..	Please Select..	Residual Likelihood	Please Select..
WHS	Please Select..	Please Select..	WHS	Please Select..
Socio-economic	Please Select..	Please Select..	Socio-economic	Please Select..
Reg/Comp (including Environment, Cultural & Heritage Protection	Please Select..	Please Select..	Reg/Comp (including Environment, Cultural & Heritage Protection	Please Select..
Reputation	Please Select..	Please Select..	Reputation	Please Select..
Financial	Please Select..	Please Select..	Financial	Please Select..
Business Continuity	Please Select..	Please Select..	Business Continuity	Please Select..
Overall Consequence			Overall Consequence	
Calculated Risk	Calculate	Calculate	Residual Risk	Calculate
Risk Level	Calculate	Calculate	Planned Risk Level	Calculate
Removal Date			Remarks	
Monthly Updates				