A Comprehensive Guide to the ISO 31000

Table of Contents

- A Comprehensive Guide to the ISO 31000
- What is ISO 31000:2018?
- What is in the Updated ISO 31000:2018?
- What is the ISO 31000 Risk Management Process?
- ISO 31000 Risk Management Standard
- The Importance of Getting Certified
- FAQs About ISO 31000 Risk Management
- Simplifying the ISO 31000 Process with iAuditor
A Comprehensive Guide to the ISO 31000

What is ISO 31000:2018?

ISO 31000 is a family of standards that pertain to risk management within an organization. These are the international standards that outline a generic approach to risk management, which organizations can use as a launching point.

There are many problems that organizations deal with on a daily basis such as looking to assess and improve different processes to boost productivity and efficiency. On top of that, they also have to deal with numerous risks that can vary depending on their industry.

The ISO 31000 risk management standard is designed to give organizations a framework when tackling the risks that they and their employees face throughout their operations.

What is in the Updated ISO 31000:2018?

In 2018, the ISO 31000 risk management standards were revised to allow companies more flexibility in implementing the principles in a way that suits their objectives and goals. ISO 31000 also redefined risk as the “effect of uncertainty on objectives” which emphasizes the effect of not knowing the entirety of potential challenges that can negatively impact an organization and its operations. The updated ISO 31000:2018 can serve as a guide for businesses to develop more robust risk management plans and apply them accordingly.

Here are the four major updates to ISO 31000:2018:

- Review of the principles of risk management, which are the key criteria for its success
- Focus on leadership by top management who should ensure that risk management is integrated into all organizational activities, starting with the governance of the organization
- Greater emphasis on the iterative nature of risk management, drawing on new experiences, knowledge, and analysis for the revision of process elements, actions, and controls at each stage of the process
- Streamlining of the content with a greater focus on sustaining an open systems model that regularly exchanges feedback with its external environment to fit multiple needs and contexts.

Learn more about the ISO 31000:2018 risk management standards revisions in this PDF.
A Comprehensive Guide to the ISO 31000

What is the ISO 31000 Risk Management Process?

The ISO 31000 provides a general approach to risk management for all businesses and industries. So, while organizations may use this as a framework for their risk management process, it’s important to understand that you may have to add or tweak the framework a bit to better cover the needs of your business.

That said, the ISO 31000 Risk Management Standard does contain all the steps necessary in an effective risk management strategy. These steps include:

1. **Identification**
   
   To start the process, organizations must first identify which risks are present throughout their operations. This involves identifying hazards, safety concerns, and other factors that may hinder a business from achieving its safety and productivity goals. During this step, it’s crucial for inspectors to cover all bases and ensure that there are no risks that remain unidentified.

---

1. **Identification**
2. **Analysis**
3. **Evaluation**
4. **Treatment**
5. **Establishing Context**
6. **Monitoring and Review**
7. **Communication and Consultation**
2. Analysis

After determining the different risks present throughout the organization, the team must analyze them. During this phase, they can identify the sources, causes of certain risks, and the probability of accidents even with the current control measures; and establish the specific risk level that employees and organizations face.

3. Evaluation

The next step is evaluating if the risk analysis results show that the residual risks of the processes are tolerable within the organization. These results are compared to specific risk criteria in this phase.

4. Treatment

This involves placing controls and measures to reduce and manage the risk within an organization. The goal of this phase is to decrease the likelihood of certain risks down to a point where the organization reaps the ideal net benefits.

5. Establishing Context

This phase was recently added to the standard and involves establishing the assessment's scope, defining the objectives, and establishing the criteria for risk evaluation. During this phase, it’s important to consider external and internal elements to ensure a comprehensive risk management process.

6. Monitoring and Review

This involves reviewing the overall risk management process and comparing performance against certain indicators. This is to determine whether the risk management process is still appropriate and relevant. If there are any lapses found in the process, it's important to take steps to correct that to set the organization on the right path.

7. Communication and Consultation

This is one of the most important phases of the risk management process. It involves regular and proper communication between all interested parties to ensure that everyone is on the same page in terms of the organization's risk management process.
A Comprehensive Guide to the ISO 31000

ISO 31000 Risk Management Standard

The latest ISO 31000:2018 Risk Management standard is depicted as a trinity of Principles, Framework, and Processes. These three components come together to ensure:

- **Principles** – Sustaining a dynamic and continuously improving risk management system that is customized, innovative, dynamic, structured, and inclusive;
- **Framework** – Senior management leads the proactive integration of risk management on all levels of the organization; and
- **Processes** – Systematic application of policies and practices that support open communication, consultation, and risk reporting

With ISO 31000:2018's iterative process to risk management, there will be a need for an organization to continuously report, review, and consider the right action to treat risks. It would be near impossible to successfully implement and sustain the ISO 31000 risk management standard if an organization's process is heavily dependent on paper-based communication and record keeping.

The Importance of Getting Certified

Any organization, regardless of the industry, is exposed to significant risks. And when conducting operations, it’s important for the organization to identify the risks, mitigate them, and manage the ones inherent to the industry. This is to ensure that all employees are safe throughout operations and that the organization remains productive and efficient.

Getting an ISO 31000 risk management certification shows that an organization has done the appropriate steps in identifying and managing the risks that employees face during operations. It also indicates that you are capable of helping other organizations identify risks and establish their risk management plan and process.

The risks that employees and businesses face in their operations could result in accidents and injuries and even hinder productivity. By taking the time and putting in the effort to manage these risks, organizations won’t just be able to improve employee safety; they will also be able to boost efficiency and productivity.
A Comprehensive Guide to the ISO 31000

FAQs About ISO 31000 Risk Management

What are the Standards Under ISO 31000?
The current standards under ISO 31000 include:

- ISO 31000:2018
- ISO 31004:2013
- ISO 31010:2019
- ISO 31022:2020
- ISO 31030:2021

All these standards deal with risk management strategies, establishing guidelines that organizations may follow.

What are the Core Principles of ISO 31000?
The core principles under ISO 31000 include:

- promoting inclusivity
- being dynamic
- finding the best available information
- identifying human factors
- integrating across all organizational activities; and
- customizing the process based on the ISO 31000 standard, the organization’s goals, and its industry.

How Does ISO 31000 Help in Risk Management?
ISO 31000 establishes a solid foundation upon which organizations can build their risk management strategy. Through ISO 31000, organizations can manage and identify certain risks that employees face, improving productivity and overall safety.

What is the ISO 31000 definition of risk?
ISO 31000 defines risk as to the effect of uncertainty on objectives. It means that every process has an element of risk that needs to be managed and every result is uncertain. It is defined in goal-oriented terms that provide a conceptual definition of risk.
Implementing and monitoring ISO 31000 within an organization can be difficult. This is why tools such as iAuditor by SafetyCulture are a huge help to various organizations.

iAuditor is a comprehensive tool with tons of features to help implement ISO 31000’s Risk Management Process and improve overall productivity.

Some of the core iAuditor features that aid with the ISO 31000 Risk Management Process includes:

- **Create smart ISO 31000 checklists** to use during inspections that cover all risk bases
- **Generate professional and comprehensive reports** right away, saving a lot of time when going through the ISO 31000 process
- **Allow employees to report any hazards or safety issues** right away for faster corrective action
- **Facilitate workplace communications** during risk assessments to ensure that everyone understands the task at hand and what they need to be doing

Find out how to transform your workplace with iAuditor. Book a demo