

ISO 31010:2009

ISO 31010:2009 provides guidance on selecting and applying risk assessment techniques to identify, evaluate, and manage organizational risks.



What it is

ISO 31010:2009 is an international standard that provides a comprehensive set of risk assessment techniques to support organizations in identifying, evaluating, and managing risks. This standard offers structured guidance for selecting and applying methodologies that help organizations strengthen decision-making and enhance risk management processes across various business functions.

Published by the International Organization for Standardization (ISO), ISO 31010:2009 is used by risk managers, compliance professionals, and internal auditors across industries and sectors. The standard covers a wide range of techniques relevant to risk management, including qualitative, quantitative, and hybrid methods, and aligns with broader risk frameworks such as ISO 31000.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2009
EFFECTIVE 2009	DOMAIN Risk Management	FAMILY ISO Management Systems
REGION International	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.iso.org/search.html?q=31010>

Why it matters

- **Strengthen decision-making confidence** Enable informed, risk-aware decisions by providing structured methodologies for identifying and evaluating potential threats and opportunities.
- **Enhance regulatory alignment** Support compliance efforts by aligning risk assessment processes with recognized international standards and regulatory expectations across industries.
- **Improve risk oversight and management** Establish consistent processes for risk identification and assessment, helping management prioritize and address critical business risks more effectively.
- **Increase audit readiness** Facilitate more efficient internal and external audits with documented, standardized risk assessments that demonstrate a proactive control environment.

How SmartSuite supports ISO 31010:2009

Control Catalog and Implementation Guidance Organize ISO 27002 control domains with defined owners, procedures, and implementation documentation.	Risk and Asset Linkage Connect security controls to risks, assets, and mitigation strategies to prioritize security investments.	Evidence Collection and Review Cadence Capture evidence demonstrating control operation and schedule recurring reviews across security processes.
Exception and Compensating Control Tracking Document control exceptions, approvals, and compensating safeguards with full traceability.	Cross-Framework Control Mapping Map ISO 27002 controls to frameworks such as NIST, CIS Controls, and SOC reporting requirements.	Security Governance and Reporting Generate dashboards showing control coverage, open issues, remediation progress, and overall security posture.

Common framework mappings

- COBIT 2019
- COSO ERM 2017
- ISO 31000:2018
- ISO 27001:2022
- NIST CSF 2.0
- NIST 800-53 Rev.5

Official resources

ISO 31010:2009 Standard Official ISO document providing risk assessment techniques for effective risk management. iso.org/standard/51073.html	ISO Risk Management Framework Overview Describes the relation of ISO 31010 within the broader risk management standards. iso.org/iso-31000-risk-management.html
--	---

Frequently asked questions

- What is ISO 31010:2009 used for?**
ISO 31010:2009 provides organizations with a structured set of risk assessment techniques to systematically identify, analyze, and evaluate risks. It supports decision-making by offering practical methodologies to improve risk visibility and strengthen risk management processes across business functions.
- Is ISO 31010:2009 a mandatory or certifiable standard?**
ISO 31010:2009 is a guidance standard and is not certifiable, nor is it typically mandated by regulators. Organizations use ISO 31010 to complement broader risk management frameworks, such as ISO 31000, but there is no formal certification process.
- Who can apply ISO 31010:2009, and in what contexts is it relevant?**
ISO 31010:2009 can be applied by any organization, regardless of size or industry, that seeks to improve its risk assessment capabilities. It is relevant for risk managers, internal auditors, compliance teams, and business leaders looking to systematically manage operational, strategic, or regulatory risks.
- What are the key concepts or artifacts in ISO 31010:2009?**
Key concepts in ISO 31010:2009 include the selection and application of appropriate risk assessment techniques. Artifacts include documented risk assessments, risk registers, evaluation criteria, and assessment results that are integrated into broader risk management and governance programs.
- How is a risk assessment performed using ISO 31010:2009?**
A risk assessment under ISO 31010:2009 involves establishing the context, identifying threats, analyzing the likelihood and impact, and evaluating risks against set criteria. Techniques such as Failure Mode and Effects Analysis (FMEA), Hazard and Operability Study (HAZOP), fault tree analysis, and bow-tie diagrams are selected based on the organization's needs.

How does ISO 31010:2009 relate to other risk management frameworks?

ISO 31010:2009 serves as a companion standard to ISO 31000, providing detailed guidance on risk assessment techniques referenced in ISO 31000's risk management process. It can also integrate with industry-specific frameworks by enhancing the rigor and traceability of risk assessments.

What are the ongoing compliance requirements for ISO 31010:2009?

Ongoing compliance involves regularly reviewing and updating risk assessments, maintaining evidence of assessment activities, and ensuring alignment with changing organizational risks and regulatory requirements. Risk management teams must document procedures and ensure that selected techniques remain fit for purpose.

How would SmartSuite support ISO 31010:2009?

SmartSuite facilitates ISO 31010:2009 implementation by providing libraries of risk assessment techniques, scheduling and tracking assessments, and linking results to risk registers and control libraries. The platform streamlines evidence collection, supports remediation workflows, enables audit-ready reporting, and ensures traceability between assessments, governance actions, and risk management practices.

License included / downloadable: No ISO 31010:2009 requires purchase through the ISO catalogue or national standards bodies. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/iso-31010-2009-risk-assessment-techniques