

ISO/IEC 27005



Search Search this site

information security risks (fourth edition)

< Previous standard

ISO/IEC 27005:2022 🌃 — Information security,

^ Up a level ^

cybersecurity and privacy protection — Guidance on managing

Next standard >

Abstract

"[ISO/IEC 27005] provides guidance to assist organizations to: fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks; [and] perform information security risk management activities, specifically information security risk assessment and treatment ..."

[Source: ISO/IEC 27005:2022]

Summary podcast



Introduction

The ISO27k standards are overtly risk-aligned, meaning that organisations are supposed to identify and assess risks to their information (called "information security risks" in the ISO27k standards, despite that term being undefined) as a prelude to dealing with ("treating") them in various ways.

Dealing with the most significant information risks as priorities makes sense from the practical implementation and management perspectives. Turning that on its head, failing to prioritise addressing the most significant risks represents a governance failure, arguably negligence or mismanagement.

Scope of the standard

The standard guides organisations interpreting and fulfilling ISO/IEC 27001:2022's requirements to address (identify, evaluate and treat) their information [security] risks. It can also be used independently of ISO/IEC 27001: it is a valuable approach to managing information risks regardless of the framework.

Content of the standard

This is a substantial, weighty standard offering ~70 pages of copious, detailed advice on:

- 5. Information security risk management describes the iterative (ongoing, 'whack-a-mole') process of identifying, assessing and treating information [security] risks, comprising both strategic/long-term and operational/medium-short-term cycles.
- 6. Context establishment despite the heading, clause 6 largely concerns methods for determining risk criteria. The organisation's business context for information risk and security management is covered in clause 10.
- 7. Information security risk assessment process another lengthy clause lays out the process of systematically identifying, analysing, evaluating and prioritising information [security] risks.
- 8. Information security risk treatment process described largely in terms of using information security

1 of 3 8/28/25, 21:26



- controls to 'modify' (mitigate or maintain) information [security] risks, barely mentioning the other risk treatment options (avoidance, sharing and acceptance).
- 9. **Operation** a short clause mentions that information [security] risks and treatments should be reviewed regularly or when changes occur.
- Leveraging related ISMS processes this is basically a re-hash and amplification of ISO/IEC 27001, offering implementation advice in a similar style to <u>ISO/IEC 27003</u>.

Annex - additional information on risk criteria and practical advice such as examples of threats and vulnerabilities.

Status of the standard

The first (2008), second (2011) and third (2018) editions are ancient history.

The current fourth edition was published in 2022.

Further reading

Read more about selecting suitable information risk analysis methods and management tools in the <u>ISO27k FAQ</u>.

<u>ISO 31000</u> Risk management - Guidelines is a popular and well-respected standard, describing a systematic risk management approach suitable for many types of risk. You may also appreciate <u>ISO/TR 31004</u> Risk management - Guidance for the implementation of ISO 31000 and <u>ISO/IEC 31010</u> Risk management - Risk assessment techniques.

NIST's Risk Management Framework is another valuable resource ... and it's FREE.

Personal comments

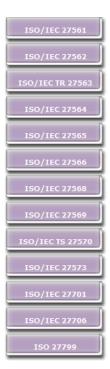
Given that the entire ISO27k approach is risk-aligned, identifying, evaluating and treating **information risks** is fundamental.

With the fourth edition, '27005 tackles the thorny issue of how to use <u>ISO/IEC 27001</u> Annex A. The annex is described as an incomplete set of *possible* controls to be checked for relevance to mitigate the organisation's identified information [security] risks - in other words, a controls-based approach to information risk management, supplementing the scenario-, event- and asset-based approaches mentioned elsewhere. Adopting all four approaches may be costly but there are advantages in exploring information risks from various perspectives.

ISO's <u>Technical Committee for Risk Management</u> looks likely to review/clarify the somewhat unhelpful definition of 'risk' in <u>ISO 31000:2018</u> ("effect of uncertainty on objectives"), and may also offer guidance on 'opportunities'. It is possible the two terms will be distinguished, rather than being portrayed as flip sides as at present. I *hope* that will eventually make things easier for ISO27k and the other management systems standards, but it may stir the already muddy waters.

< <u>Previous standard</u> ^ <u>Up a level</u> ^ <u>Next standard</u> >

2 of 3 8/28/25, 21:26



Copyright © 2025 IsecT Ltd. Contact us re Intellectual Property Rights

3 of 3