Risk Management
Self-Assessment Guidelines

2011/2012 Program
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Risk Management Maturity</td>
<td>5</td>
</tr>
<tr>
<td>Carrying out the self-assessment</td>
<td>5</td>
</tr>
<tr>
<td>Evidential support for rating</td>
<td>5</td>
</tr>
<tr>
<td>Summary of Elements and Criteria</td>
<td>6</td>
</tr>
<tr>
<td>Self-Assessment Guidance</td>
<td>9</td>
</tr>
<tr>
<td>Elements and Criteria</td>
<td></td>
</tr>
<tr>
<td>Principles for Managing Risk</td>
<td>10</td>
</tr>
<tr>
<td>Process for Managing Risk</td>
<td>11</td>
</tr>
<tr>
<td>Framework for Managing Risk</td>
<td>12</td>
</tr>
<tr>
<td>Sources of Information</td>
<td>14</td>
</tr>
</tbody>
</table>
The management of risk is an essential element of good governance and is regarded as integral part of sound management practice.

Risk management is a key business strategy for Government departments and agencies and much has been achieved in this area over recent times. Through a structured approach to risk management, departments and agencies should achieve improved business outcomes, whilst enhancing and encouraging the identification of greater opportunities for innovation and continuous improvement.

The South Australian Government has an endorsed Risk Management Policy Statement. This policy makes Public Sector Chief Executives accountable to their Ministers for the development and implementation of a risk management framework specific to the organisation's business and organisational context. The design of this framework reflects the principles and the process outlined in the international risk management standard, AS / NZS / ISO 31000.

These guidelines provide practical information for agencies undertaking the Risk Management Self-Assessment and participating in the Risk Management Benchmarking program.

**Confidentiality**

Agencies that participate are assured that all information received by SAICORP is strictly for the purpose of scoring and coordinating the benchmarking program.

Accordingly, all information is regarded as confidential. While SAICORP will need to analyse the information received, any publication of findings will be in aggregate and a form that will not enable the identification of an individual agency.

**Enquiries**

For enquiries regarding the Risk Management Benchmarking program or Self-assessment Guidelines contact:

**Darryl Bruhn**
Risk Management Coordinator
SAICORP
Phone 822 63429
Email: Darryl.Bruhn@sa.gov.au
Risk Management Maturity

The Risk Management Self-Assessment focuses upon the three elements contained in the recently released International Standards Organisation, Risk Management Standard, AS/NZS/ISO 31000:2009. These elements follow the key clauses, namely Principles (clause 4), Framework (clause 5) and Process (clause 6) for Managing the effect of uncertainty on objectives (i.e. Risk).

Each element states specific criteria against which to benchmark current performance, together with some guidance on how to interpret the criteria and examples of verification of achievement.

The criteria were developed from the requirements of Government of South Australia Risk Management Policy Statement, the International Standards Organisation, Risk Management - Principles and Guidelines AS/NZS/ISO 31000, and the SA Department of Treasury and Finance, Treasurer’s Instructions TI Nos. 2 & 28. The format draws from similar benchmarking concepts utilised by other Treasury Managed Funds within Australia.

The criteria are not all-inclusive and assessments need not be confined to only considering the requirements of the above documents. Individual agencies and organisations should also consider wider issues, including local controls such as policies, procedures and compliance programs where they are not already covered.

The self-assessment has four levels of risk management, namely:

- **Basic (0-15%)** – minimal organisational awareness of the need for risk management and no structured approach to managing uncertainty;
- **Initial (16-50%)** – an organisational commitment to managing uncertainty in a structured manner is starting to emerge.
- **Repeatable (51-85%)** – the assignment of responsibilities and integration of risk management into organisational business processes and across all functions is well advanced and continues to be consolidated;
- **Best Practice (86-100%)** – the organisation is managing uncertainty in a systematic, structured and timely manner, has developed a risk management culture and utilises risk management effectively and efficiently to improve organisational performance.

**Carrying out the self-assessment**

Completion of this self-assessment will require the involvement of a cross section of people with the knowledge and capacity to openly and honestly examine the workings of the organisation against the core documents, namely:

- Government of South Australia Risk Management Policy Statement;
- Risk Management - Principles and Guidelines on Implementation, AS/NZS/ISO 31000; and
- SA Department of Treasury and Finance, Treasurer’s Instructions 2 & 28.
Rating is best undertaken as a team process. The subjectivity of the rating process means that group consensus ratings that draw on a wider range of knowledge and experiences are generally more accurate than an individual's rating.

**Evidential Support for Rating**

The self-assessment will be undertaken by public sector organisations that will vary considerably in terms of organisation size, nature of business environment and factors such as extent of regional operations. Accordingly, evidence cited supporting the rating assigned for specific criteria, may vary considerably for participants.

The larger, more complex organisations may need to rely on more formalised systems while the smaller agencies will be able to meet some criteria with a more informal approach. The essence is that the criteria are met in the most appropriate manner given the organisational circumstances rather than one particular approach being better than another.

Please note that the actual evidence is not required with the Self-Assessment Worksheet. The citing of supporting evidence is for your reference and for consideration when reviewing the benchmarking program.
ELEMENT 1: Principles for managing risk (Clause 4)

This clause requires an assessment of the adherence to the eleven risk management principles and associated behaviours that underpin successful management of uncertainty within an organisation.

1.1 Awareness of the need for a systematic, structured and timely approach to managing risk using the risk management process described in AS/NZS/ISO 31000.

1.2 Executive commitment to risk management demonstrated by appropriate behaviours.

1.3 Acceptance of risk management as a key driver for organisational success. Change management is occurring to move from reactive to proactive mindset. Risk Management facilitates continual improvement and enhancement of the organisation.

1.4 An understanding that the application of risk management discipline will demonstrate due diligence by the organisation irrespective of the actual outcome.

1.5 Entrenched “way of life” for the organisation. Risk management is accepted as an integral part of “day to day” business operations. Risk management is everybody’s business.

1.6 Risk management takes into account the diversity of the workforce, clients and other stakeholders and considers how this may affect their perspective of risk.

1.7 A Risk is considered at all stages of the life cycle for new and existing programs and services. i.e. from conception to realisation.
ELEMENT 2: Process for managing risk (Clause 6)

This clause requires the assessment of the level of awareness, understanding and application of the Risk Management Process defined in AS / NZS / ISO 31000. This includes considering the extent that the Risk Management Process is used as a key business process by the organisation to maximise the achievement of business and strategic objectives and improve performance of programs.

2.1 Level of understanding in how to apply the risk management process within the organisation to consider and manage risk to improve performance.

2.2 Now sub-element 3.2A

2.3 Understanding of risk assessment as a discrete activity of the risk management process involving identification, analysis and evaluation.

2.4 Understanding of the necessity to define the specific objectives of the strategic, organisational and business context to provide a focus for risk assessment.

2.5 Understanding of the need to be able to describe the essence of any risks identified accurately including the identification of the underlying root causes that create the risk to achievement of specific objectives.

2.6 Levels of risk are compared against pre-established criteria and consideration given to the balance between potential benefits and adverse outcomes and overall feasibility.

2.7 Communication and consultation planning as appropriate for risk management effectiveness.

2.8 Now sub-element 3.8
ELEMENT 3: Framework for managing risk (Clause 5)

This clause requires the assessment of the risk management framework developed by the organisation to manage uncertainty in an efficient and effective manner.

3.1A Mandate and commitment to risk management is evident with a policy and the allocation of resources for risk management.

3.1 Responsibilities for risk management clearly delineated to an oversight body, executive and line management. Relationship with Internal Audit function defined.

3.2 Appropriate systems are available to enable risk registers and associated risk treatment plans to be reported easily and concisely.

3.2A Development of a risk management framework that is organic to best meet the organisation’s business environment, particular objectives and the nature of the industry engaged in.

3.3 Implementation and maintenance of risk management to include an education program for management and staff to enable them to fulfil their risk management responsibilities and increase risk ownership.

3.4 The risk management strategy is aligned with the organisation’s goals, and objectives. The organisation learns and improves its performance through continuous improvement of its systems and processes.

3.5 Now sub-element 1.7

3.6 The program of risk management activity aligns with the organisation’s planning, budgetary and reporting cycle.

3.7 Responsibilities are clearly delineated for business continuity, emergency response and disaster recovery planning within the organisation.

3.8 The organisation’s core functions and critical systems have been identified, acceptable downtimes estimated and continuity, emergency response, contingency and recovery plans developed.
The following pages contain a set of indicators relating to the elements of risk management maturity to be used for guidance when rating current risk management practices. Please note that the examples quoted are not definitive and accordingly do not reflect the only indicators of risk management practices.

Every organisation is unique and what may be appropriate for one organisation may not be appropriate for another. Each organisation must ultimately decide for itself what is “right” for it and how to obtain the maximum value for its risk management effort.

### Risk management level

<table>
<thead>
<tr>
<th>BEST PRACTICE</th>
<th>3. Management of uncertainty by the organisation is achieved using a framework specifically designed to meet the organisation’s business context. This framework is underpinned by risk management principles and the appropriate application of the risk management process.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Risk management is regarded as “the way we work” and fundamental to maximising the creation of sustainable value.</td>
</tr>
<tr>
<td></td>
<td>2. A risk management culture is emerging and evident in the language and the emphasis on using the risk management process within the organisation. The integration of risk management into business functions is well advanced as is the consideration of risk information in decision-making.</td>
</tr>
<tr>
<td></td>
<td>1. Acceptance of need for a corporate approach to risk management. Initial effort to increase knowledge and develop a risk management program commenced or possibly restarted.</td>
</tr>
<tr>
<td></td>
<td>0. Risk management is perceived to relate to hazards, accidents, claims and negative outcomes only. Internal specialists using specific risk disciplines for each silo of risk.</td>
</tr>
</tbody>
</table>
Element 1: Principles for managing risk

<table>
<thead>
<tr>
<th>BASIC</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-active with focus on problem prevention</td>
<td>Understanding of principles and their application emerging but still some resistance to overcome</td>
<td>Widespread acceptance of principles for managing risk</td>
<td>Pro-active with focus on managing uncertainty to create sustainable value</td>
<td></td>
</tr>
<tr>
<td>Understanding of principles and their application emerging but still some resistance to overcome</td>
<td>“Risk silo” mentality towards risk management diminishing but still the main understanding.</td>
<td>Risk management language demonstrates shared understanding of risk management</td>
<td>Managing uncertainty using principles for managing risk embedded into organisational culture</td>
<td></td>
</tr>
<tr>
<td>“Risk silo” mentality towards risk management diminishing but still the main understanding.</td>
<td>Risk management information is considered as part of all strategic and high level decision-making.</td>
<td>Responsible risk taking and learning from experience encouraged and supported</td>
<td>Risk management information is considered as part of all strategic and high level decision-making.</td>
<td></td>
</tr>
</tbody>
</table>

Examples of Verification

- Establishment of a committee with responsibility for risk management. May be combined with audit or by extending the terms of reference for an existing committee (e.g. quality) or other regular executive meeting.
- Executive and senior management participation in risk assessment
- Executive presentations to the responsible committee on their business unit’s risk profile
- Executive and senior management performance management appraisal to include risk management performance
- Risk profile required to be appended to all board and management papers
- Risk assessment undertaken as part of all business, strategic, project planning activities.
- Senior and line managers seek advice and assistance on risk management as necessary.
- Expected standards of ethical behaviour are communicated to all members of the organisation
- Executive and management behaviour demonstrates the expected standard of ethical behaviour.
- Engagement of wide range of staff in developing/reviewing risk management policy and procedures as means of increasing ownership.
- Current level of risk management maturity assessed using SAICORP self-assessment or similar.
- Risks are identified and reported even if no treatment is available. Will be monitored thereafter in case a treatment opportunity arises.
• Senior managers focus on balancing organisational performance and conformance.

• Responsible risk taking and learning from experience encouraged and supported.

• Organisation-wide knowledge and belief in the principles of risk management as essential to good management.

• Liaison between business units within the organisation regarding common risk management issues.

• Collaborative work with other government and private organisations on the management of risk.

• Linked to quality program and/or Corporate Strategy.

• Outcomes of risk management processes are integrated and support informed decision-making and priority setting.

• Risk management personnel professional development supported and encouraged.

• Executive uses risk management in setting priorities and allocating resources.

• Stakeholders are identified, particularly those with differing needs, minority and “at risk” groups. Effective system of communication and consultation considers such stakeholders.

• Planning documentation indicates integration of risk management is accepted and progressing.

• Risk facilitators/champions attend as observers at Risk Management Committee meetings.

• Whistle blowing policy, commitment to equity, staff involvement.

• A clear and shared vision of the organisation’s purpose, values and key outcomes identified.
## Element 2: Process for managing risk

<table>
<thead>
<tr>
<th>BASIC</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>BEST PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimal knowledge and understanding of the risk management process prescribed in 31000.</td>
<td>Some awareness of 31000, the risk management process and the elements that make it up.</td>
<td>Good understanding of risk management process, and how, and when it can be used. Still some inconsistency across the organisation.</td>
<td>Application of the risk management process is fully utilised as a key business tool.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management responsibility is perceived to reside with internal risk specialists, e.g. insurance, OH &amp; S, Clinical.</td>
<td>Risk management activities but some confusion on how relates to silos of risk such as OH &amp;S, Clinical etc.</td>
<td>Most appropriate application of the risk management process given the nature of the business and the environment in which it operates is starting to crystallise.</td>
<td>The risk management process is used appropriately throughout the business lifecycle and on major projects or any significant activity.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Some understanding of individual elements in the risk management process.</td>
<td></td>
<td></td>
<td>Risk assessment is updated as significant changes occur in operational objectives or circumstances.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Examples of Verification

- Context is clear and specific to whether whole of organisation, divisional or at business unit level and the reason being undertaken.
- Stakeholders are identified, particularly those with differing needs, minority and “at risk” groups. Communication & consultation planning appropriate for these stakeholders.
- Risk assessment undertaken as part of all business, strategic, project planning activities.
- Risk management procedures, planning and strategy refer to risk management process elements.
- Risk assessments conducted as part of any policy and procedure development or review, projects initiation, or key decision-making process.
- Checklists, records of past experience, workshop outcomes, systems analysis and scenario analysis.
- Objectives are built around a strategic plan, reviewed regularly and changed when necessary.
- Risks are identified and reported even if no treatment is available. Will be monitored thereafter in case a treatment opportunity arises.
- Regular reports on risk and control self-assessments.
- Existing controls such as include strategic and business plans, policies, procedures, compliance programs, delegations, training, qualified personnel, safe work practices, complaints handling and asset registers.
## Element 3: Framework for managing risk

<table>
<thead>
<tr>
<th>BASIC</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management responsibilities relate to specific silos of risk such as OH &amp; S, clinical risk, Business Continuity, Disaster Recovery, etc only.</td>
<td>Risk management policies and procedures with responsibilities assigned including an oversight committee.</td>
<td>Commitment to continual improvement of risk management reporting capability, access and education.</td>
<td>Staff that are capable of applying risk management skills and knowledge at the level appropriate to them.</td>
</tr>
<tr>
<td>Reporting on losses, claims, hazards and incidents.</td>
<td>Recognition of the need to report on risk &quot;per se&quot; using risk registers is emerging.</td>
<td>Coordinated reporting on risk is occurring and includes performance reporting on “soft” indicators</td>
<td>Framework developed assists the organisation to respond to changing circumstances in an efficient manner</td>
</tr>
<tr>
<td>Education commences and risk management becoming integrated into some business processes. Some basic tools available for line management.</td>
<td>Education commences and risk management becoming integrated into some business processes. Some basic tools available for line management.</td>
<td>Substantial integration of risk into business processes and alignment of risk management activities into business cycle.</td>
<td>Framework for managing uncertainty refined to maximise its contribution to organisational performance.</td>
</tr>
</tbody>
</table>

### Examples of Verification

- Establishment of a committee with responsibility for risk management. May be combined with audit or by extending the terms of reference for an existing committee (e.g. quality) or other regular executive meeting.
- Executive responsibility to certify that risks have been identified and rated with appropriate controls in place.
- CE accountability for implementing effective risk management standards and practices.
- Finance & Audit Committee has strong focus on risk management. Reflected in Terms of reference.
- Risk management promotion, staff surveying and other awareness raising including branding. E.g. PIRRISK, TEIRisk.
- Expected standards of ethical behaviour are communicated to all members of the organisation
- Engagement of wide range of staff in developing/reviewing risk management policy and procedures as means of increasing ownership.
- Current level of risk management maturity assessed using SAICORP self-assessment or similar.
- Risk management personnel professional development supported and encouraged.
- Risk management procedures, planning and strategy refer to risk management process elements.
- Risk management responsibilities stated in job descriptions.
• Communication plan addresses issues relating to the risk itself and the process to manage it.

• Compliance program in place to monitor and report on breaches of risk assessment requirements.

• Engagement of external consultant to support internal specialists. Also contribute to refinement of the framework.

• Executive management determine acceptable level of risk as indicated in risk matrices that are reviewed annually.

• Risk sources are collated by category using appropriate classification categories in use within the organisation. Common categories used include Corporate/Strategy, Financial, Human Resources, Information Technology, Operations, Communication, Relationships & Reputation, Property /Assets.

• “Risk Champions” network established, trained and supported.

• Risk management education programs, information sessions on risk management.

• Links between key organisational strategies (operations, finance, HR, IT, OHS&W, etc).

• Adequate funds and human resources are available to implement the Risk Management Program.
Sources of information


Attributes of Enhanced Risk Management, ISO 31000 Annexure A

AS 8000, Corporate governance - Good governance principles, Standards Australia, 2003

ASX Corporate Governance Council’s Corporate Governance Principles and Recommendations, Principle 7: Recognise and Manage Risk, August 2007

South Australia’s Strategic Plan 2004, 2007 & 2011

Risk Management Policy Statement, Government of South Australia, November 2009

Victorian Managed Insurance Authority, Risk Management Survey, (VIMPAT) 2005

South Australian Public Sector, Code of Ethics, July 2009