SOCIETY OF ACTUARIES

Article from:

Risk Management

March 2011 – Issue 21

The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework

By Dorothy Gjerdrum and Mary Peter

ISO 31000:2009 – BACKGROUND

"Risk Management – Principles and Guidelines" is the title of the new international standard on the practice of risk management. Also known as ISO 31000:2009, it was published in November of 2009. The standard was created by a working group that included technical advisors from more than 20 countries. In a series of six meetings over several years, the group revised the Australia/New Zealand risk management standard (AS/NZS 4360:2004) to create a standard that can be used by a wide variety of organizations in any country for any type of operation, regardless of complexity, size or type. The new standard references definitions that are laid out in a related ISO document, Guide 73 (also published in November, 2009), which is a compilation of risk-related definitions and terms. Another closely related document is the standard on the process of risk assessment (ISO 31010), also published in November of 2009.

Dorothy Gjerdrum, ARM-P, is executive director of Gallagher's Public Entity and Scholastic Division. She can be reached at Dorothy_Gjerdrum@ajg.com.

Mary Peter is director of Enterprise Risk Management at Eide Bailly and can be reached at mpeter@eidebailly.com.

THE IMPORTANCE OF RISK MANAGEMENT & ITS EVOLUTION IN THE UNITED STATES

The basis for ISO 31000 follows this trajectory:

1. All organizations exist to achieve their objectives;
2. Many internal and external factors affect those objectives, causing uncertainty about whether the organization will achieve its objectives;
3. The effect this uncertainty has on an organization's objectives is "risk."

The management of risk, therefore, is central to the livelihood and success of all organizations.

Within the United States, this represents an expansion of the practice of risk management. The field of operational risk management grew out of industrial safety practices and the purchase of insurance. Therefore many organizations with traditional risk management programs included hazard identification, safety and loss control, workers' compensation, insurance procurement, self-insurance administration, claims oversight and contractual risk transfer as key functions. Those practices have been evolving and become more integrated in the past 35+ years, but the focus on operational hazard risks and the transfer and financing of those risks is still at the core of the practice.

One of the key differentiators between traditional operational risk management and this new practice of risk management as defined in ISO is the linking of key risks and the risk management process to an organization's strategic objectives. Other differentiators include identifying risks beyond insurable or industrial safety risks (including strategic, reputational and financial risks), expanding the responsibility for managing risk broadly across the organization to "risk owners" and defining a framework for managing risk that will build resilience and continual improvement throughout the process.

The ISO standard outlines a long list of the attributes of effective risk management, which includes improving corporate governance, financial reporting and stakeholder trust. When done effectively, the management of risk will raise awareness of the need to identify and treat risk throughout the organization and improve the identification of both opportunities and threats, as well as including emerging risks in the process. It will improve controls as well as operational effectiveness and efficiency. The successful implementation of risk management helps organizations comply with relevant legal and regulatory requirements and international norms. The process of risk management establishes a reliable basis for decision- making and planning, which includes the appropriate allocation of resources for the entire process. Some of the more traditional attributes of operational risk management are also included in the standard, including enhancing health and safety performance, environmental protection, improving loss prevention and incident management and minimizing

losses. And from a wider organizational perspective, the standard states that effective risk management will improve organizational learning and resilience.

The ISO standard is intended to address a wide range of stakeholders, including those responsible for developing risk management policy (e.g., policy makers), the staff members responsible for ensuring that risk is effectively managed (as a whole or for a specific project or activity), the people and departments responsible for evaluating whether risk is being managed effectively (such as audit) and for developers of standards and codes of practice.

The standard states that it can be used by any public, private or community enterprise, association, group or individual. It is not intended to be specific to any industry or sector. It is also not intended as a compliance standard.

THE PRINCIPLES, FRAMEWORK AND PROCESS OF RISK MANAGEMENT

The ISO standard outlines the principles that make risk management effective, the framework in which risk management occurs and the process for managing risk.

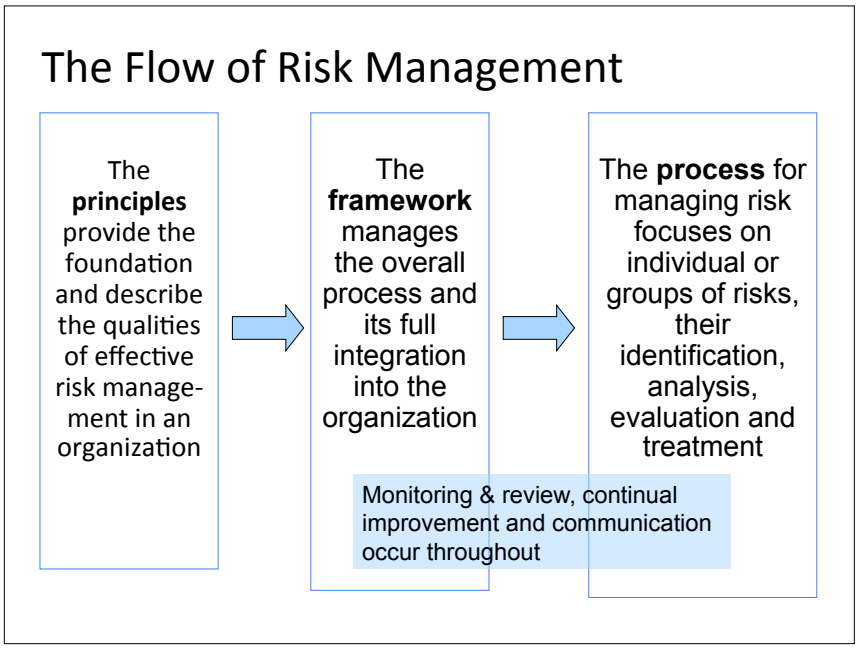
THE PRINCIPLES

The principles that govern the risk management process establish the values and philosophy of the process. The principles support a comprehensive and coordinated view of risk that applies to the entire organization. Risk management principles link the framework and practice of risk management to the strategic goals of the entity. The principles also help align risk management to corporate activities.

THE FRAMEWORK

ISO 31000:2009 emphasizes the development of a framework that will fully integrate the management of risk into the organization. The framework assures that the corporate-wide process is supported, iterative and effective. That means that risk management will be an active component in governance, strategy and planning, management, reporting processes, policies, values and culture. The framework provides for the integration of risk management, reporting and accountability. It is intended to be adapted to the particular needs and structure of each organization.

The component parts of the framework include establishing the mandate and commitment to risk management, designing the framework for managing risk (which includes understanding the organization's internal and external context, establishing a risk management policy, integration of risk management into organizational processes, internal and external communication and reporting and allocation of appropriate resources), implementing the risk management process (details follow), monitoring and review of the process and continual improvement of the framework.



CONTINUED ON **PAGE 10**

The New International Standard … | from Page 9

THE RISK MANAGEMENT PROCESS

The core of the risk management process incorporates the five steps of a traditional operational risk management process (identify risks, analyze risk treatment options, select the best response, implement risk mitigation and controls and monitor results and revise as necessary). In the ISO model, they are central to the process of managing both individual and portfolios of risks. A significant difference from the traditional process is that the ISO model includes the elements of 'establishing the context' and continuous 'communication and consultation'. Before you begin the process of assessing risk, you must establish the detailed context, which sets the scope and risk criteria for the process. Then, in addition to the core steps of the process, the ISO Standard identifies two key functions that should happen continually throughout the risk management process: 1) Communication & Consultation, which needs to be built into the process and involve both internal and external stakeholders, and 2) Monitoring & Review, which occurs continually during the process.

Establishing the context of the risk management process will vary according to the structure and the needs of the organization. It will include activities like setting goals and objectives for risk management, and defining the responsibilities, scope, depth and breadth of the process. This is a critically important step in the process because it will assure that the risk management approach is appropriate to the organization, its risks and objectives. It also includes a detailed analysis of the internal and external stakeholders, environment and key drivers and trends that have an impact on the objectives of the organization.

Risk assessment is the overall process of risk identification, analysis and evaluation. Identifying risk includes understanding the sources of risk, areas of impact, events and their causes and potential consequences. The goal is to create a comprehensive list of risks, including risks that may be associated with missed opportunities and risks out of the direct control of the organization. A comprehensive review allows a full consideration of potential effects of risk upon the organization.

The purpose of analyzing risk is to understand everything possible about risks, including the causes and sources, consequences and likelihood of occurrence. Existing controls and their effectiveness and efficiency are also taken into account.

The purpose of risk evaluation is to review the analysis, criteria and tolerance of risks in order to prioritize and choose appropriate risk treatment methods. An organization's legal and regulatory environment and its internal and external context will also be considered at this stage. The evaluation process helps organizations make appropriate decisions about whether and how to treat risks.

Risk treatment involves selecting one or more options for modifying risks and implementing those options. It is a cyclical process that assesses a risk treatment, determines whether the residual risk is at a tolerable level (and if not, which additional treatments need to be implemented) and assessing the effectiveness of treatments.

Communication and consultation must take place throughout the process and should include both internal and appropriate external stakeholders. Risk management cannot succeed if it does not consult with and engage stakeholders in the process.

Monitoring and review is critical to the process because it assures that controls are effective, lessons are learned, risks will be appropriately addressed and the organization will be resilient and ready for change.

COMPARISON OF ISO AND COSO

The comparison of a few key definitions will illustrate key differences between ISO 31000 and the COSO ERM Framework. The COSO ERM Framework is a complex, multilayered and complicated directive that many organizations have found difficult to implement. ISO provides a more streamlined approach that is easier to digest. ISO is based on a management process, and through tailoring the process for each organization, it integrates into existing management and strategic initiatives. The COSO model is control and compliance based, and that contributes to it being difficult for traditional risk managers to embrace. If COSO were implemented by an organization's internal audit team, there is the problem of having the program audited by the same people who enacted it; ISO allows for the independent audit function to occur during the monitoring and review phase. COSO was authored by auditors, accountants and financial experts; ISO was authored by risk management practitioners and international standards experts.

"A significant difference from the traditional process is that the ISO model includes the elements of 'establishing the context' and continuous 'communication and consultation'."

Key Term or Description	ISO 31000:2009	COSO ERM Framework
Scope.	This International Standard provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.	This definition (of ERM) is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.
Risk management, defined.	Coordinated activities to direct and control an organization with regard to risk.	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.
Risk, defined.	The effect of uncertainty upon objectives.	The possibility that an event will occur and adversely affect the achievement of objectives.
Risk appetite, defined.	The amount and type of risk that an organization is willing to pursue or retain.	A broad amount of risk an entity is willing to accept in pursuit of its mission or vision.
Risk assessment, defined.	The overall process of risk identification, risk analysis and risk evaluation.	Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
Risk management process	Continually and iteratively : Communicate and consult • Establish the context • Risk assessment: o Identification o Analysis o Evaluation • Risk treatment Continually & iteratively: Monitor and review	• Internal environment • Objective setting • Event identification • Risk assessment • Risk response • Control activities • Info & communication • Monitoring

CONTINUED ON **PAGE 12**

The New International Standard … | from Page 11

Reviewing ISO and COSO together may provide the opportunity for risk management practitioners and auditors to integrate and strengthen their activities. Depending if your organization's view and success with COSO, it may be beneficial to review how ISO may provide an approach to design a path that would be more effective toward accelerating growth and profitability across the enterprise.

CONCLUSION

For internal auditors and traditional risk managers in the United States, it is important to remember that this new ISO 31000 standard is intended to build upon what is already being done well and expand your view about risk. For decades, traditional operational risk managers have been incredibly creative and forward-thinking about risk finance and risk transfer techniques. Internal auditors have been focused on the control mechanisms with respect to mitigating risk. Organizations have not been as forward-thinking about identifying a broad range of risks (beyond insurable risk, beyond hazard identification, beyond emergency planning or disaster preparedness) or addressing cumulative or crossover risks. COSO ERM supports and can expand upon the internal financial control concepts of Sarbanes-Oxley for companies in the United States. Its objectives look to improve organization performance through better integration of risk management, strategy, control, and governance.

The authors believe that there is more in common between the two standards than in opposition. If you have fully implemented COSO, there may be no need for you to consider switching your format to the ISO standard – as long as you recognize the weaknesses of COSO and compensate for them. On the other hand, if you have not been able to achieve full implementation of COSO, you could switch to ISO without losing any ground, and you would likely simplify and strengthen your process during the transition.

A real strength of this new ISO 31000 risk management approach is the identification of risk owners and the necessary widespread education about risk—both within and without your organization. It increases accountability and strengthens communication. The link to business objectives (at all levels) strengthens both the relevance and the importance of risk management. Ultimately, the ISO 31000 standard provides a vehicle to make risk management central to the success of an organization, and an intimate part of key processes such as planning, management and governance.

Dorothy M. Gjerdrum, ARM-P, is executive director of Gallagher's Public Entity and Scholastic Division. She leads 300 Gallagher insurance brokers and specialists dedicated to public sector clients across the United States, focusing on issues of risk management, exposure identification, pool operations and enterprise risk management. In addition to leading the broker group, Dorothy provides consulting and risk management services to select Gallagher public sector clients. She is chair of the ISO 31000 US Technical Advisory Group.

Mary Peter is Director of Enterprise Risk Management at Eide Bailly LLP and leader of their ERM consulting services. She brings over 20 years of risk management experience, including 10 as a corporate risk manager. Mary designs and implements client-specific ERM programs, training, and deliverables to respond to regulatory requirements and strategic objectives of her clients. She is a member of the ISO 31000 US Technical Advisory Group and co-chair of an ERM Roundtable bringing traditional risk management and audit disciplines together. ■

RESOURCES

- COSO ERM Framework, www.coso.org
- ISO 31000, Guide 73, ISO 31010 can be purchased in US$, www.ansi.org

A few important acronyms:

TAG = Technical Advisory Group. Each participating country had a sponsoring organization (in the US, it was ANSI) which formed a TAG comprised of experts from various industries and disciplines. In the US, ANSI delegated the TAG administration to ASSE.

ASSE = the American Society of Safety Engineers. ASSE is the world's oldest and largest professional safety organization.

ANSI = the American National Standards Institute. ANSI oversees the creation and promulgation of thousands of norms and guidelines for US business operations.

COSO = Committee of Sponsoring Organizations of the Treadway Commission

COSO II or COSO ERM = COSO Enterprise Risk Management – Integrated Framework Published in 2004.

ISO = the International Organization for Standardization. ISO is based in Geneva, Switzerland and is the world's largest developer and publisher of international standards.