Risk management

At the end of 2009, the International Organization for Standardization (ISO) issued a new set of principles and guidelines that should benefit all organizations confronting the always problematic challenges of managing risk:

Title/Link	Date of Issue
ISO 31000:2009 Risk management - Principles and guidelines	Nov 13, 2009
ISO Guide 73:2009 Risk management - Vocabulary	Nov 13, 2009
ISO/IEC 31010:2009 Risk management - Risk assessment techniques	Dec 1, 2009

Standard ISO 31000 provides principles and generic guidelines on risk management and is not intended for the purpose of certification. ISO/IEC 31010:2009 describes more than thirty tools to use for risk assessment and explains their application. The ISO Guide 73:2009 contains risk management terminology and definitions. These three standards can be applied to any type of risk, whatever its nature, by organizations of any type or by individuals.

Risk, as defined by the ISO Guide 73:2009, is the impact of uncertainty on objectives. It is very important to emphasize that the impact of uncertainty can be positive as well as negative. "Not pursuing an opportunity" is also a risk.

John Shortreed **, PhD, who served on the ISO technical committees for Guide 73 (Risk Management—Vocabulary, 2002) and its revision (2009) as well as for ISO 31000 (2009), listed the following seven innovations introduced by ISO series 31000:

1. Formal principles for risk management and ERM (Enterprise Risk Management) that can be used for measuring the risk maturity of an organization.

2. Consideration of any risks or uncertainty that affects objectives of the organization, whether they have positive or negative consequences.

3. Organizational ability to tailor risk management to its own internal structure and governance processes.

4. Principle-based rather than performance-based.

5. Requires an organization to formalize and continuously improve a framework for ERM that integrates the management of risk into all processes in the organization.

6. Updates the risk management process used for assisting any decision through the five steps of context, risk assessment, risk treatment, communication, and consultation, followed by formal monitoring and review.

7. Requires accountability for any and all risks through the designation of a "risk owner" whose annual performance partly depends on how well risk is managed.

Questions and Answers

Question: As part of implementing an Enterprise Risk Management program, I'm trying to align Sr. management by providing them with ISO 31000 training. I would appreciate if you can recommend trainers /firms that can provide this service.

Answer: There are two reasons I cannot recommend trainers/firms for ISO 31000 training.

1. I am not sure where your organization is in terms of risk maturity, context, existing risk management, etc. and

2. My knowledge of training organizations is very limited and so mentioning one or two would not be helpful. As with all such selections the first rule is to know the answer to 1. This will ensure that you have an understanding of where your organization is, what it needs in the way of training to implement 31000 and how you might assess the variety of offers available.

So let me comment on **1. Where is your organization?** The first step is to get a copy of ISO 31000 (available on line from most National Standards Organizations, e.g. Canada or Australia), read it over and as you read make checkmarks or comments against the text. Once you have done that you will have a once over crude gap analysis, a list of questions, and so idea of the extent of the task ahead.

Since your current focus is senior management the starting point may be an understanding of their objectives and the context and environment in which they go about making decisions as well as the nature of those decisions and the associated risks.

It may be helpful to look on the web and see if you can find some background material to help you on the context part for the decision you have to make – How to engage senior management in ERM (31000 style)? According to ISO 31000 there is a structured way of considering the risks for any decision including the risks behind your current decision to assist senior management with 31000.

For example a person I know who, John Fraser, has been quite successful in ERM and has written a book last year (I did a chapter for 31000) can be seen in a presentation that hits most of the key "how to get started" things he has found useful in doing ERM in an organization. I caution you that his organization has a relatively straightforward structure and set of day to day tasks so for other more complex organizations the task is more complicated. Also he uses older terminology (understandable since it was prior to 31000). However, it is a good place to start.

http://events.grantthornton.ca/ERM2010/video_101202.cfm

I would stress one of the main messages of ISO 31000 – the decision-maker is in charge – and so one of the

first steps is to get as much of the picture as possible.

As you surf the web you will find, like the John Fraser presentation that most of the sites want to sell you something, which is good in a way but it does mean that you need to have a good understanding of your needs. For example, one other site you might look at as you begin surfing the web is http://www.broadleaf.com.au/iso31000/index.html which is done by an organization where Grant Purdy works – he heads up the Australian New Zealand standards committee for risk management and as you may know their standard was the starting point for ISO 31000. Grant also put ERM into one of the world's largest mining companies in just 4 years with 3 people – similar to John Fraser's experience with Hydro1 – a facilitation role with relatively small staff but with senior management commitment.

Please ask me any follow up questions. Also a little general description of your organization would be helpful as would be the assessment of the present level of risk maturity (see Annex A of 31000 for help there).

Question: I have a copy of the ISO 31000. Does the organization or the Risk Manager have to establish and publish the Risk Policy and the Risk Objectives? How specific do they have to be? Thank you.

Answer: 31000 in section 4.3.2 Establishing the risk management policy (statement of the overall intentions and direction of an organization related to **risk management**) **reads as follows**:

> The risk management policy should clearly state the organization's objectives for, and commitment to, risk management and typically addresses the following:
>
> - the organization's rationale for managing risk;
> - links between the organization's objectives and policies and the risk management policy;
> - accountabilities and responsibilities for managing risk;
> - the way in which conflicting interests are dealt with;
> - commitment to make the necessary resources available to assist those accountable and responsible for managing risk;
> - the way in which risk management performance will be measured and reported; and
> - commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.
>
> The risk management policy should be communicated appropriately.

Since it is in the framework section it is an organization task this is likely put together by the Chief Risk Officer working with senior management and the Board who will adopt it, but this will depend on the organization. Note that with 31000 Risk management is integrated into the organization and so depending on the structure of the organization the risk management will necessarily follow the specific organization's structure and processes. This means that every organization may be unique, although they will (hopefully) follow 31000 and it will be

possible to map the risk management framework established in clause 4, to the terminology and generic framework of 31000.

In terms of how specific the statement should be the old rule of "short as possible while preserving clarity" should be followed.

This URL (BHP Billiton's web site) is a typical example of a policy similar to a risk management policy (some of the items in the 31000 list are missing) for a large company – it is renewed each year (see also comments by John Fraser's video earlier on the blog) and in this instance covers a variety of "objectives" set out by the organization. I did not do it but likely if you search around BHP's web site you may find a structured and nested set of objectives and policies – typical of an organization that has a good risk culture.

Last but not least it is probably incorrect to speak of "risk objectives" There will be at the level of risk management of individual risks (i.e. in clause 5) in the risk management context section **5.3.4 Establishing the context of the risk management process** some details of the risk management process to be used for a specific risk that ensure that the organizations policies for risk management are followed.

In the next few years while ISO 31000 (hopefully) becomes the norm, it might be a good idea to review risk terminology in general to be sure that the term and associated definition is what is meant. It may be necessary to insert the existing meaning as for example – "risk treatment (mitigation)" or in your question "risk management policy (risk policy)". My experience is that many of the differences in risk and risk management are really differences in terminology not in substance.

Question: Do you have information on risk management with respect to organizational structure and impartiality for an organization that offers ISO 9001 registration services?

Answer: Not sure I understand the question – an organization that offers ISO 9001 registration – and risk management with respect to organization structure and impartiality. I think the question is – Suppose an organization exists to register other organizations for compliance with regulation x or certification y (does not really matter if it is 9001 or pollution regulation, or whatever, the situation is the same) how can they assure others that they are impartial and how is this expressed in their risk management framework and organizational structure?

Since the business of the organization is certification or assurance of compliance their organizational objectives will have this front and centre – they are not likely to exist for very long if they do not meet this objective (otherwise there will be complaints, investigations, their clients may realize difficulties with regulators, suppliers, and switch providers, and so forth). The structure of the organization will take many forms but likely

involves clear statements of policy and procedures for audits/certifications, supervision and possible repeating of audits/certification, quality control of auditor/certification performance with remedial actions, forensic like approaches to 'partial' outcomes, annual publication of performance outcomes with regards to impartiality, etc.

So the risk management for this objective will be to identify risks and then manage those risks. Risks might include, for example:

- variable performance of auditors/certification due to unclear policies/communications, lack of training,
- partiality and/or fraud due to lack of supervision and oversight of line operators,
- etc.

These risks will be identified in the usual way – through review of historical data (particularly the year to year results of audits/certifications if available), industry wide data on complaints, review of processes to identify critical control points for bigger risks, etc.) Then a process of generating risk treatments analyzing them and evaluating them will result in optimized (with regard to objectives) procedures for audits and certifications. There may also be modifications to the structure of the organization if systemic problems are found.

Share this article!