New Standards for the Management of Risk

Kevin W Knight AM;
CPRM; Hon FRMIA; FIRM (UK); LMRMIA; ANZIIF (Mem).

CHAIRMAN
ISO WORKING GROUP - RISK MANAGEMENT STANDARD

MEMBER
STANDARDS AUSTRALIA / STANDARDS NEW ZEALAND
JOINT TECHNICAL COMMITTEE OB/7 - RISK MANAGEMENT

P 0 BOX 226, NUNDAH Qld 4012, Australia
E-mail: kknight@bigpond.net.au
History of the ISO and Risk Management

• Over 80 separate ISO and IEC Technical Committees are addressing aspects of risk management


• ISO Technical Management Board (TMB)
  – 2004, approached by Australia and Japan
  – AS/NZS 4360:2004 to be adopted by ISO???

• June 2005, TMB sets up Working Group (WG)

Terms of Reference as approved by Technical Management Board

• The WG provides a document which provides principles and practical guidance to the risk management process.

• The document is applicable to all organizations, regardless of type, size, activities and location and should apply to all type of risk.
The document should:

• establish a **common concept** of a risk management process and related matters.

• provide practical guidelines to:
  – understand how to implement risk management
  – identify and treat all types of risk,
  – treat and manage the identified risks,
  – improve an organization's performance through the management of risk,
  – maximize opportunities and minimize losses in the organization;
  – raise awareness of the need to treat and manage risk in organizations.
Terms of Reference as approved by TMB (Continued)

2. Type of deliverable
The standard to be developed is a Guideline document, and is NOT to be used for the purpose of certification.
ISO Guide 73:2009 - Scope

- provides a basic vocabulary of the definitions of generic terms related to risk management

- aims to encourage a mutual and consistent understanding, a coherent approach to the description of activities relating to the management of risk, and use of risk management terminology in processes and frameworks dealing with the management of risk.
Terms included in ISO Guide 73
in Alphabetical order

- COMMUNICATION & CONSULTATION
- CONSEQUENCE
- CONTROL
- ESTABLISHING THE CONTEXT
- EVENT
- EXPOSURE
- EXTERNAL CONTEXT
- FREQUENCY
- HAZARD
- INTERNAL CONTEXT
- LEVEL OF RISK
- LIKELIHOOD
- MONITORING
- PROBABILITY
- RESIDUAL RISK
- RESILIENCE
- REVIEW
- RISK
- RISK ACCEPTANCE
- RISK AGGREGATION
- RISK ANALYSIS
- RISK APPETITE
- RISK ASSESSMENT
- RISK ATTITUDE
- RISK AVERSION
- RISK AVOIDANCE
- RISK CRITERIA
- RISK DESCRIPTION
- RISK EVALUATION
- RISK FINANCING
- RISK IDENTIFICATION
- RISK MANAGEMENT
- RISK MANAGEMENT AUDIT
- RISK MANAGEMENT FRAMEWORK
- RISK MANAGEMENT PLAN
- RISK MANAGEMENT POLICY
- RISK MANAGEMENT PROCESS
- RISK MATRIX
- RISK OWNER
- RISK PERCEPTION
- RISK PROFILE
- RISK REGISTER
- RISK REPORTING
- RISK RETENTION
- RISK SHARING
- RISK SOURCE
- RISK TOLERANCE
- RISK TREATMENT
- STAKEHOLDER
- VULNERABILITY
The Pivotal Definition

**risk**

*effect of uncertainty on objectives*

**NOTE 1** An effect is a deviation from the expected — positive and/or negative.

**NOTE 2** Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

**NOTE 3** Risk is often characterized by reference to potential events and consequences, or a combination of these.

**NOTE 4** Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

**NOTE 5** Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

<table>
<thead>
<tr>
<th>KNOWLEDGE ABOUT OUTCOMES</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Well-defined outcomes</strong></td>
<td><strong>Poorly defined outcomes</strong></td>
</tr>
<tr>
<td>Some basis for probabilities</td>
<td>risk</td>
</tr>
<tr>
<td>No basis for probabilities</td>
<td><strong>“INCERTITUDE”</strong></td>
</tr>
</tbody>
</table>

Senior Executive’s Seminar – HRH the Prince of Wales’s Business and the Environment Programme. 
University of Cambridge.
risk owner
person or entity with the accountability and authority to manage a risk

risk attitude
organization's approach to assess and eventually pursue, retain, take or turn away from risk

risk appetite
amount and type of risk that an organization is prepared to pursue, retain or take

risk tolerance
organization's or stakeholder's readiness to bear the risk after treatment in order to achieve its objectives
NOTE Risk tolerance can be influenced by legal or regulatory requirements.

risk aversion  
attitude to turn away from risk

risk aggregation  
consideration of risks in combination

risk acceptance  
*informed decision to take a particular risk*

NOTE 1 Risk acceptance can occur without risk treatment or during the process of risk treatment.

NOTE 2 Accepted risks are subject to monitoring and review.
control
measure that is modifying risk
NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk.
NOTE 2 Controls may not always exert the intended or assumed modifying effect.

risk retention
acceptance of the potential benefit of gain, or burden of loss, from a particular risk
NOTE 1 Risk retention includes the acceptance of residual risks
NOTE 2 The level of risk retained can depend on risk criteria.

residual risk
risk remaining after risk treatment
NOTE 1 Residual risk can contain unidentified risk.
NOTE 2 Residual risk can also be known as “retained risk”.

resilience
adaptive capacity of an organization in a complex and changing environment

risk profile
description of any set of risks
NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.
Yet to be defined

• Accountable
  liability for the outcomes of actions or decisions
  NOTE: includes failure to act or make decisions
  OR
  being obligated to answer for a decision.
  OR
  obligation to answer for an action
Yet to be defined

Responsible

obligation to carry out duties or decisions, or control over others
OR
having the obligation to act.
OR
obligation to act
ISO 31000:2009 is intended to be used by a wide range of stakeholders including:

- those responsible for implementing risk management within their organization;
- those who need to ensure that an organization manages risk;
- those who need to manage risk for the organization as a whole or within a specific area or activity;
- those needing to evaluate an organization’s practices in managing risk; and
- developers of standards, guides, procedures, and codes of practice that in whole or in part set out how risk is to be managed within the specific context of these documents.
A Business Principles Approach to the Management of Risk
a) Creates value  
b) Integral part of organizational processes  
c) Part of decision making  
d) Explicitly addresses uncertainty  
e) Systematic, structured and timely  
f) Based on the best available information  
g) Tailored  
h) Takes human and cultural factors into account  
i) Transparent and inclusive  
j) Dynamic, iterative and responsive to change  
k) Facilitates continual improvement and enhancement of the organization  

**Principles (Clause 3)**

**Framework (Clause 4)**

**Process (Clause 5)**

ISO 31000:2009 Figure 1 – Relationship between the principles, framework and process
Corporate Governance

The way in which an organisation is governed and controlled in order to achieve its objectives. The control environment makes an organisation reliable in achieving these objectives within a tolerable degree of risk.

It is the glue which holds the organisation together in pursuit of its objectives while risk management provides the resilience.

Queensland Audit Office – Report No. 7 1998-99: -
“The system by which entities are directed and controlled.”

“Corporate governance generally refers to the processes by which organisations are directed, controlled and held to account. It encompasses authority, accountability, stewardship, leadership, direction and control exercised in the organisation.”

SAA HB 254-2005

Governance, risk management and control assurance
Standards Australia. ISBN 0 7337 6892 X
Potential greater future role of risk management

Traditional and current risk management application

Risk Management’s Role in Corporate Governance
Business Principles Approach

ISO 31000:2009 Principles (Clause 3)

Risk management should....

1. Create value
2. An integral part of organisational processes
3. Part of decision making
4. Explicitly address uncertainty
5. Be systematic and structured
6. Be based on the best available information
7. Be tailored
8. Take into account human factors
9. Be transparent and inclusive
10. Be dynamic, iterative and responsive to change
11. Be capable of continual improvement and enhancement
Attributes of enhanced risk management

1. A pronounced *emphasis on continuous improvement* in risk management through the *setting of organizational performance goals*, measurement, review and the subsequent modification of *processes, systems, resources and capability/skills*.

2. Comprehensive, fully defined and fully accepted accountability for risks, controls and treatment tasks. Named individuals fully accept, are appropriately skilled and have adequate resources to check controls, monitor risks, improve controls and communicate effectively about risks and their management to interested parties.
3. All decision making within the organization, whatever the level of importance and significance, involves the explicit consideration of risks and the application of the risk management process to some appropriate degree.

4. Continual communications and highly visible, comprehensive and frequent reporting of risk management performance to all “interested parties” as part of a governance process.
Attributes of enhanced risk management

5. *Risk management is always viewed as a core organizational process* where risks are considered in terms of sources of uncertainty that can be treated to maximize the chance of gain while minimizing the chance of loss. Critically, effective risk management is regarded by senior managers as essential for the achievement of the organization’s objectives. *The organization’s governance structure and process are founded on the risk management process.*
PDCA – a starting point for a framework

Plan

Do

Check

Act

Commitment and Mandate
Policy Statement
Risk Management Plan
Assurance plan
Standards
Procedures/Guidelines

Communicate and Train
Communications and reporting plan
Training strategy
RM Network

Organise and Allocate
Board RM Committee
Exec RM Committee
Manager, RM
RM Champions
Risk, Control, Risk owners
Assurance providers

Measure and review
Control assurance
RM Plan progress
Governance reporting
Benchmarking
Performance criteria
Clause 4 (framework)

• The framework in Clause 4 of ISO 31000:2009 is not intended to describe a management system; but rather, it is to assist the organization to integrate risk management within its overall management system.

• Therefore, organizations should adapt the components of the framework to their specific needs.
4.3 Design of framework
   - 4.3.1 Understanding the organization and its context
   - 4.3.2 Risk management policy
   - 4.3.3 Integration into organizational processes
   - 4.3.4 Accountability
   - 4.3.5 Resources
   - 4.3.6 Establishing internal communication and reporting mechanisms
   - 4.3.7 Establishing external communication and reporting mechanisms

4.4 Implementing risk management
   - 4.4.1 Implementing the framework
   - 4.4.2 Implementing the risk management process

4.5 Monitoring and review of the framework

4.6 Continual improvement of the framework

ISO 31000:2009 Figure 2 — Relationship between the components of the framework for managing risk
ISO 31000:2009 Risk management process (Clause 5)

• should be an integral part of management, be embedded in culture and practices and tailored to the business processes of the organization.

• includes five activities: communication and consultation; establishing the context; risk assessment; risk treatment; and monitoring and review.
ISO 31000:2009
Process Overview

- Establishing the Context
- Risk Identification
- Risk Analysis
- Risk Assessment
- Risk Evaluation
- Risk Treatment

Communication & Consultation

Monitor & Review
5.3 ESTABLISHING THE CONTEXT
5.3.2 External Context
5.3.3 Internal Context
5.3.4 Risk Management Process Context
5.3.5 Developing Risk Criteria

5.4 RISK ASSESSMENT
5.4.2 RISK IDENTIFICATION
What can happen, when, where, how & why

5.4.3 RISK ANALYSIS
Determine existing controls
- Determine Likelihood
- Determine Consequences
- Estimate Level of Risk

5.4.4 RISK EVALUATION
Compare against criteria.
Identify & assess options.
Decide on response.
Establish priorities.

5.5 RISK TREATMENT
5.5.2 Selection of risk treatment options
5.5.3 Preparing and implementing risk treatment plans

ISO 31000:2009 Risk management process in detail
Risk assessment attempts to answer the following fundamental questions:
- what can happen and why (by risk identification)?
- what is the likelihood of their future occurrence?
- what are the consequences?
- are there any factors that reduce the likelihood of the risk or that mitigate the consequence of the risk?
In particular, those carrying out risk assessments should be clear about:

- the context and objectives of the organization,
- the extent and type of risks that are tolerable, and how unacceptable risks are to be treated,
- how risk assessment integrates into organizational processes,
- methods and techniques to be used for risk assessment, and their contribution to the risk management process,
- accountability, responsibility and authority for performing risk assessment,
- resources available to carry out risk assessment,
- how the risk assessment will be reported and reviewed.

- Avoids organisations re-inventing the wheel
- Allows all to benefit from proven best practice
- Provides a universal benchmark
- Reduces barriers to trade
- Advises exactly what you need to do and how you need to do it – no wasted effort and no false starts
- Scalable – works for all sizes of organisation
- Risk management = making optimal decisions in the face of uncertainty
And Finally!!

• ISO 31000:2009 is the natural successor to AS/NZS 4360:2004
• Hopefully it will influence a revision of COSO
• It will fit ‘ERM’ requirements, but will also allow silo/project risk management
• Following ISO 31000:2009 will provide a low cost, high chance of success approach to ERM
• ISO 31000:2009 will add value and reduce risk in risk management

• Managing risk is about creating value out of uncertainty
YOU DO NOT HAVE TO MANAGE RISK!!

SURVIVAL IS NOT COMPULSORY
The greatest risk of all is to take no risk at all!
ISO 31000, ISO/IEC 31010 and ISO Guide 73 provide generic guidance on how to embed risk management, and reinforce the concept of “positive” risk to help you on your journey.