Advisera

Article

What is ISO 31000?

By Rhand Leal

ISO 31000 is an international standard published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). Its full name is ISO 31000 – Risk management – Guidelines.

ISO 31000 is the leading international standard focused on risk management. It provides a framework to help organizations, of any size or any industry, to identify, assess, evaluate, and treat risks in a systematic and cost-effective way.

What is the purpose of ISO 31000?

The purpose of this standard is to develop a risk management approach and awareness of the importance of monitoring and managing risks among employees and stakeholders.

ISO 31000 provides principles, a framework, and a process to help organizations, of any size or any industry, manage risks in a systematic and cost-effective way. Its principles, framework, and process allow for the management of any type of risk (e.g., information security risks, business continuity risks, financial risks, environmental risks, quality risks, etc.).

Contrary to the widely used financial-based risk management standards and models, ISO 31000 is a standard that can be implemented easily by any public, private sector, or non-governmental organization, regardless of its size or field of activity.

ISO 31000 structure

ISO 31000 consists of an introduction, six clauses, and a bibliography.

The introduction and clauses 1 to 3 (Scope, Normative references, and Terms and definitions) serve as a presentation of the ISO 31000 standard, and provide a detailed glossary of risk management terms.

Clause 4 is about risk management principles, the foundations to be considered when defining a risk management framework and process. There are eight principles: Integration, Structured and comprehensive, Customized, Inclusive, Dynamic, Uses best available information, Considers human and culture factors, and Practices continual improvement.

Clause 5 is about the risk management framework, the elements to be considered to ensure that the risk management process is fit for purpose and can adapt to the organization's needs. There are six framework components: Leadership and commitment, Integration, Design, Implementation, Evaluation, and Improvement.

Clause 6 is about the risk management process, the logical steps to be considered to perform risk management. There are six steps: Communication and consultation; Definition of scope, context and criteria; Risk assessment; Risk treatment; Monitoring and review; and Recording and reporting.

Finally, the bibliography refers to other ISO standards relevant to ISO 31000 (currently just ISO 31010, Risk management – Risk assessment techniques).

Does ISO 31000 provide risk methodology?

ISO 31000 does not provide a specific methodology for, e.g., information security risk management, quality risk management, or environmental risk management. Instead, it is a basic framework upon which other standards are developed that do provide more specific methodologies – for example, the ISO 27005 standard is largely based on ISO 31000, and it provides guidelines for information security risk management.

What is the ISO 31000 definition of risk, and what is risk management?

ISO 31000 defines risk as the effect of uncertainty on objectives. Uncertainty is doubt – the possibility of a different outcome, whether more positive or negative, than the expected one.

Now, risk management, according to ISO 31000, refers to coordinated activities to direct and control an organization regarding risks. Simply put, risk management is the method of dealing with possible dangers that threaten a company.

For example, an organization may be situated in a location susceptible to natural disasters (e.g., earthquakes, floods, etc.), be part of an industry with a lot of competitors, or be highly dependent on the global economy (e.g., overseas suppliers and customers).

To minimize the consequences related to these scenarios, organizations have to manage their risks; and, by adopting ISO 31000, they will have the basis to do so in a cost-effective way.

Related Articles

How to use the inputs from the context of the organization (clauses 4.1 and 4.2) to build your management system

by Mark Hammar

Risk-Based Auditing: A Smarter Way to Ensure Management System Effectiveness

by Carlos Pereira da Cruz

ISO 27001 and the Data Governance Act (DGA): Ensure Secure Data Management

by Rhand Leal

What are the eight principles of ISO 31000?

ISO 31000 clause 4 defines eight principles to be considered when establishing the organization's risk management framework and processes:

- **Integration**. Organizations should **integrate** risk management into their business activities. The risk management process should not be separate, but connected to the organization's other processes.
- **Structured and comprehensive**. Approaching risk management in a systematic, **structured, and comprehensive** way will bring reliable and comparable results for the company.
- **Customized**. Companies should determine their internal and external context and have a **customized** risk management framework and processes established. An organization's context includes its values; stakeholders; and local, national, and international relationships; as well as its social, cultural, political, legal, regulatory, financial, technological, economic, natural, and competitive environment.
- **Inclusive**. Organizations should have an **inclusive** approach for stakeholder (employee, customer, investor, government) engagement. Communicating, as well as getting and sharing information, views, and perceptions with stakeholders will help the company to be aware of needs and changes.
- **Dynamic**. Today's companies should be aware of the internal and external nature of the changes in trends and the environment. This means that new risks may emerge in such

transformations and processes. Therefore, risk management must be **dynamic**, so that the organization stays up to date.

- **Uses best available information**. The risk management process is based on collected data, experience, observation and expert opinion. Having **best available information** is essential for carrying out activities and recognizing models and data that are important.
- **Considers human and culture factors.** Organizations must take **human and cultural factors** into account. Understanding the capabilities, perceptions, and culture of the people who work for the organization will help the organization to understand better risks, and it will facilitate the achievement of objectives and their positive results in business operations. If not considered, these factors can cause errors such as lack of knowledge and failures to detect, and demand a system to respond with early warnings for incidents.
- **Practices continual improvement**. Similar to other ISO standards, ISO 31000's last principle emphasizes **continual improvement**, which can be gained through learning and experience.

What are the benefits of ISO 31000?

The implementation of ISO 31000 not only helps businesses to see positive opportunities and negative consequences related to various risks, but also enables them to:

- Give confidence to employees, customers, and other stakeholders
- Build a culture of prevention
- Minimize surprises and losses
- Provide analysis of opportunities and threats
- Comply with relevant legal and regulatory requirements and international norms
- Ensure precautions are taken before risks arise

What is the ISO 31000 risk management framework?

The ISO 31000 risk management framework, defined in clause 5, describes how to manage and control the risk management process. The success of risk management depends on how well it is managed and controlled.

The elements of the framework can be detailed as follows:

Leadership and commitment are at the center of the framework. Top management needs to be engaged and supportive, which is critical for risk management. This can be demonstrated by:

- Issuing and communicating a risk management policy
- Allocating financial resources to risk management
- Assigning roles and responsibilities at appropriate organizational levels
- Monitoring risks and results of risk management activities systematically
- Being accountable for managing risk

Integration is about ensuring all risk management activities are embedded in the company's daily operations and key activities. When this integration is achieved properly, risk management becomes a natural part of the job, not an additional thing to do.

Design refers to understanding the organizational context, and articulating with top management, to structure how the steps of the risk management process, and the necessary components, will relate to each other.

Implementation refers to the deployment of documents (e.g., policies and procedures), technologies, and other resources so the designed risk management process can work. At the implementation phase, the company should develop a risk management plan. The plan should detail the specific actions to be taken and their sequence, including time and resources, and define who will make the decisions.

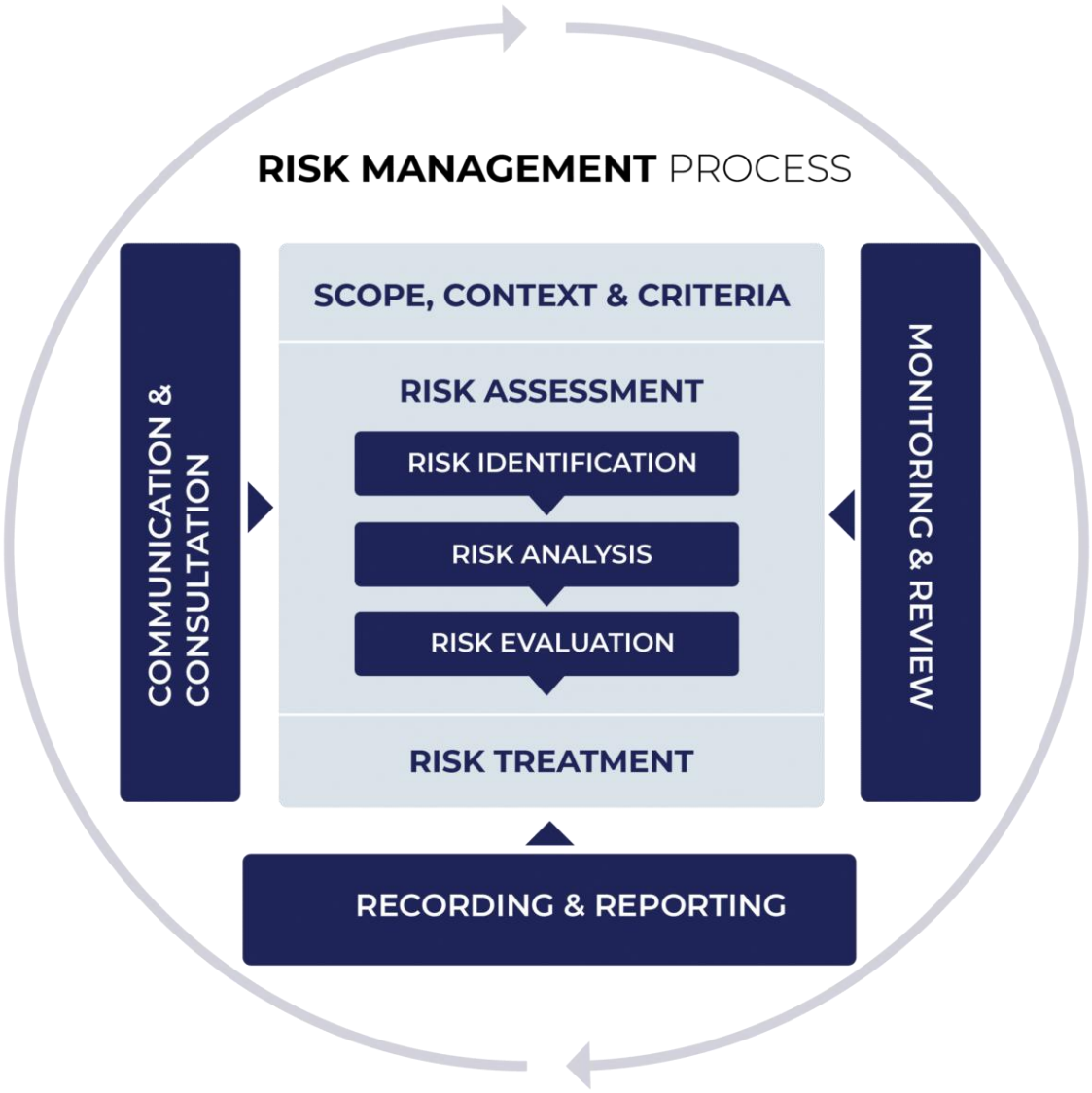
When considering **evaluation**, the effectiveness of the risk management process and activities are measured and periodically reviewed. The significant issues identified during evaluation should be reported to those who are accountable, where the last element of the risk management framework is applied.

Based on the results of the evaluation, the organization will be able to see their progress and gaps and make decisions for **improvement**. Other triggers for improvement besides evaluation include the availability of new knowledge, as well as significant changes to the organization's internal and external context.

This framework is very similar to the plan-do-check-act (PDCA) approach of management system standards.

What is the ISO 31000 risk management process?

ISO 31000 doesn't have specific requirements, but its clause 6 provides general guidance on the risk management process – it describes the six steps needed for risk management.



1) Communication and consultation

These activities are performed throughout all other steps of risk management to ensure that relevant stakeholders (internal and external):

- Are aware of and understand the risks and how to deal with them

- Receive feedback and information for proper decision-making

These activities often involve bringing different areas of expertise, and consideration of different points of view and scenarios, to the remaining activities of the risk management process.

2) Scope, context and criteria

The risk management process effectively starts by defining what we want to achieve and attempting to understand the external and internal factors that may influence our success. This step is called "Scope, context and criteria," and it is essential before risk identification. In keeping with the ISO 31000 risk management process, developing appropriate risk criteria is vital and needs to be defined when establishing the context, and then applied during risk evaluation. Risk criteria simply refers to the level of risk the company may or may not take. To set the risk criteria, organizations may consider the following:

- Nature and type of uncertainties
- Method of defining and measuring consequences and likelihood
- Time-related factors
- Levels of risk
- Organization's capacity
- Management of combinations and sequences of multiple risks

3) Risk assessment

The next step is **risk assessment**, which has three activities in sequence:

1. **Risk identification**: understanding of uncertainties, threats, and scenarios, and listing all risks.
2. **Risk analysis**: understanding the consequences and likelihood of risks. Risk analysis enables risks to be prioritized.
3. **Risk evaluation**: refers to the definition of the level of priority of each risk through the application of the risk criteria developed when the context was established.

There are various methods for risk assessment, such as the popular probability and consequence matrix, the Delphi technique, the decision tree model, and FMEA (Failure Modes and Effects Analysis). For further information, you can check ISO 31010.

4) Risk treatment

After the assessment stage, the next step is risk treatment, which involves selecting and implementing options for addressing risks. Selection involves comparing potential benefits with costs or efforts of implementation of alternatives. The options may be selected from one or more of the following:

- **Avoidance**: If the risk is too high, you can decide not to start (or continue) the activity you had planned. For example, if there are too many strict regulations in an area where you want to open a new branch of your company, you avoid risk by not starting it at all.
- **Sharing**: You can distribute the risk to another party. Joint ventures exist precisely for this reason. You open your branch in partnership with another company that has expertise on using the regulations to its advantage.
- **Transferring**: You can transfer all or part of the risk to a third party. For example, a company may outsource some of its activities from the scope of IT security, or take out an insurance policy.
- **Acceptance**: Knowing and being aware of the consequences, you may prefer to face the risk. You just open that branch in a highly regulated area. Acceptance is also known as risk retention.
- **Reducing**: Risk reduction is the most common option, and it's taking mitigation actions to decrease risk levels. An example of this would be training your staff on how to identify a phishing email; or, by implementing backup, you can decrease the risk of data loss.

For implementation, you will need a risk treatment plan that defines activities, resources, responsible parties, and deadlines.

5) Monitoring and review

Monitoring involves continually checking actual performance, and then comparing that with the expected or required performance. The review involves periodic or impromptu checking of the current situation for changes in the environment, industry practices, or organizational practices. It

is an activity undertaken to determine the suitability, adequacy, and effectiveness of the framework and process to achieve the established objectives.

6) Recording and reporting

The risk management process and its outcomes should be documented and communicated. Therefore, they should be recorded and reported. Organizations should decide what they should record, such as incidents, near misses, non-compliance, system availability, etc. These records provide information for decision-making to increase the effectiveness of activities.

Reporting should provide information to top management and the organization's stakeholders about whether the risks are within the risk criteria, or whether there are credible risk treatment plans that will ultimately lead to this result. Additionally, it may provide information about new and emerging risks, and the report may provide recommendations for system improvements based on what the reviewers have observed.

Is ISO 31000 free?

No, unfortunately ISO 31000 is not free. Like most ISO publications, you can purchase it from the ISO website. You can also check your national standards organization to find out if a translation is available in your native language.

Is there an ISO 31000 certification?

ISO 31000 cannot be used for certification, because it doesn't specify requirements. However, organizations using ISO 31000 can compare their risk management practices with an internationally recognized framework, and individuals can attend courses related to ISO 31000 and become certified as competent in its concepts.

To see how to manage information security risks through the Risk Register, sign up for a 14-day free trial *of Conformio, the leading ISO 27001 compliance software.*

About the author:

Rhand Leal

Rhand Leal has more than 15 years of experience in information security, and for six years he continuously maintained a certified Information Security Management System based on ISO 27001. Rhand holds an MBA in Business Management from Fundação Getúlio Vargas. Among his certifications are: ISO 27001 Lead Auditor, ISO 9001 Lead Auditor, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), and others. He is a member of the ISACA Brasília Chapter.

Advisera Expert Solutions Ltd
for electronic business and business consulting
www.advisera.com

Our offices

US Office
1178 Broadway, 3rd Floor #3829
New York NY 10001
United States

EU Office
Zavizanska 12
10000 Zagreb
Croatia, European Union

EMAIL:
suport@advisera.com

Advisera