ASSE Tech Brief

August 6, 2012

ANSI/ASSE/ISO Risk Management & Risk Assessment Standards

ASSE, as administrator of the U.S. Technical Advisory Group for the American National Standards Institute (ANSI) to the International Organization for Standardization (ISO) continues to receive inquiries related to the ANSI/ASSE/ISO Risk Assessment and Risk Management Standards. Thousands of these standards have been sold globally since their original approval by ISO and are having a significant impact in the U.S. and worldwide. The 31000 document ranks in the top 5 for all standards sold by ISO.

These standards received final ANSI approval on January 11, 2011. They are:

- Vocabulary for Risk Management (ANSI/ASSE/ISO Guide 73)
- Risk Management Principles and Guidelines (ANSI/ASSE/ISO 31000)
- Risk Assessment Techniques (ANSI/ASSE/IEC/ISO 31010)

All three standards are identical national adoptions of ISO standards.

ANSI/ASSE/ISO Guide 73 provides definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.

The guide is intended to be used by those engaged in managing risks, those who are involved in activities of ISO and IEC and developers of national or sector-specific standards, guides, procedures and codes of practice relating to risk management.

ANSI/ASSE/ISO 31000 can be used by any public, private or community enterprise, association, group or individual. It can be applied throughout the life of an organization and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. It can also be applied to any type of risk.

Although the standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. Design and implementation of risk management plans

and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services or assets and specific practices employed.

ANSI/ASSE/IEC/ISO 31010 is a supporting standard for Guide 73 and provides guidance on selection and application of systematic techniques for risk assessment. Risk assessment carried out in accordance with this standard contributes to other risk management activities. The application of a range of techniques is introduced, with specific references to other national and international standards where the concept and application of techniques are described in greater detail.

It should be noted that the standard is not intended for certification, regulatory or contractual use. It does not provide specific criteria for identifying the need for risk analysis, nor does it specify the type of risk analysis method that is required for a particular application. This standard does not refer to all techniques and does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature.

The standards are available for purchase as a package through ASSE's website. Given the high level of interest in these standards prior to their approval and their potential impact on the U.S. risk management and insurance industry, ASSE believes these standards will no doubt transform the way SH&E professionals manage their risk management responsibilities.

How Government Agencies Develop & Use Standards in the U.S.

- ANSI Essential Requirements
- ASSE Info on Standards Development Process
- Official Memorandum of Understanding Between OSHA & ANSI
- Office of Management & Budget Circular OMB-A119
- Position Statement on Consensus Standards
- Safeguarding: Are ANSI Standards Really Voluntary?
- What's the Difference Between an OSHA Rule and an ANSI Standard?

ISO 31000 Links, Resources & Examples of Recognition

- Canada Adopts ISO 31000 Risk Management Standard
- Dr. Marc Siegel Discussion International Security Standards & ISO 31000
- First Global Survey on ISO 31000
- ISO 31000:2009—Setting a New Standard for Risk Management
- ISO 31000 LinkedIn Site
- ISO 31000 LinkedIn Site Discussion Topics
- ISO Management Systems Special Report
- Primo-Europe
- Results of May 2012 ISO 31000 Paris Conference
- Use of ISO 31000 Risk Management Standards in Russia

May 2012 ISO 31000 Conference in Paris

- Conference Pack
- Links
- Program
- Speakers

An Inside Look at the New Risk Management Standards

Karen Hardy, Ed.D., is deputy director for risk management at the U.S. Department of Commerce. In this interview, Hardy discusses her role within the U.S. Technical Advisory Group (TAG) for Risk Management (ISO 31000) and explains the importance of the new risk management standards.

Please provide a brief description of your professional background and of your role within the U.S. TAG for Risk Management (ISO 31000).

I first engaged in the practice of risk management several years ago, right after the White House Office of Management and Budget directed government managers to strengthen their organizations' internal control system. Since that time, I have been involved in the development of risk management programs at the National Institutes of Health and contacted by other agencies to give advice about how to approach enterprise risk management.

I became the first volunteer from the federal arena to serve on the U.S. TAG for ISO 31000. As a direct result of my involvement, I was able to engage a larger community of federal risk practitioners into the ISO 31000 process, which may not have happened if I did not see the significance of this standard.

To ensure that a federal professional's viewpoint was considered in this dynamic process, I established and chaired a federal advisory group for ISO 31000, creating an opportunity that did not exist before. This was an ad hoc voluntary group of federal risk professionals who were given the opportunity to comment on the draft U.S. version of ISO 31000. I thoroughly enjoy making these inroads because quite frankly, the federal sector is usually the last to know about these emerging trends and ends up using tools and processes not designed to facilitate government-type organizations.

What are the long-term benefits of adopting these particular ISO standards as American National Standards?

Speaking from my own professional perspective, I think these standards could not come at a better time. There is an increased interest in risk management at the federal level. More agencies inquire about what risk management is and what it looks like within a federal setting. Federal agencies sponsor an annual Federal Enterprise Risk Management Summit (http://www.FederalERM.com), which is dedicated to educating the federal workforce about risk management. At a recent summit, the ISO standards were introduced to a predominately large federal audience. This type of activity did not exist six years ago, and the standards can only help expand the practice.

These catalyst standards are perfect for addressing a longstanding view that risk management is not a one-size-fits-all process. This will be a big issue for government agencies interested in referencing this standard because they all have different missions and objectives and cannot possibly adapt a one-size-fits-all process.

In my opinion, risk management can be applied programmatically, strategically and operationally in the federal government. As the practice of risk management in the federal arena matures, I think ISO 31000 will be needed to better understand the general principles for starting off on the right foot.

How do ANSI/ASSE/ISO 31000 and ANSI/ASSE/IEC/ISO 31010 complement each other?

I think the two work hand in hand. Having the global overview of the principles—"the what"—and then an accompanying document that focuses on "the how" balances out the entire process. I do not think you can have one without the other.

How do the three standards distinguish between risk assessment and risk management? Is assessment considered part of risk management?

Just from experience in instituting and designing risk management models in the federal space, I would say that risk assessment is often equated to fully being risk management though I think it is more cyclical than that. This perception is okay to some extent, but I think the overall problem is that risk assessment and risk management is often practiced in stovepipes and silos. This approach can overshadow the long-term benefit of having a more cross-cutting view of risk because risk assessment is often confined to a specific organization or area of operation. Top leadership will not have the luxury of conducting a litmus test of risk impacts (on resources or otherwise) at an enterprise-wide level.

It is important for risk to be elevated at an appropriate enterprise level to determine what the management or lack of management of the key risk areas would mean to the organization.

In your opinion, which areas of U.S. government could benefit most from the risk management standards and why?

In my professional observation, the standards serve as relative points of reference in educating federal risk professionals about risk management, risk principles and associated techniques. The standards could be used as a guide to help establish a general awareness of risk management within their organizations.

Karen Hardy, Ed.D., is deputy director for risk management at the U.S. Department of Commerce. Her comments do not reflect the viewpoints of the U.S. Department of Commerce. She may be contacted at drkarenhardy@yahoo.com.

OHSAS 18001 & ISO 31000

The following is excerpted from a discussion on the ANSI/ASSE SH&E Standards Information Center LinkedIn site:

"OHSAS 18001 has been developed to be compatible with the ISO 9001 (Quality) and ISO 14001 (Environmental) management systems standards in order to facilitate the integration of quality, environmental and occupational health and safety management systems by organizations, should they wish to do so.

"The (OHSAS) specification gives requirements for an occupational health and safety (OH&S) management system, to enable an organization to control its OH&S risks and to improve its performance. It does not state specific OH&S performance criteria, nor does it give detailed specifications for the design of a management system.

"OHSAS 18001 is not a specific BSI standard. BSI is also publishing the OHSAS standard under BS OHSAS 18001.

"ISO 31000:2009 provides principles and generic guidelines on risk management. ISO 14001 and OHSAS 18001 can be implemented into 31000.

"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 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 organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

"It is intended that ISO 31000:2009 be used to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors and does not replace those standards. ISO 31000:2009 is not intended for the purpose of certification."

ANSI/ASSE/ISO 31000
National Adoption of ISO 31000:2009
American National Standard for Risk Management Principles & Guidelines

Table of Contents & Scope

Scope
This standard provides principles and generic guidelines on risk management.

This standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this standard is not specific to any industry or sector.

Note: For convenience, all of the different users of this standard are referred to by the general term "organization".

This standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans

and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

ANSI/ASSE/ISO Guide 73
National Adoption of ISO Guide 73:2009
American National Standard—Vocabulary for Risk Management

Table of Contents & Scope

Scope
This standard provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.

This standard is intended to be used by:

- those engaged in managing risks,
- those who are involved in activities of ISO and IEC, and
- developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk.

For principles and guidelines on risk management, reference is made to ANSI/ASSE Z690.2 (ISO 31000).

ANSI/ASSE/IEC/ISO 31010
National Adoption of IEC/ISO 31010:2009
American National Standard for Risk Assessment Techniques

Table of Contents & Scope

Scope

This standard is a supporting standard for ANSI/ASSE/ISO Guide 73, *Vocabulary for Risk Management* (ISO 31000:2009), and provides guidance on selection and application of systematic techniques for risk assessment.

Risk assessment carried out in accordance with this standard contributes to other risk management activities.

The application of a range of techniques is introduced, with specific references to other national and international standards where the concept and application of techniques are described in greater detail.

This standard is not intended for certification, regulatory or contractual use.

This standard does not provide specific criteria for identifying the need for risk analysis, nor does it specify the type of risk analysis method that is required for a particular application.

This standard does not refer to all techniques, and omission of a technique from this standard does not mean it is not valid. The fact that a method is applicable to a particular circumstance does not mean that the method should necessarily be applied.

Note: This standard does not deal specifically with safety. It is a generic risk management standard and any references to safety are purely of an informative nature. Guidance on the introduction of safety aspects into IEC standards is laid down in ISO/IEC Guide 51.