SmartSuite

Framework / Risk Management / ISO Management Systems

ISO 31000:2018

ISO 31000 provides guidelines for identifying, assessing, and managing organizational risks to improve resilience and decision-making.

What it is

ISO 31000 is an international risk management guideline that provides a systematic approach for organizations to identify, assess, and manage a wide range of risks, including cybersecurity, operational, and compliance risks. Its purpose is to enhance organizational resilience and informed decision-making in the face of uncertainty.

Published by the International Organization for Standardization (ISO), ISO 31000 is applicable to organizations of all sizes and industries. The framework covers principles and processes for risk identification, risk assessment, risk treatment, monitoring, and continuous improvement, and is frequently referenced alongside standards such as ISO 27001 and NIST RMF for integrated risk management.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2018
EFFECTIVE 13 February 2018	DOMAIN Risk Management	FAMILY ISO Management Systems
REGION International	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY Moderate

Source: https://www.iso.org/iso-31000-risk-management.html

Why it matters

- **Strengthen risk oversight** Enable clear accountability and ongoing monitoring for risk management practices throughout the organization.
- **Enhance compliance support** Align internal risk controls with regulatory requirements to support legal obligations and industry standards.
- **Promote operational resilience** Improve the ability to anticipate, withstand, and recover from disruptive incidents or emerging threats.
- **Support informed decision-making** Provide a structured process for evaluating risks, supporting leaders in making data-driven and strategic business decisions.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 31000:2018

Enterprise Risk Register
Centralize risks, scoring, owners, and treatments with consistent methodology.

Risk Assessments and Reviews
Run recurring risk reviews and maintain evidence of decisions and updates.

Treatment Plans and Accountability
Track mitigation actions, due dates, approvals, and residual risk acceptance.

KRIs and Threshold Monitoring
Define indicators, thresholds, and reporting to spot changing risk early.

Issues, Findings, and Risk Linkage
Connect issues, findings, and corrective actions to the risks they impact.

Executive Reporting
Provide leadership-ready dashboards across risk exposure, trends, and actions.

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

What is ISO 31000 used for?
ISO 31000 is used to establish a systematic process for identifying, assessing, and managing all types of risks within an organization. It guides organizations in developing a risk management culture that promotes proactive mitigation and informed decision-making.

Is ISO 31000 mandatory or certifiable?
ISO 31000 is a voluntary guideline and is not certifiable by external auditors. Organizations can adopt its principles to improve risk management processes, but there is no formal certification for compliance with ISO 31000.

Who can apply ISO 31000 and to what scope?
ISO 31000 is applicable to organizations of all sizes, sectors, and industries. It can be tailored to address enterprise-wide risk, specific business units, or individual projects, enabling flexibility in defining the scope according to organizational needs.

What are the key concepts in ISO 31000?
Key concepts include risk identification, risk assessment (risk analysis and evaluation), risk treatment, and ongoing monitoring and review. The standard emphasizes establishing a risk management framework, defining risk appetite and criteria, and continuous communication and consultation.

How does risk management work under ISO 31000?
Risk management under ISO 31000 is a lifecycle process involving setting the organizational context, identifying risks, analyzing and evaluating those risks, selecting appropriate risk treatments, and monitoring outcomes. This lifecycle supports ongoing improvement and alignment with organizational objectives.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does ISO 31000 relate to other frameworks such as ISO 27001 or NIST RMF?

ISO 31000 provides overarching risk management principles that can complement more specialized frameworks like ISO 27001 (for information security) and NIST RMF. It is often integrated with other standards to achieve comprehensive governance, risk, and compliance (GRC) programs.

What are the ongoing compliance requirements for ISO 31000?

While ISO 31000 does not require formal certification, organizations should conduct regular risk assessments, maintain clear documentation, monitor and review risk controls, and update risk management processes based on lessons learned and changing risks.

How would SmartSuite support ISO 31000?

SmartSuite enables organizations to operationalize ISO 31000 by using risk registers to document, track, and prioritize risks, and by offering control libraries to align and manage risk treatments. Evidence collection modules ensure records for audit readiness, while compliance tracking and automated workflows support effective monitoring, reporting, and ongoing risk management activities.

License included / downloadable: No ISO 31000 requires purchase through the ISO standards catalog. License not included with platform

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