ISO/IEC 27005

Search
Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | DONATE!

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27021
ISO/IEC TS 27022
ISO/IEC TR 27024
ISO/IEC TS 27028
ISO/IEC TR 27029
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035

< Previous standard ^ Up a level ^ Next standard >

Hot ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — **Guidance on managing information security risks** (*fourth edition*)

Abstract

Summary podcast

"[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]

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

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

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.
10. **Leveraging related ISMS processes** - this is basically a re-hash and amplification of ISO/IEC 27001, offering implementation advice in a similar style to ISO/IEC 27003.

    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 ISO27k FAQ.

ISO 31000 *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 ISO/TR 31004 *Risk management - Guidance for the implementation of ISO 31000* and ISO/IEC 31010 *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 ISO/IEC 27001 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 Technical Committee for Risk Management looks likely to review/clarify the somewhat unhelpful definition of 'risk' in ISO 31000:2018 ("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.

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799