Risk Management’s Standard of Practice – An Overview of ISO 31000

Gallagher ERM Practice
Background

ISO 31000 (published in the United States as ISO/ANSI/ASSE 31000) is the only international standard for the practice of risk management. It was issued in December of 2009, by an international working group that included technical advisors from 26 countries. In a series of six meetings over several years, the group revised the Australia/New Zealand risk management standard (AS/NZS 4360, published in 2004) to create a standard that can be used by any type of organization in any country for any type of operation. It is scheduled to be revised for the first time in late 2015 by a consortium of experts from around the world; the expected publication date of the revision will be sometime in 2017.

ISO 31000 was intended to be a guide for practitioners, decision makers, policy makers and those interested in risk management. It provides a framework for organizations wanting to manage risk consistently, efficiently and effectively. The standard was published along with two related risk management documents; Guide 73, which is a compilation of risk-related definitions and terms and ISO 31010, a compilation of risk assessment techniques. Guide 73 applies to other standards, including safety related documents, and is intended as a guide for developing a universal language of risk. ISO 31010 is currently under revision, in an effort to expand upon, categorize and clarify risk assessment techniques.

An implementation guide (published as a technical report) was released in 2014 as ISO 31004. A technical report does not carry the same weight of a standard; it a working document of best practices from around the world. The purpose was to provide examples and advice about implementation of ISO 31000.

Introduction & Applicability

The basis for ISO 31000 follows these assumptions:

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.”

In summary, the management of risk is central to the livelihood and success of all organizations.

ISO 31000 applies to organizations of all types and sizes. It outlines the principles that make risk management effective; a framework to support the implementation and continual improvement of risk management throughout the organization and the process for managing risk. This is the basic “architecture” of risk management, which, if applied, will create a consistent and coherent basis for managing the effects of uncertainty upon organizational objectives – or, in simpler terms – for managing risk.

The standard delineates 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. It will improve controls and treatments 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, and will appropriately allocate and use resources for risk treatment. Some of the more traditional attributes of effective 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 an organizational perspective, effective risk management will improve organizational learning and resilience.

Intended Audience

ISO 31000 is intended to meet the needs of a wide range of stakeholder; including those responsible for developing risk management policy (e.g., policy makers), ensuring that risk is effectively managed (as a whole or for a specific project or activity), evaluating whether risk is being managed effectively (such as audit) and developers of standards and codes of practice.

The standard 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.

Key Definitions

Risk is the effect of uncertainty on objectives.

Risk management is the coordinated activities to direct and control an organization with regard to risk.

Risk management framework is the set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

Risk attitude is an organization’s approach to assess and eventually pursue, retain, take or turn away from risk.
Risk appetite is the amount and type of risk that an organization is prepared to pursue, retain or take.

Risk tolerance is an organization’s or stakeholder’s readiness to bear the risk after risk treatment in order to achieve its objectives.

Risk owner is the person or entity with the accountability and authority to manage the risk.

External context is the external environment in which the organization seeks to achieve its objectives. This includes the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment – whether international, national, regional or local; key drivers and trends that will have an impact upon objectives and the relationships with and perceptions and values of external stakeholders.

Internal context is the internal environment in which the organization seeks to achieve its objectives. This includes governance, organizational structure, roles and accountabilities, policies, objectives, strategies, capabilities, resources, standards, the perceptions and values of internal stakeholders, information systems, the organization’s culture and contractual relationships.

Risk criteria is the terms of reference against which the significance of a risk is evaluated.

Residual risk is the risk remaining after risk treatment.

For additional definitions and explanations of terminology, refer to Guide 73 and the explanatory notes.

The Principles

The principles provide guidance on the rationale for managing risk and the characteristics of effective risk management. They shape the design and structure of an organization’s risk management framework and can assist in assessing the effectiveness and quality of risk management.

There are 11 principles guide the way that risk management is integrated and deployed:

1. Risk management creates and protects value;
2. Risk management is an integral part of all organizational processes;
3. Risk management is part of decision making;
4. Risk management explicitly addresses uncertainty;
5. Risk management is systematic, structured and timely;
6. Risk management is based on the best available information;
7. Risk management is tailored;
8. Risk management takes human and cultural factors into account;
9. Risk management is transparent and inclusive;
10. Risk management is dynamic, iterative and responsive to change; and
11. Risk management facilitates continual improvement of the organization.

The Framework

The standard outlines a framework that will assure that the process for managing risk is fully integrated into the organization. That means that the management of risk is an explicit component of governance, strategy and planning, management, reporting processes, policies, values and culture. The framework provides for the integration of risk management information, 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 framework and continual improvement of the framework and approach to risk management.

The full and active development of a sustainable framework for managing risk and integrating risk management into key management processes is the “heart” of the ISO 31000 standard and it is what will keep the “beat” of risk management alive in an organization. It provides the basis for sustainable effort and continual improvement.

The Risk Management Process

The ISO 31000 model puts emphasis on each organization’s context of operations. Context affects the design of the framework for managing risk and it is a part of each and every risk management process. The context of operations includes explicit consideration of internal and external aspects of operations (such as governance, policies, technology, culture—and more) as well as stakeholders (both internal and external). Understanding these critical factors help to shape the process of assessing, treating and communicating about risk.

The core of the risk management process incorporates the five steps from a “traditional” risk management process (identify, analyze, select the best response, implement and monitor)–but expands upon them in two significant ways. The first is that the consideration of context is always the starting point for a risk management process. This is true whether you are assessing the risks of a part of your operations (a department with high-risk activity, for example), creating a broad inventory of risks or making an individual decision. The explicit consideration of context grounds the process into your organizational reality.

Context includes the review of organizational objectives and mission and establishes the objectives, scope and parameters of the risk management process. It also requires understanding of the internal and external environment of operations and the stakeholders that might be affected by the results of the risk management process. The context will also define the parameters, methodology and risk criteria to be used in the process.

The other unique aspect of the ISO 31000 risk management process is the clear consideration and inclusion of stakeholders. Stakeholders are both internal and external to the organization and they include any person or organization that can affect, be affected by or perceive themselves to be affected by a decision or activity. ISO 31000 expects that you will consider, consult and communicate with stakeholders throughout the risk management process. This is represented in the diagram by arrows at every step of the process.

Here are some examples of how stakeholders are engaged in risk management:

• A broad cross-section of internal stakeholders participate in a risk identification workshop to identify and assess key risks.
• Key external stakeholders provide input to a university's register of key risks, verifying risk rankings and giving input to emerging risks.
• For a key decision, both internal and external stakeholders participate in a risk assessment process that considers how uncertainties may affect the ability to achieve successful results.
• The corporate risk profile is provided to financial rating agencies as proof of the organization's ability to manage risk and address emerging risks (this has the potential to improve credit rating scores).
Working through each step in the risk management process includes:

- Considering the **context** of the organization and establishing the **context** of the risk management process

**Risk assessment process:**

- Identify risks
- Analyze risks
- Evaluate risks

**Risk treatment**

**Monitor and review** (which happens continually and at each step)

**Communication and consultation** (which happens continually and at each step)

**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.

**Risk evaluation** is the step that will help determine the need for treatment. Risk tolerance must be taken into consideration, along with legal, regulatory and other requirements. The evaluation process will help you make the appropriate decision about whether and how to treat risks.

**Risk treatment** involves selecting one or more options for modifying risks and implementing those options. Options include avoiding the risk, removing the risk source, changing the likelihood or consequence, sharing the risk, taking or increasing risk in order to pursue an opportunity or retaining the risk by informed choice. 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 evaluates the effectiveness of treatments.

ISO 31000 emphasizes that you must **monitor and review** at each step along the way and also **communicate and consult** at every step of the risk assessment process; not just at the end of the process. Monitoring and review assures that controls are effective, lessons are learned and that risks will be appropriately addressed and the organization will be resilient and ready for change. Communication and consultation need to be built into the process and involve appropriate internal and external stakeholders. This makes the ISO 31000 approach to risk assessment more dynamic, resilient and engaged.

---

The International Organization for Standards (ISO) is headquartered in Geneva Switzerland. Its sole purpose is to develop and publish international standards to ensure that products and services are safe, reliable and of good quality. A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose. ISO has published more than 19,500 standards covering almost all aspects of technology and business. [www.iso.org](http://www.iso.org)

In the United States, standards are adopted and published by the American National Standards Institute (ANSI). For the development of standards relating to risk management, ANSI has designated the American Society of Safety Engineers (ASSE) as the secretariat for U.S. experts who contribute to the ISO 31000 suite of standards. You can purchase the ISO 31000 series of standards from ASSE at [www.asse.org/publications](http://www.asse.org/publications).
What Do We Gain From Using ISO 31000?

For traditional risk managers in the U.S., it is important to remember that this new standard is intended to build upon what you already do well and expand your views about risk. For decades, we have been creative and forward-thinking about risk finance and risk transfer techniques. We 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 (such as IT or pandemic planning). We can also learn how to expand the application of risk management to decision making, which will strengthen the understanding and application of risk management throughout our organizations.

The identification of risk owners and education about risk – for stakeholders inside and outside of our organizations – is another key expansion from a more traditional approach to managing risk. Those activities will increase accountability and strengthen communication. The link to business objectives (at all levels) strengthens both the relevance and the importance of risk management. Ultimately, it will make risk management central to the success of an organization, and an influential part of key processes such as planning, management and governance.

Conclusion

The goal of effective risk management is to ensure that an organization has a current, correct and comprehensive understanding of its risks – and that those risks are within its risk tolerance. The attributes include full accountability, the application of risk management in all decision making, continual communication, full integration into the organization’s governance structure and continual improvement.

Implementing a broader approach to managing risk is a process that takes time, planning and sustained initiative. You need a good road map and a plan. The model for implementation and tools provided in the ISO suite of standards can guide your course of action and assure leadership that you are following an internationally approved model, based on best practices from around the world.

If you are ready to lead your organization’s approach to evolving risk management, this standard should be your first step and your guide.
About the Author

As Senior Managing Director, Dorothy Gjerdrum leads Gallagher’s largest client practice group, which includes cities, counties, K-12 public schools, state governments, special districts and public sector pools. She has 25 years of public sector risk management experience.

In 2015, Dorothy accepted an additional leadership role as Managing Director of Gallagher’s ERM Practice Group. From 2008-2014, Dorothy was the Chair of the US Technical Advisory Group to ISO 31000 which is responsible for representing the interests of the United States risk management community in the standards development process. In addition to leading Gallagher Public Sector, Dorothy is a leading ERM consultant for cities, counties, public school districts, community colleges and public universities. She is a frequent speaker on ERM and ISO 31000 and its application in the public sector.

For more information, contact:

Dorothy Gjerdrum, ARM-P
Senior Managing Director, Gallagher Public Sector
Managing Director, Gallagher ERM Practice Group
dorothy_gjerdrum@ajg.com