

ISO/IEC 27005:2022

Information security, cybersecurity and privacy protection — Guidance on managing



What it is

ISO/IEC 27005:2022 provides guidance on managing information security risks. It describes how to establish the context, identify, analyze, evaluate, and treat risks to information, and how to monitor, review, record, and communicate the results, in support of an information security management system (ISMS) built on ISO/IEC 27001. It is a guidance standard, not a set of certifiable requirements.

The standard is published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and developed by ISO/IEC JTC 1/SC 27, the subcommittee responsible for the ISO/IEC 27000 family. The fourth edition was published in October 2022, replacing ISO/IEC 27005:2018, and is aligned with the risk clauses of ISO/IEC 27001:2022 and the risk management principles of ISO 31000:2018. It applies to organizations of all types and sizes that manage information security risks, whether or not they pursue ISO/IEC 27001 certification.

At a glance

PUBLISHER International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC JTC 1/SC 27	TYPE Guidance	VERSION 2022 (Edition 4)
EFFECTIVE October 2022	DOMAIN Risk Management	FAMILY ISO 27000 Series
REGION International	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: <https://www.iso.org/standard/80585.html>

Why it matters

- **Direct support for ISO/IEC 27001** The guidance maps to the risk assessment and treatment requirements that auditors test during ISMS certification.
- **Better threat identification** Event-based and asset-based approaches help organizations find risks they would otherwise miss.
- **Prioritized security investment** Risk analysis and evaluation against defined criteria show which risks justify treatment first.
- **Informed, defensible decisions** Recorded risk criteria, results, and acceptance decisions give management and auditors a clear rationale.

How SmartSuite supports ISO 27005:2022

Information Security Risk Register

Record risks with sources, events, assets, owners, and scores using the likelihood and consequence scales you define.

Risk Owners and Reassessment
Cadence

Assign owners and schedule periodic and change-triggered reassessments with reminders and escalation.

Risk Decisions and Audit Trail

Capture evaluation results, treatment choices, and residual risk approvals with timestamps and approvers.

Treatment Plans and Control Testing

Link treatments to ISO/IEC 27002 controls, track implementation, and test that controls operate as intended.

ISMS and Vendor Risk Alignment

Connect risks to ISO/IEC 27001 clauses, the Statement of Applicability, and third-party assessments.

Risk Reporting

Report risk levels, treatment progress, and acceptance status to management and certification auditors.

Common framework mappings

ISO 27001:2022

ISO 27002:2022

ISO 27000

ISO 31000:2018

ISO 31010:2009

NIST SP 800-39

NIST 800-37 Rev.2

NIST CSF 2.0

NIST 800-53 Rev.5

ISO 27017

ISO 27018

ISO 27701

COSO ERM 2017

CIS Controls v8.1

Official resources

ISO/IEC 27005:2022 Guidance on managing information security risks

ISO's catalog page for the fourth edition, with status, edition history, committee, and purchase options.

iso.org/standard/80585.html

ISO/IEC 27001:2022 Information security management systems

ISO's catalog page for the ISMS requirements standard that ISO/IEC 27005 supports.

iso.org/standard/27001

ISO/IEC 27000 family — Information security management

ISO's overview of the ISO/IEC 27000 family of standards and the committee that develops them.

iso.org/standard/iso-iec-27000-family

ISO 31000:2018 Risk management — Guidelines

ISO's catalog page for the general risk management standard whose process ISO/IEC 27005 follows.

iso.org/standard/65694.html

Frequently asked questions

What is ISO/IEC 27005:2022 used for?

ISO/IEC 27005:2022 is used to design and run the information security risk management process that supports an information security management system (ISMS). It guides organizations through establishing context and risk criteria, identifying, analyzing, and evaluating risks, treating them, and monitoring and recording the results.

Is ISO/IEC 27005 certifiable?

No. ISO/IEC 27005 is a guidance standard and organizations are not certified against it. Certification applies to ISO/IEC 27001; ISO/IEC 27005 helps organizations meet the risk assessment and treatment requirements that ISO/IEC 27001 auditors examine.

How does ISO/IEC 27005 relate to ISO/IEC 27001 and ISO/IEC 27002?

ISO/IEC 27001 requires an organization to define and perform information security risk assessment and treatment; ISO/IEC 27005 explains how to do it. Treatment plans typically select controls from ISO/IEC 27002, and the resulting decisions feed the Statement of Applicability that ISO/IEC 27001 requires.

How does ISO/IEC 27005 relate to ISO 31000?

ISO/IEC 27005 follows the principles, framework, and process of ISO 31000, the general risk management standard, and applies them to information security. That alignment lets information security risk be reported in the same terms as other enterprise risks.

What changed in the 2022 edition of ISO/IEC 27005?

The fourth edition, published in October 2022, replaced ISO/IEC 27005:2018. It aligned terminology with ISO/IEC 27001:2022 and ISO 31000:2018, organized the process into context, assessment, treatment, and operation clauses, and expanded guidance on event-based and asset-based risk identification.

What does an ISO/IEC 27005 risk assessment produce?

It produces documented risk criteria, a register of identified risks with owners and levels, an evaluation of which risks need treatment, a risk treatment plan with selected controls, and approval of residual risk by the risk owners. These records serve as evidence for ISO/IEC 27001 audits.

How does SmartSuite support ISO/IEC 27005?

SmartSuite holds the risk register, rating scales, treatment plans, and control links in one system, with owners, reassessment schedules, approvals, and a full audit trail. Teams use it to keep risk information current and to report risk status to management and auditors.

License included / downloadable: No ISO/IEC 27005:2022 is sold by ISO and national standards bodies and is not included with the platform; a read-only sample is available on ISO's Online Browsing Platform.

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27005-2022-information-security-risk-management