The changing faces of risk management: The evolution of a concept

Simona Fionda, CIRM
Content

What is Risk Management?
Risk Management Standards
ISO and ISO 31000:2009
  • ISO standards development
  • ISO 31000:2009
Complements to ISO 31000:2009
A look to the future
What is Risk Management?

The concept of risk management evolved from the insurance industry where risk financing was the main risk management activity.

A few definitions:

‘**Coordinated activities** to direct and control an organization with regard to risk’ (ISO/IEC Guide 73:2002).

‘Enterprise risk management is 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’ (COSO, 2004, *Enterprise Risk Management – Integrated Framework*).

Financial services crisis in 2008 demonstrates the extent to which uncontrolled risk taking has damaged entire economies.
Risk Management Standards

There are a number of standards around the world but the most used are:


The newest addition to the standards’ list is BSI 31100 2008 Risk Management: Code of Practice which is based on the final draft of ISO 31000 and therefore aligned to it.
## Risk definition over time

<table>
<thead>
<tr>
<th>Source</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frank H. Knight (1921) <em>Risk, Uncertainty and Profit</em></td>
<td>‘Measurable uncertainty.’</td>
</tr>
<tr>
<td>ISO/IEC Guide 51:1999</td>
<td>‘Combination of the probability of occurrence of harm and the severity of that harm.’</td>
</tr>
<tr>
<td>ISO/IEC Guide 73:2002</td>
<td>‘Combination of the probability of an event and its consequence.’</td>
</tr>
<tr>
<td>AS/NZS 4360:2004</td>
<td>‘Chance of something happening that will have an impact on objectives.’</td>
</tr>
<tr>
<td>COSO (2004) ERM - Integrated Framework</td>
<td>‘Events with a negative impact represent risks, which can prevent value creation or erode existing value. Events with positive impact may offset negative impacts or represent opportunities.’</td>
</tr>
<tr>
<td>Lars Oxelheim and Clas Wihlborg (2008) <em>Corporate Decision-Making with Macroeconomic Uncertainty</em></td>
<td>‘The concept of risk refers in general to the magnitude and likelihood of unanticipated changes that have an impact on a firm’s cash flows, value or profitability. […] Risk has a negative connotation, but uncertainty can be a source of opportunities as well as costs.’</td>
</tr>
</tbody>
</table>

ISO and ISO 31000:2009
What is ISO?

International Organization for Standardization (ISO) is the world's largest developer and publisher of International Standards.

ISO is a specialized international organization founded in Geneva in 1947 and concerned with standardization in all technical and non-technical fields except electrical and electronic engineering (the responsibility of the International Electrotechnical Commission).

Upon request, the ISO establishes international technical committees to investigate and resolve specific issues of standardization.
Development of ISO standards

ISO launches the development of new standards in response to the sectors that express a need for them.

- An industry or business sector communicates its requirement for a standard to one of ISO's national members.
- The ISO’s national member proposes the new work item to ISO.
- If accepted, the work item is assigned to an existing technical committee. A proposal can also be made to set up technical committees to cover new scopes of activity.

ISO standards are developed by experts from the sectors which have asked for them.
Stages of ISO Standards development

International Standards are developed by a six-step process:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposal</td>
<td>Confirm that a particular International Standard is needed by gathering votes from the technical committee members.</td>
</tr>
<tr>
<td>Preparatory</td>
<td>A working group is set up and develops the draft version of the standard.</td>
</tr>
<tr>
<td>Committee</td>
<td>The draft is reviewed and the member of the technical committee comment on and approve the technical content.</td>
</tr>
<tr>
<td>Enquiry</td>
<td>The draft standard is circulated to all ISO member bodies and if approved it becomes a final draft. If not it is returned to the committee for further consideration.</td>
</tr>
<tr>
<td>Approval</td>
<td>The final draft is re-submitted to all ISO member bodies for final approval.</td>
</tr>
<tr>
<td>Publication</td>
<td>Once approved the standard is published.</td>
</tr>
</tbody>
</table>
Why an ISO standard in Risk Management?

Organizations around the world are facing increasing and greater risks and risk management is not consistently defined and applied across sectors and countries.

The public and private sectors approach risk in a very different way as do profit and non-profit organizations.

Guidance and publications from government and risk specialists are prolific but they are not harmonized by a common terminology or approach.

Multinational companies operating in many countries around the globe face the challenges of inconsistent practices and definitions.

An international standard, whereby expert representatives from different countries participate in the definition and creation of a common terminology and approach, was undoubtedly needed.
ISO 31000:2009 Risk Management Principles and Guidelines

ISO 31000:2009 was published in **November 2009** and it is the result of four years of consultation between risk and standards experts in 30 countries.

It pulls together and replaces a number of similar international standards. AS/NZS 4360:2004, which was due for revision in 2009, formed the basis of ISO 31000.

This new standard was prepared by the ISO Technical Management Board Working Group on risk management.

ISO 31000 is **not** intended for certification and does not contain compulsory requirements. It is a collection of suggested best practices.
The standards specifies that:

- **Risk management** refers to the architecture (principles, framework and process) for managing risk effectively;
- **Managing risk** refers to applying that architecture to particular risks.

**Risk appetite** is not defined in ISO 31000 (it is in ISO Guide 73:2009), the Standard defines **risk attitude** as the ‘organization's approach to assess and eventually pursue, retain, take or turn away from risk’.

**Risk**

Effect of uncertainty on objectives.
An effect is a deviation from the expected – positive and/or negative.

**Risk Management**

Coordinated activities to direct and control an organization with regard to risk.
Key components of ISO 31000

ISO 31000 is organized in three sections:

- Principles,
- Framework,
- Process.

The key innovations of this standard include:

- Risk is not positive or negative, but consequences are;
- Shift of emphasis from event to effects;
- Risk management creates and protects value;
- Definition of specific attributes of enhanced risk management.
Principles – Framework – Process

Source: ISO 31000:2009 Relationships between the risk management principles, framework and process.
Principles – Clause 3

ISO 31000 contains 11 Principles for risk management:

a) Creates and protects value;
b) Integral part of all 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 of the organization.
Framework – Clause 4

Success of risk management will depend on the effectiveness of the management framework.

Risk management needs to be integrated into the overall management system and needs to be supported by strong management commitment.

ISO 31000 does not prescribe a risk management process but advocates full integration and customisation of the framework to fit the organization.

The framework needs to be tailored to the organization and take into account the organization’s internal and external context.

There need to be accountability, sufficient resources and internal and external reporting mechanisms.

Once implemented the framework needs to be monitored and reviewed to ensure that the feedback process results in continuous improvement (Quality Management Process).

Source: ISO 31000:2009 Relationship between the components of the framework for managing risk
Process – Clause 5

Before engaging in risk assessment and treatment activities there is a need to establish the internal and external context in which the organization operates and to have the right mechanisms to ensure communication and consultation with internal and external stakeholders is in place. At each stage there needs to be continuous monitoring and review.

Risk Assessment is effected by applying the classic process of:

- **Risk Identification**
  Identify sources of risk, areas of impact and consequences.

- **Risk Analysis**
  Understanding the risk and whether it needs to be fully evaluated.

- **Risk Evaluation**
  Compare the level of risk established in the previous stage with the risk tolerance criteria established.

- **Risk Treatment**
  Modification of risk and decision on treatment option.

Source: ISO 31000:2009 Risk management process
Attributes of enhanced risk management

Annex A of ISO 31000 is an informative annex where the committee lists the attributes of enhanced risk management.

Different organizations have different levels of risk management framework’s maturity and this annex provides them with a framework to help measure performance against these attributes.

The committee identified five attributes to enhanced risk management:

- **Continual improvement** in risk management;
- Full **accountability** for risks, controls and risk treatment;
- Explicit consideration of risk in all **decision making**;
- Continual **communication** with internal and external stakeholders;
- Risk management is seen as **central** to the organization **management process**.

The annex also suggests indicators to be used to measure performance.
Complements to ISO 31000:2009

ISO 31000 is complemented by:


BSI released the BS ISO 31000:2009 on 31 March 2010. This publication does not replace BSI 31100 which remains current.
In Summary

ISO 31000:2009

• Provides a common vocabulary and approach for risk management internationally.
• Contains best practices and guidance for all types of organizations.
• Recognises risk as a neutral event and focuses on effects which can be either positive or negative for the organization.
• Provides a list of enhanced risk management attributes and suggested measurements to gauge the maturity of the risk management framework.
• It is not intended for the purpose of certification.
• In the UK it is adopted via the BS ISO 31000:2009.
A look to the future

All ISO standards are subject to a review process which results in one of three outcomes: **Confirmation, Revision, Withdrawal**.

All International Standards are reviewed, by all the ISO member bodies, at least three years after publication and every five years after the first review.

The burning question:
Will risk management standards ever be widely applied?
Thank you!