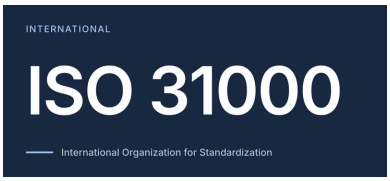
SmartSuite

Framework / Risk Management / Other

ISO 31000:2018

ISO 31000:2018 gives guidelines on managing risk through eight principles, a framework and a process for any organization. It is not certifiable. ISO published it on February 14, 2018.



What it is

ISO 31000:2018, Risk management — Guidelines, is the international standard that provides guidelines on managing the risk faced by organizations, through eight principles, a framework and a process that apply to any type of risk and any organization. The International Organization for Standardization (ISO) published the second edition on February 14, 2018 through technical committee ISO/TC 262, Risk management. It replaces ISO 31000:2009, and it is guidance, not a certifiable specification.

The document defines risk as the effect of uncertainty on objectives (Clause 3.1) and states that the purpose of risk management is the creation and protection of value (Clause 4). Its guidelines can be customized to any organization and its context, are not industry or sector specific, and can be applied to any activity, including decision-making at all levels (Clause 1). Top management is accountable for managing risk, and oversight bodies are accountable for overseeing it (Clause 5.2).

At a glance

PUBLISHER International Organization for Standardization (ISO), ISO/TC 262	TYPE Standard	VERSION ISO 31000:2018 (second edition)
EFFECTIVE February 14, 2018 (publication date)	DOMAIN Risk Management	FAMILY Other
REGION International	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: iso.org/standard/65694.html

Why it matters

- **Value creation and protection** Clause 4 states that the purpose of risk management is the creation and protection of value, and that it improves performance, encourages innovation and supports the achievement of objectives.
- **Accountability at the top** Top management is accountable for managing risk and oversight bodies are accountable for overseeing risk management, with authority, responsibility and accountability assigned at appropriate levels (Clause 5.2).
- **One approach for any type of risk** The guidelines provide a common approach to managing any type of risk and are not industry or sector specific (Clause 1).
- **Fitted to the organization** The framework and process are customized and proportionate to the organization's external and internal context and objectives (Clause 4, principle c, and Clause 5.4.1).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 31000:2018

Risk Register and Criteria

Record risks with their sources, events, consequences, likelihood and the risk criteria used to rate them (Clauses 3 and 6.3.4).

Assessment Records

Keep risk identification, analysis and evaluation results with owners and review dates (Clauses 6.4.2 to 6.4.4).

Treatment Plans

Track the selected treatment options, plans, owners, due dates and residual risk decisions (Clauses 6.5.2 and 6.5.3).

Key Risk Indicators and Review

Define indicators, thresholds and review cycles for monitoring and review (Clause 6.6).

Roles and Accountability

Assign risk owners and record the responsibilities and accountabilities of top management and oversight bodies (Clauses 5.2 and 5.4.3).

Recording and Reporting

Report risk exposure, treatment progress and open actions to top management and oversight bodies from the same records (Clause 6.7).

Common framework mappings

COSO ERM 2017 | ISO 22301 | ISO 31010:2009 | ISO 27001:2022 | NIST 800-37 Rev.2

Official resources

ISO 31000:2018 Standard

Defines guidelines for effective risk management within organizations of any size.

iso.org/standard/65694.html

ISO 31000 Implementation Guide

Provides detailed instructions for implementing ISO 31000 risk management principles.

iso.org/iso-31000-risk-management.html

ISO Risk Management Principles

Outlines core principles of risk management in ISO 31000 framework.

iso.org/iso-31000-principles.html

Frequently asked questions

Can an organization be certified to ISO 31000?

No. ISO states that ISO 31000 cannot be used for certification; it is guidance, not a specification to certify against. Organizations use it to build a risk management framework and process, and to compare their practice with an internationally recognized benchmark. It does provide guidance for internal or external audit programs.

What are the eight principles of ISO 31000:2018?

Clause 4 lists them: integrated; structured and comprehensive; customized; inclusive; dynamic; best available information; human and cultural factors; and continual improvement. They state the purpose of risk management, which is the creation and protection of value, and the characteristics of effective risk management.

What is the difference between the framework and the process in ISO 31000?

The framework (Clause 5) is how the organization integrates risk management into governance and activities: leadership and commitment, integration, design, implementation, evaluation and improvement. The process (Clause 6) is the repeatable cycle applied to risks: communication and consultation; scope, context and criteria; assessment; treatment; monitoring and review; and recording and reporting.

What does ISO 31000 expect from top management and oversight bodies?

Clause 5.2 says top management and oversight bodies should customize and implement the framework, issue a risk management statement or policy, allocate resources and assign authority, responsibility and accountability. Top management is accountable for managing risk, and oversight bodies are accountable for overseeing risk management.

 © 2026 SmartSuite Inc. All rights reserved.

Is ISO 31000:2018 still the current edition?

Yes. ISO published the second edition on February 14, 2018, and it replaced ISO 31000:2009. ISO's catalog lists the standard as to be revised after a systematic review closed on October 11, 2024, and shows ISO/CD 31000 under development. Until ISO publishes a new edition, the 2018 text applies.

License included / downloadable: No ISO 31000:2018 is a copyrighted ISO standard sold by ISO and by national standards bodies; its text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-31000-risk-management-guidelines-2018