

We live in an ever-changing world where we are forced to deal with uncertainty every day. But how an organization tackles that uncertainty can be a key predictor of its success.



Risk is a necessary part of doing business, and in a world where enormous amounts of data are being processed at increasingly rapid rates, identifying and mitigating risks is a challenge for any company. It is no wonder then that many contracts and insurance agreements require solid evidence of good risk management practice.

ISO 31000 provides direction on how companies can integrate risk-based decision making into an organization's governance, planning, management, reporting, policies, values and culture. It is an open, principles-based system, meaning it enables organizations to apply the principles in the standard to the organizational context.

Who is **ISO 31000** for?

ISO 31000 is applicable to all organizations, regardless of type, size, activities and location, and covers all types of risk. It was developed by a range of stakeholders and is intended for use by anyone who manages risks, not just professional risk managers.

What are the **benefits** for my business?

ISO 31000 helps organizations develop a risk management strategy to effectively identify and mitigate risks, thereby enhancing the likelihood of achieving their objectives and increasing the protection of their assets. Its overarching goal is to develop a risk management culture where employees and stakeholders are aware of the importance of monitoring and managing risk. Implementing ISO 31000 also helps organizations see both the positive opportunities and negative consequences associated with risk, and allows for more informed, and thus more effective, decision making, namely in the allocation of resources. What's more, it can be an active component in improving an organization's governance and, ultimately, its performance.



Why was it **revised**?

All ISO standards are reviewed every five years and then revised if needed. This helps ensure they remain relevant, useful tools for the marketplace. A revised version of ISO 31000 was published in 2018 to take into account the evolution of the market and new challenges faced by business and organizations since the standard was first released in 2009. One example of this is the increased complexity of economic systems and emerging risk factors such as digital currency, both of which can present new and different types of risks to an organization on an international scale.

What are the **main differences**?

ISO 31000:2018 provides more strategic guidance than ISO 31000:2009 and places more emphasis on both the involvement of senior management and the integration of risk management into the organization. This includes the recommendation to develop a statement or policy that confirms a commitment to risk management, assigning authority, responsibility and accountability at the appropriate levels within the organization and ensuring that the necessary resources are allocated to managing risk.

The revised standard now also recommends that risk management be part of the organization's structure, processes, objectives, strategy and activities. It places a greater focus on creating value as the key driver of risk management and features other related principles such as continual improvement, the inclusion

of stakeholders, being customized to the organization and consideration of human and cultural factors.

The content has been streamlined to reflect an open systems model that regularly exchanges feedback with its external environment in order to fit a wider range of needs and contexts. The key objective is to make things clearer and easier, using plain language to define the fundamentals of risk management in a way that the reader will find easier to comprehend. The terminology is now more concise, with certain terms being moved to ISO Guide 73, Risk management – *Vocabulary*, which deals specifically with risk management terminology and is intended to be used alongside ISO 31000. Work has commenced on a terminology standard and implementation handbook to further enhance the understanding and applicability of the standard.

2 – ISO 31000, *Risk management*



Who was ISO 31000 developed by?

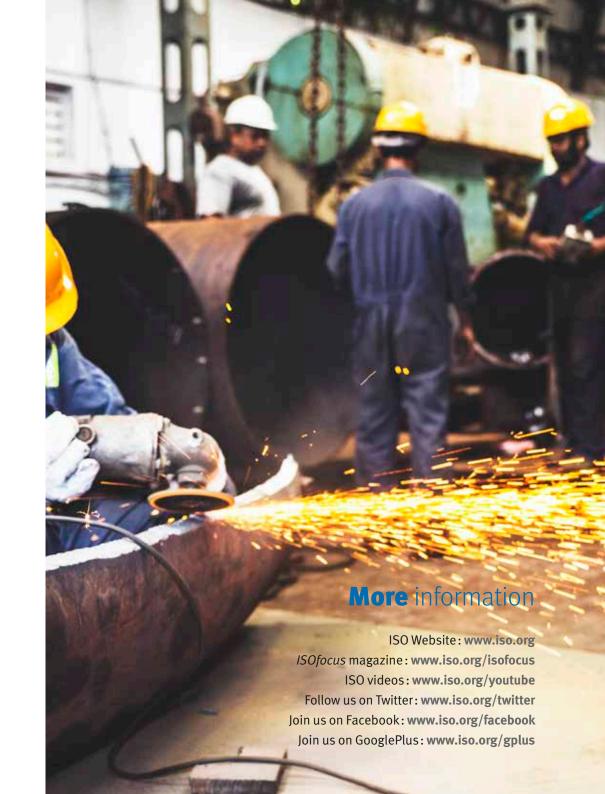
ISO 31000 was developed by
ISO's technical committee on risk
management, ISO/TC 262. Other
standards in its portfolio, which supports
ISO 31000, include technical report
ISO/TR 31004, Risk management —
Guidance for the implementation of
ISO 31000, and International Standard
ISO/IEC 31010, Risk management
— Risk assessment techniques,
developed jointly with the International
Electrotechnical Commission.

What about **certification**?

ISO 31000 provides guidelines, not requirements, and is therefore not intended for certification purposes.

How do | get started?

- Be aware of your organization's key objectives this will help you clarify the targets and requirements of your risk management system.
- Assess your current governance structure – this will ensure you allocate the right roles, responsibilities and reporting procedures when it comes to risk.
- Define your level of commitment what resources will you be able to allocate to implementing or maintaining a risk management system.



About ISO

ISO (International Organization for Standardization) is an independent, non-governmental organization with a membership of 162* national standards bodies. Through its members, ISO brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant International Standards that support innovation and provide solutions to global challenges.

ISO has published more than 22000* International Standards and related documents covering almost every industry, from technology to food safety, to agriculture and healthcare. For more information, please visit: www.iso.org.

* February 2018

International Organization for Standardization

ISO Central Secretariat
Ch. de Blandonnet 8
Case Postale 401
CH – 1214 Vernier, Geneva
Switzerland

iso.org

© ISO, 2018 All rights reserved ISBN 978-92-67-10784-4

