VMIA’s inaugural Risk Conference 2009

• 21 & 22 October 2009
• For organisational leaders, risk management and insurance professionals in the Victorian Public Sector
• Early bird rates close 31 August 2009

For the conference program and to register, visit:

www.vmia.vic.gov.au
Current status

• Final draft ISO/FDIS 31000:2009(E) issued
• Voting begins on 25 May 2009
• Voting terminates on 25 July 2009
• For more information
Abstract of ISO31000:2009 (Draft)

• ISO 31000:2009 provides principles and generic guidelines on risk management.
• ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector.
• ISO 31000:2009 can be applied throughout the life of an organisation, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.
• ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.
• Although ISO 31000:2009 provides generic guidelines, it is not intended to promote uniformity of risk management across organisations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organisation, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.
• ISO 31000:2009 is not intended for the purpose of certification.

(Source: ISO Website on ISO31000 – 16 June 2009)
All organisations manage risk

Risk management can be applied to an entire organisation, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Changing definition of risk

• “Measurable uncertainty” – Knight, Frank H. (1971), “Risk, Uncertainty and Profit” (University of Chicago Press), Orig. pub. 1921

• “Combination of the probability of occurrence of harm and the severity of that harm” – Source: ISO/IEC Guide 51:1999

• “Combination of the probability of an event and its consequence” – ISO/IEC Guide 73:2002

• “Chance of something happening that will have an impact on objectives” – AS/NZS 4360:2004

• “Effect of uncertainty on objectives” – ISO 31000:2009 (Draft)
Control and risk treatment

• Risk treatment – “Process to modify risk”

• Control – “Measure that is modifying risk”
## Comparing the risk standards

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Universal application across all organisations – Australia and New Zealand</td>
<td>Universal application across all organisations – International</td>
</tr>
<tr>
<td>Context for risk management</td>
<td>Organisation's objectives</td>
<td>Organisation's objectives</td>
</tr>
<tr>
<td>Process for managing risk (&quot;What you do&quot;)</td>
<td>Core of AS/NZ 4360</td>
<td>Part of ISO 31000</td>
</tr>
<tr>
<td>Framework for managing risk (&quot;How you do it&quot;)</td>
<td>Revised substantially in 2004</td>
<td>Expanded on AS/NZ 4360</td>
</tr>
<tr>
<td>Principles for managing risk</td>
<td>Implicit - to some extent</td>
<td>Now clear and explicit</td>
</tr>
<tr>
<td>Attributes of enhanced risk management</td>
<td>Not covered</td>
<td>Annex in ISO 31000 as informative (optional)</td>
</tr>
</tbody>
</table>
# Differences in definitions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Chance of something happening that will have an impact on objectives</td>
<td>Effect of uncertainty on objectives</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects</td>
<td>Coordinated activities to direct and control an organisation with regard to risk</td>
</tr>
<tr>
<td>Risk Management Framework</td>
<td>Set of elements of an organisation’s management system concerned with managing risk</td>
<td>Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation</td>
</tr>
<tr>
<td>Risk Management Policy</td>
<td>Not defined</td>
<td>Statement of the overall intentions and direction of an organisation related to risk management</td>
</tr>
<tr>
<td>Risk Management Plan</td>
<td>Not defined</td>
<td>Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk</td>
</tr>
<tr>
<td>Risk Management Process</td>
<td>Systematic application of management policies, procedures and practices to the task of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk</td>
<td>Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk</td>
</tr>
</tbody>
</table>
Principles for managing risk

For risk management to be effective, an organisation should at all levels comply with the following principles:

- **Risk management creates and protects value**
- Risk management is an integral part of all organisational processes
- Risk management is part of decision making
- Risk management explicitly addresses uncertainty
- Risk management is systematic, structured and timely
- Risk management is based on the best available information
- Risk management is tailored
- Risk management takes human and cultural factors into account
- Risk management is transparent and inclusive
- Risk management is dynamic, iterative and responsive to change
- Risk management facilitates continual improvement of the organisation.
Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organisational processes.

Overview of ISO31000 and AS4360

Principles for managing risk (Clause 3)
1) Creates value
2) Integral part of organisational processes
3) Part of decision making
4) Explicitly addresses uncertainty
5) Systematic, structured & timely
6) Based on the best available information
7) Tailored
8) Takes human & cultural factors into account
9) Transparent & inclusive
10) Dynamic, iterative & responsive to change
11) Facilitates continual improvement & enhancement of the organisation

AS4360 – Implicit, to some extent

Framework for managing risk (Clause 4)
- Mandate & commitment
- Design of framework for managing risk
- Continual improvement of the framework
- Implementing risk management
- Monitoring & review of the framework

AS4360 – Covered partially in Section 4 “Establishing effective risk management”

Process for managing risk (Clause 5)
- Establishing the Context
- Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Monitoring & Review

AS4360 – Fully covered in Section 3 “Risk Management Process”

Attributes of enhanced risk management (Annex A - Informative)
- AS4360 – Not covered

Mandate & commitment
- Establishing the Context
- Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Monitoring & Review

Continual improvement of the framework
- Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Monitoring & Review

Implementing risk management
- Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Monitoring & Review

Monitoring & review of the framework
- Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Monitoring & Review
Adapting the framework to specific needs

(The risk management) framework is not intended to prescribe a management system, but rather to assist the organisation to integrate risk management into its overall management system.

Framework for managing risk

4.2 Mandate and commitment

4.3 Design of framework for managing risk
4.3.1 Understanding the organisation and its environment
4.3.2 Establishing risk management policy
4.3.3 Accountability
4.3.4 Integration into organisational processes
4.3.5 Resources
4.3.6 Establishing external communication & reporting mechanisms
4.3.7 Establishing internal communication & reporting mechanisms

4.4 Implementing risk management
4.4.1 Implementing the framework for managing risk
4.4.2 Implementing the risk management process

4.5 Monitoring and review of the framework

4.6 Continual improvement of the framework
Process for managing risk

- General (5.1)
- Communication and consultation (5.2)
- Establishing the context (5.3)
  - General (5.3.1)
  - Establishing the external context (5.3.2)
  - Establishing the internal context (5.3.3)
  - Establishing the context of the risk management process (5.3.4)
  - Developing risk criteria (5.3.5)
- Risk assessment (5.4)
  - General (5.4.1)
  - Risk identification (5.4.2)
  - Risk analysis (5.4.3)
  - Risk evaluation (5.4.4)
- Risk treatment (5.5)
  - General (5.5.1)
  - Selection of risk treatment options (5.5.2)
  - Preparing and implementing risk treatment plans (5.5.3)
- Monitoring and review (5.6)
- Recording the risk management process (5.7)
Attributes of enhanced risk management (optional) - 1

The list of attributes below represents a high level of performance in managing risk.

• An emphasis is placed on continual improvement in risk management through the setting of organisational performance goals, measurement, review and the subsequent modification of processes, systems, resources, capability and skills (A.3.1)

• Enhanced risk management includes comprehensive, fully defined and fully accepted accountability for risks, controls and risk treatment tasks. Designated individuals fully accept accountability, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to external and internal stakeholders. (A.3.2)
Attributes of enhanced risk management (optional) - 2

• All decision making within the organisation, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree (A.3.3)

• Enhanced risk management includes continual communications with external and internal stakeholders, including comprehensive and frequent reporting of risk management performance, as part of good governance (A.3.4)

• Risk management is viewed as central to the organisation's management processes, such that risks are considered in terms of effect of uncertainty on objectives. The governance structure and process are based on the management of risk. Effective risk management is regarded by managers as essential for the achievement of the organisation's objectives (A.3.5)
Criteria for success

- Gaining total support from the top – without this, the process will fall and staff will not support the implementation with anything but lip service
- Incorporate risk management within the development and review of business plans and targets
- Follow through – tools, templates, training, self-checks and self-assessment, review, audit and confirmation are vital for the ongoing success of the risk management program
- Getting the message across that risk management is not just another fad but is something that can assist all staff and managers to be more effective
- A simple system that all staff can access and use on a regular basis
Key points

• Draft ISO standard is still a flexible guidance
  – Not prescriptive
  – Not for certification
• Consider the development and improvement of risk framework, as well as process for managing risks
• Risk management *creates* value (Clause 3)
  – Not just a compliance exercise
  – Performance indicators are important - *What gets measured, gets done*
• Use ISO 31000 principles as ‘health check’ of maturity of risk management framework and process
VMIA Contact

Should you require more information about the draft ISO31000:2009, please contact:

Patrick Ow
Risk Management Advisor
Phone: (03) 9270 6968
E-mail: p.ow@vmia.vic.gov.au