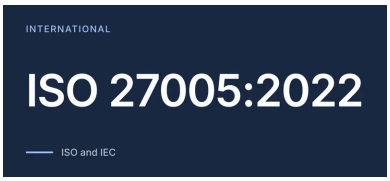
SmartSuite

Framework / Risk Management / ISO 27000 Series

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

ISO/IEC 27005:2022 provides guidance on identifying, analyzing, evaluating, and treating information security risks ...



What it is

ISO/IEC 27005:2022 is the international guidance standard for managing information security risks, giving organizations a process for the risk assessment and risk treatment that ISO/IEC 27001 requires. ISO and IEC published this fourth edition on October 25, 2022; it was prepared by ISO/IEC JTC 1/SC 27, cancels and replaces ISO/IEC 27005:2018, and is not a certifiable standard. Its Clause 1 says it applies to all organizations regardless of type, size or sector.

At a glance

PUBLISHER
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC JTC 1/SC 27

TYPE
Guidance

VERSION
Fourth edition (ISO/IEC 27005:2022; replaces ISO/IEC 27005:2018)

EFFECTIVE
October 25, 2022

DOMAIN
Risk Management

FAMILY
ISO 27000 Series

REGION
International

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
Medium

Source: iso.org/standard/80585.html

Why it matters

- **Follows the ISO/IEC 27001 steps** Clauses 7 and 8 follow Clauses 6.1.2 and 6.1.3 of ISO/IEC 27001:2022 step by step, including the comparison with Annex A (8.4) and the Statement of Applicability (8.5).
- **Risk scenarios and two ways to identify risks** The 2022 edition introduced risk scenario concepts and contrasts the event-based approach with the asset-based approach to risk identification (Foreword and Clause 7.2).
- **Prioritized security investment** Analysis and evaluation against defined criteria (7.3 and 7.4) show which risks to treat first (7.4.2).
- **Informed, defensible decisions** Documented information about processes and results (10.4) and risk owners' approval and acceptance of residual risk (8.6) give management and auditors a clear rationale.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 27005:2022

Information Security Risk Register

Use Cyber & IT Risk to record risks with sources, events, assets, risk owners and levels using the consequence and likelihood scales you define (Clauses 6.4 and 7).

Risk Criteria and Owners

Keep the risk acceptance criteria and assessment criteria with owners, and schedule reassessments with reminders (Clauses 6.4.2, 6.4.3 and 7.2.2).

Evaluation and Residual Risk

Record the evaluation results, the treatment choices and the risk owners' acceptance of residual risk with timestamps and approvers (Clauses 7.4 and 8.6.3).

Treatment Plans and Control Testing

Link each treatment to the controls determined, track implementation, and test that the controls operate as intended (Clauses 8.3 and 8.6.1).

Statement of Applicability

Hold the comparison with ISO/IEC 27001:2022 Annex A and the Statement of Applicability in Compliance Management (Clauses 8.4 and 8.5).

Risk Reporting

Report risk levels, treatment progress and acceptance status to management and to certification auditors (Clauses 10.4 to 10.6).

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 · NIST SP 800-30 Rev. 1 · Open FAIR

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?

It gives guidance on managing information security risks, specifically risk assessment and risk treatment, to help organizations fulfill the requirements of ISO/IEC 27001 for actions that address risks (Clause 1). Clause 5 sets out the process, Clauses 6 to 8 the context, assessment and treatment, and Clauses 9 and 10 operation and related ISMS processes.

Is ISO/IEC 27005 certifiable?

No. It is a guidance document, not a set of certifiable requirements. Certification applies to the ISMS under ISO/IEC 27001, whose risk assessment and treatment requirements are in Clauses 6.1.2, 6.1.3, 8.2 and 8.3; ISO/IEC 27005 explains how to meet them.

Updated Oct 29, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How do the clauses of ISO/IEC 27005:2022 relate to ISO/IEC 27001:2022?

The 2022 edition adjusted its structure to the layout of ISO/IEC 27001:2022. Clauses 7.2 to 7.4 follow the identification, analysis and evaluation steps of 27001 Clause 6.1.2, and Clauses 8.2 to 8.6 follow the treatment steps of 6.1.3: options, necessary controls, comparison with Annex A, the Statement of Applicability, the treatment plan, and approval and acceptance of residual risk by risk owners.

What is the difference between the event-based and the asset-based approach?

The 2022 edition contrasts the two approaches to risk identification (Foreword). The event-based approach starts from events and the risk sources behind them, and the asset-based approach starts from assets and their threats and vulnerabilities; the guidance is in Clause 7.2, and the 2022 edition also introduced the risk scenario concept, defined in 3.1.4 as a sequence or combination of events leading from the initial cause to the unwanted consequence.

What changed from the 2018 edition?

The Foreword lists six main changes: all guidance aligned with ISO/IEC 27001:2022 and ISO 31000:2018, terminology aligned with ISO 31000:2018, the clause structure adjusted to the layout of ISO/IEC 27001:2022, risk scenario concepts introduced, the event-based approach contrasted with the asset-based approach, and the annexes revised and restructured into a single Annex A.

License included / downloadable: No ISO/IEC 27005:2022 is a paid standard sold by ISO and national standards bodies, and the text is not included with the platform.

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