The Benefits of Enterprise Risk Management and implementing ISO31000

Tom Teixeira | VP Enterprise Risk Solutions (EU)
STG - Active Risk Manager

The latest PWC survey* of more than 1000 board directors highlighted that they feel an increased onus to manage risk. When asked what keeps them awake at night, 59% of respondents cited worrying about "unknown risks"*

Fortunately for those sleep deprived directors, in November last year ISO, the international standard setting body, published "ISO 31000:2009 Risk management – Principles and Guidelines" to help industrial, commercial and public sector organizations confidently address risk management so that there will be fewer "unknown risks". The ISO 31000 standard sets out principles, a framework and a process for the management of risk that is applicable to any type of organization in the public or private sector. It does not mandate a "one size fits all" approach, but rather emphasizes the fact that to be effective the management of risk must be tailored to the specific needs, culture and structure of a particular organization.

The foundation and purpose of ISO

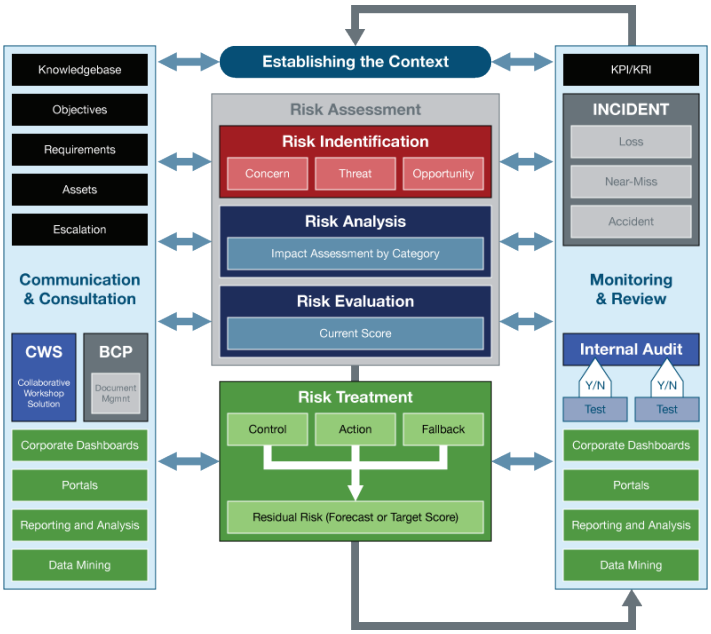
In 1946, delegates from 25 countries met in London and decided to create a new international organization with the objective to "facilitate the international coordination and unification of industrial standards". The new body, the International Organization for Standardisation, officially began operating on 23 February 1947 from Geneva, Switzerland. Because the name would have different acronyms in different languages (IOS in English, OIN in French for Organization international de normalisation), its founders decided to give the body a short, all-purpose name. ISO was chosen, derived from the Greek isos, meaning equal. Whatever the country, whatever the language, the short form of the organization's name is ISO.

Why are standards important – what do they do?

Standards make an enormous and positive contribution to many aspects of business life. Standards contribute to making the development, manufacture and supply of products and services more efficient, safer and environmentally-friendly. Standards facilitate trade between countries and strive to make it fairer. In short standards make life simpler by providing common solutions to common problems. ISO standards are voluntary. As a non-governmental organization, ISO has no legal authority to enforce the implementation of its standards. ISO does not regulate or legislate. However, directors and leaders of all organizations would be well advised to take note of ISO standards as they build their businesses, particularly when a common technical language, sharing of best practice and international standardization can provide a business advantage.

The what, why and how of ISO 31000

Like many standards, ISO 31000 is strong on the "What" – it outlines the components needed for a robust risk management process. However, there is less emphasis on "why" a strong risk management process is required and "how" to actually implement a system to make this a reality.



It is fair to say that "why and how" are not the remit of a standard, although both are vitally important from a cost justification or business case point of view and the eventual success of the management of risk within a particular organization.

Therefore, while ISO 31000 is an important tool in the risk management kit bag, it needs to be supported by strong executive direction, a cultural change within the business and an underpinning system for it to make a real difference.

Where to focus?

From experience gained from numerous risk management projects Strategic Thought Group (STG) has identified that there are three major elements to the successful implementation of a risk management process:

- The risk culture of the organization
- The risk management principles, policy framework and process documentation
- The risk recording and sharing system

These concepts are all referred to within the documentation of the ISO 31000 standard. Indeed it may be helpful to have a copy of the ISO 31000 document available to refer to as you read this article. Let's look at the key elements in more detail:

>>>>>>>>>>>>>>>>Continued on Page 7

very quickly and professionally. Typically, the facts and evidences are presented on a big screen through an overhead projector in the room. We, then, can be highly confident that we can fully support our findings and presentation in the courtroom or war room.

In conclusion, the team's confidence is higher and the frustration is reduced as we can find document backups in seconds. This is not about technology. It is about Success! this is about finding ways to practice more profitably, deliver higher quality services to clients, improve response times, and ultimately win the case.

Dr. Apirath Prateapusanond is Managing Director of Warner Construction Consultants (Thailand), Limited. She holds a Ph.D in Civil Engineering and Management from Virginia Polytechnic Institute and State University, as well as Master's Degrees in Marketing Management from the University of Maryland and Operations Research from The George Washington University. She also holds a Bachelor of Science in Industrial Management from Thammasat University in Bangkok. Dr. Prateapusanond has served as an expert in complex construction litigations, and also worked on such notable construction projects as the Integrated Project Controls System for Honeywell on Boston's Central/Artery Tunnel, and the Burj Dubai Mall in Dubai, UAE. Dr. Prateapusanond is also an authorized representative for CT Summation iBlaze in Thailand and UAE

The Benefits of Enterprise Risk Management and implementing ISO31000

Continued from Page 5 >>>>>>>>>>>>>>

- **The risk culture:** What is the organization's risk appetite and how does it want to engage with risk and the management and reduction of risk? How can a culture which manages risks within the boundaries set by management be established and maintained? How can this culture be developed from where it is now to support a maturing process?

  Establishing and driving the necessary cultural change is often the most neglected part of risk management. Many see it as a side show, when in truth it needs to be centre stage. Without the right risk culture the policy, process and performance of risk management will run into difficulties. This is acknowledged within ISO 31000 as necessary, in order to implement and maintain a successful risk management process.
- **The risk management principles, policy framework and process documentation:** This relates to the suite of documentation that tells people what risk means for an organization. It encapsulates the organization's method for capturing risks, exploiting opportunities, communicating the appetite for risk held within the business and it lists the principles against which the organization operates.
- **The risk recording and sharing system:** The ability to capture risks, share information appropriately and ability to mine risk data to enable decision making and to spot emerging trends, is the way an organization's risk management process will ultimately meet the ISO 31000 principles around process and improve business performance.

It is highly unlikely that an array of risk registers held in spreadsheets will be up to this task. One of the principles identified in ISO 31000 is the ability to address uncertainty which definitely means that information cannot be locked away in multiple spreadsheets or in a software tool that lacks the ability to share information at an enterprise level.

Addressing these three elements is the basis for a living risk management process that will meet the organizational principles of ISO 31000.

Capturing risk and opportunity data

In ISO 31000 a risk is defined as: [The] 'effect of uncertainty on objectives'. This definition means a risk can be either a threat or an opportunity. At the heart of a good enterprise risk management (ERM) system is the ability to capture both risks, which could have a negative result, and opportunities which should have a positive effect. In order to do this an automated, integrated software solution such as Active Risk Manager (ARM) from Strategic Thought is key.

ARM's ability to record both quantitative and qualitative data means that a risk or opportunity can be placed in context together with its causes, in other words what might lead to a risk occurring, and its consequences, which is the way of describing the impact the risk may have in general terms that people can understand. ARM also captures the risk owner which is defined in ISO 31000 as an important requirement.

With traditional spreadsheet-based risk recording systems, having data captured but locked within multiple hard to access files, means employees often see only the work involved in capturing the data but do not see the benefits that result from its collection and sharing. Using ARM as the enterprise-wide risk management system unlocks the information and knowledge captured and helps embed a risk and opportunity-aware culture into the organization.

Who needs to be involved and when?

Not everyone within an organization needs to be close to the risk process on a day-to-day basis. For example the Audit committee, board members and non-executive directors will want to receive distilled information to improve periodic strategy setting and decision making. Other levels of employees across the organization will need to enter risks but will need a simple to use method of doing this. Every employee may need to be involved to form a complete picture of risks and opportunities.

What is required is a range of ways for different types of users to get involved in the process and to enter and access data. ARM, for example, has a variety of different user types which balance the relevant degree of functionality and the simplicity of the user interface.

Tom started his career in the Ministry of Defence and during his 11 years there he achieved a Masters in Defence Systems Engineering and won the GEMS award for innovation in recognition of his pioneering development of risk management software. Tom was key to the original concept and development of Active Risk Manager (ARM), and has provided risk management services and advice to most of our existing customers. The experience he gained gave him the opportunity to join Rolls-Royce corporate headquarters in 2005 as Head of Enterprise Risk Management where he was responsible for the deployment of an effective corporate risk reporting process supported by an enterprise risk software capability