WORKING DRAFT #3

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 6.5 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.

WORKING DRAFT #3

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.

WORKING DRAFT #3

4 KNOWLEDGE MANAGEMENT

4.1 REFERENCES AND FURTHER INFORMATION

Sources used in developing this document are included in Attachment 6.11 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

WORKING DRAFT #3

- 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.

WORKING DRAFT #3

5 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 0 – the risk register template (database) in which details of risk events, scores, treatments and actions are recorded
- Attachment 6.9 – the risk tables used to determine likelihood and consequence scores and an overall risk score
- Attachment 6.10 – risk responses based on overall risk score.

WORKING DRAFT #3

6 ATTACHMENTS

The intention is that the following attachments will be excised from this document and form stand-alone references on the WSC intranet. They are included here as a single document in order to give the reader all ERM Framework information in a single document, apart from the implementation outline and risk IT functional specification which are contained in a separate document.

6.1 GLOSSARY

Term	Definition/Comments	Source
Council	Wyong Shire Council's elected representatives	
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, effected 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 (COSO)
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 Guidelines
residual risk	Risk remaining after risk treatment	AS/NZS ISO31000:2009
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

WORKING DRAFT #3

Term	Definition/Comments	Source
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 "accident".	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 management - Vocabulary
risk owner	Person or entity with the accountability and authority to manage a risk	ISO Guide 73:2009 Risk management - Vocabulary
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

WORKING DRAFT #3

Term	Definition/Comments	Source
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

WORKING DRAFT #3

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.

WORKING DRAFT #3

- 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, workers 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.

WORKING DRAFT #3

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.

WORKING DRAFT #3

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.

	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.
(f) Risk management is based on the best available information	

WORKING DRAFT #3

	WSC Response
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, 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 learnings.

WORKING DRAFT #3

6.5 WSC RISK POLICY

Policy for Enterprise Risk Management

Wyong Shire Council
CENTRAL COAST

Wyong Shire Council

POLICY FOR ENTERPRISE RISK MANAGEMENT

Policy No:
Policy Author: Capital Insight

History of Revisions:

Version	Date	Authority	TRIM Doc. #
Draft V0.1	15/5/12	Draft for discussion with ERMS Working Party	
Draft V0.3	23/5/12	Draft for discussion with ERMS Project Control Group	
Draft V0.4	22/11/12	Updated draft for Working Draft #2	
1			
2			

Wyong Shire Council
2 Hely Street Wyong
PO Box 20 Wyong NSW 2259
P 02 4350 5555 **F** 02 4351 2098
E wsc@wyong.nsw.gov.au
W www.wyong.nsw.gov.au

A. 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.

B. POLICY BACKGROUND

B.1. 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.

B.2. Risk management explicitly addresses uncertainty but can never eliminate all risks.

B.3. 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.

C. DEFINITIONS

C.1. **Council** means the elected representatives, Councillors, who form the governing body of Wyong Shire Council.

C.2. **The Act** means the *Local Government Act 1993*.

C.3. **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.

C.4. **Risk** is the effect of uncertainty on objectives

C.5. **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.

C.6. **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).

C.7. **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.

C.8. **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.

D. POLICY STATEMENTS

Jurisdiction

D.1. 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.

D.2. This policy does not confer any delegated authority upon any person. All delegations to staff are issued by the General Manager.

General

D.3. 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.

D.4. It is the personal responsibility of all WSC employees and agents thereof to have knowledge of, and to ensure compliance with this policy

D.5. WSC is committed to the formal, systematic, structured and proactive management of risks across the organisation.

D.6. 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.

D.7. Effective risk management:

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

E. POLICY IMPLEMENTATION - PROCEDURES

E.1. 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.

E.2. 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

E.3. 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.

E.4. 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.

E.5. **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

WORKING DRAFT #3

6.6 RISK MATURITY ASSESSMENT – JUNE 2012

FEASIBILITY & PLANNING
Strategic Planning
Business Cases
Service Reviews
Asset & Portfolio Reviews
Feasibility Studies
Economic Appraisals
Value Management

PROPERTY ADVISORY
Corporate Portfolio Strategies
Accommodation Planning
Tenant Representation
Site Masterplanning
Rezoning & Approvals
Asset Investment Services
Development Management

PROJECT STRATEGY
Procurement Strategies
PPP Investigations
Risk Management
Tendering & Transactions
Probity Auditing & Advice
Change Management

DELIVERY
Project Direction
Project Management
Contract Administration
Verification Auditing
Expert Reviews
Dispute Resolution
Privately Financed Infrastructure

Capital Insight Pty Ltd
ABN 76 056 297 100

Sydney 61 2 9955 2300
Brisbane 61 7 3002 7700
Melbourne 61 3 9888 8853

WYONG SHIRE COUNCIL

Enterprise Risk Management Strategy
Risk Management Maturity Assessment Report

May 2012

DRAFT

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:

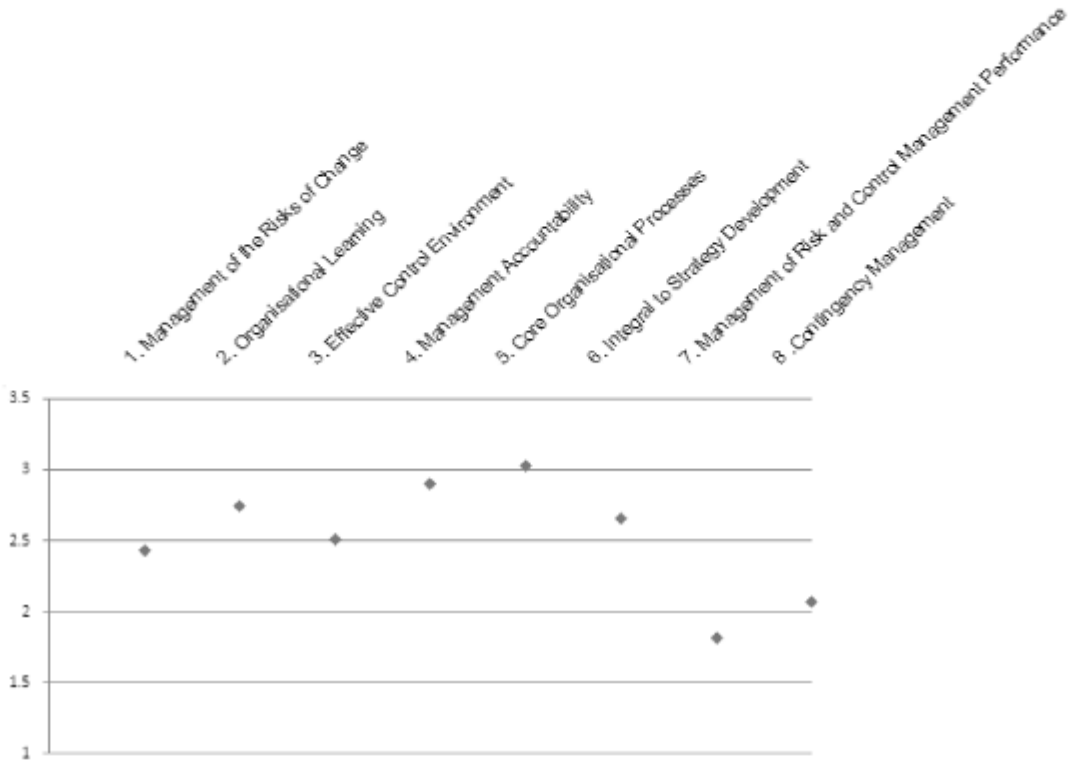
- identify gaps in risk management processes, capacity and culture
- identify relative strengths and weaknesses in risk management performance across different functions within WSC
- identify variations in perceptions between different groups within WSC
- provide an input for subsequent phases which 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.

Rating Description	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 learnings following significant changes, activities or events
- ensuring that root cause analysis techniques are adopted where appropriate
- mechanisms to capture, record and communicate learnings
- 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 learnings.

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 learnings, 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 learnings 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

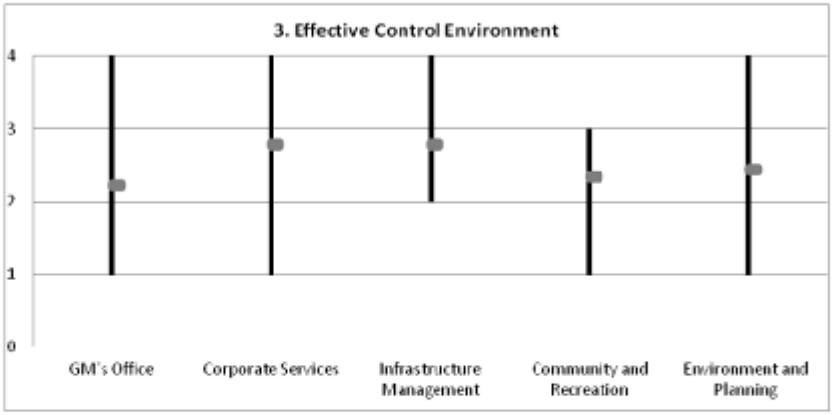
This attribute aims to ensure that risk is effectively and consistently managed within an explicit, established and efficient internal control environment.

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

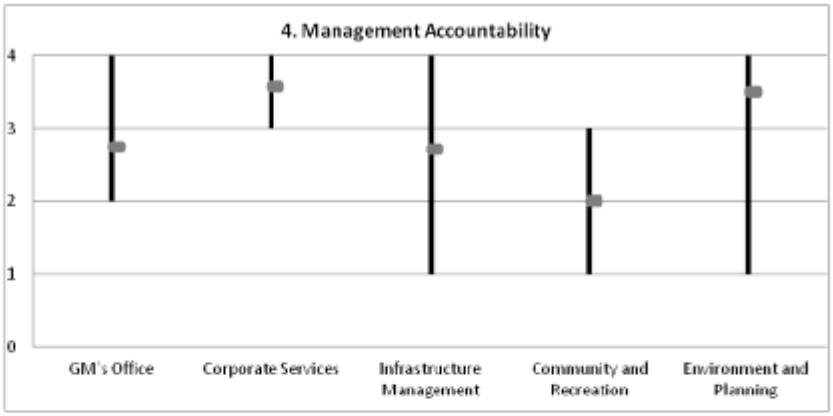
Attribute Overview

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, learnings and lessons from the past.
- 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

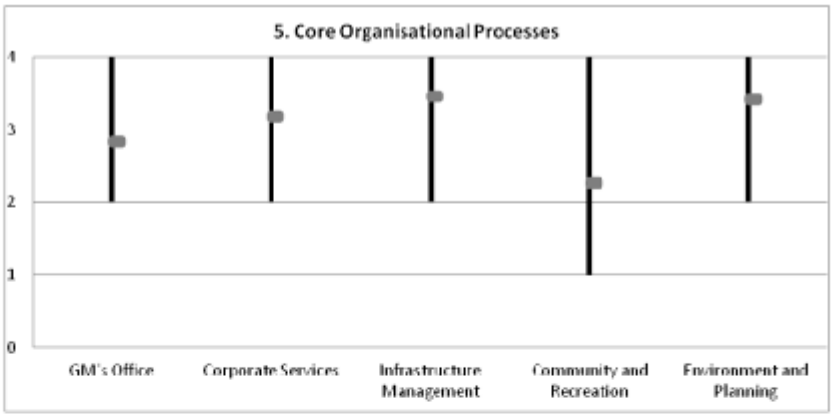
Attribute Overview

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

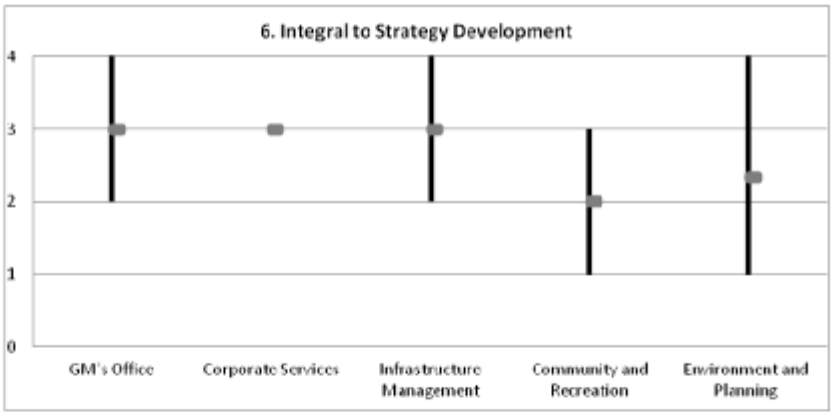
Attribute Overview

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

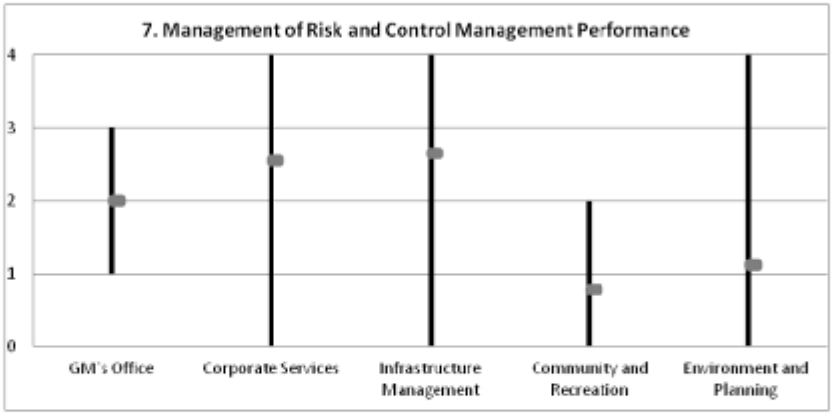
Attribute Overview

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.

Best practice includes requirements for:

- a documented and current risk management plan
- a documented risk management framework
- completion of a risk management maturity evaluation
- definition of explicit risk management KPIs
- establishing risk management role models and leaders with appropriate skills and experience
- provision of training to ensure appropriate levels of risk management knowledge at all levels
- risk management professional development by Directors and Managers
- measuring and reporting risk management performance
- application of risk management principles for decision making by Councillors.

Rating Results



- 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

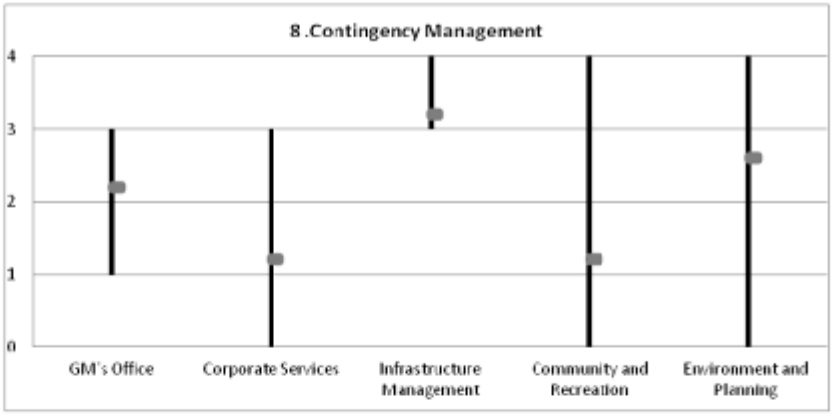
Attribute Overview

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.

Corporate Services

Name	Role
David Jack	Director Corporate Services
Stephen Bignill	Senior Project Executive
Meliisa McKee	Corporate Planning Executive
Kathleen Morris	Manager Integrtated Planning
Brett Phillips	Manager Economic and Property Development
Bob Platt	Chief Information Officer

Infrastructure Management

Name	Role
Greg McDonald	Director Infratructure Services
John Barnard	Manager Plant Fleet Depots
Stefan Botha	Manager Waste
Darrly Mann	Manager Water and Sewerage
David Norbury	Senior Assets Engineer
Andrew Pearce	Manager Raods and Stormwater
David Witherdin	Manager Contract and Project Management

Community and Recreation

Name	Role
Maxine Kenyon	Director Community and Recreation
Ian Clarke	Manager Community Buildings
Adam Holand	Manager Life Long Learning
Sue Ledingahm	Manager Customer and Community Relations
Tara Mills	Manager Sport Liesure and Recreation
Brett Sherar	Manager Open Space
Julie Vaughan	Manager Community and Cultural Development

Environment and Planning

Name	Role
Gina Vereker	Director Environment and Planning
Paul Bowditch	Manager Palce 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

Name	Role
Michael Whittaker	General Manager
Brian Glendinning	General Counsel
Stefano Laface	Executive Manager to the GM

ATTACHMENT B: RISK MATURITY EVALUATION TABLES

#	Requirement	Guidance on evaluation
1. Management of the Risks of Change *All risks created by both internal and external changes and events are effectively and efficiently managed.*		
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.*		
2.1	WSChas a system to capture significant learnings 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 learnings 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.

#	Requirement	Guidance on evaluation
2.3	There is a formal mechanism to efficiently capture and disseminate significant learnings 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).
2.5	Time is specifically allocated in management meetings to discuss opportunities for improvement, based on learnings 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.
2.6	When things go wrong we're mostly concerned with preventing this from recurring.	A lessons learned approach is taken rather than looking to someone to blame when things go wrong.
2.7	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
2.8	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
2.9	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
2.10	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 be for risk management or other key processes or activities.
2.11	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.
2.12	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.

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.

#	Requirement	Guidance on evaluation
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.
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.*		
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.

#	Requirement	Guidance on evaluation
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
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.		
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

#	Requirement	Guidance on evaluation
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.
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.

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.