SecAware Policies

ISO/IEC TS 27008

SecAware Awareness

Search

● Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | About us

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 27009
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC TR 27019
ISO/IEC 27021
ISO/IEC 27022
ISO/IEC TR 27023
ISO/IEC 27030
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034

ISO/IEC TS 27008:2019 — Information technology — Security techniques — **Guidelines for the assessment of information security controls** *(second edition)*

Introduction

This standard (actually a “technical report”) on “technical auditing” complements ISO/IEC 27007. It concentrates on auditing the information security controls - or rather the “technical controls” (as in IT security or cybersecurity controls), whereas ’27007 concentrates on auditing the management system elements of the ISMS.

Scope

This standard provides guidance for all auditors regarding “information security management systems controls” [*sic*] selected through a risk-based approach (*e.g.* as presented in a statement of applicability) for information security management. It supports the information risk management process and internal, external and third-party audits of an ISMS by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which required “ISMS controls” are implemented. Furthermore, it supports any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and as a strategic platform for information security governance.

Purpose and justification

The standard:

- Is applicable to all organizations, including public and private companies, government entities and not-for-profit organizations and organizations of all sizes regardless of the extent of their reliance on information;
- Supports planning and execution of ISMS audits and the information risk management process;
- Further adds value and enhances the quality and benefit of the ISO27k standards by closing the gap between reviewing the ISMS in theory and, when needed, verifying evidence of implemented ISMS controls (*e.g.* in the ISO27k user organizations, assessing security elements of business processes, IT systems and IT operating environments);
- Provides guidance for auditing information security controls based on the controls guidance in ISO/IEC 27002;
- Improves ISMS audits by optimizing the relationships between the ISMS processes and required controls (*e.g.* mechanisms to limit the harm caused by failures in the protection of information - erroneous financial statements, incorrect documents issued by an organization and intangibles such as reputation and image of the organization and privacy, skills and experience of people);
- Supports an ISMS-based assurance and information security governance approach and audit thereof [?? That would appear to stray into the area of management systems auditing rather than information security controls or technical auditing];
- Ensures effective and efficient use of audit resources.

ISO/IEC 27035
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 27099
ISO/IEC TS 27100
ISO/IEC TS 27101
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27558
ISO/IEC 27559
ISO/IEC 27560
ISO/IEC TS 27570
ISO/IEC 27701
ISO 27799
Other ISO27k

Whereas ISO/IEC 27007 focuses on auditing the *management system* elements of an ISMS as described in ISO/IEC 27001, ISO/IEC TR 27008 focuses on checking some of the *information security controls* themselves, such as (for example) those as described in ISO/IEC 27002 and outlined in Annex A of ISO/IEC 27001.

'27008 "focuses on reviews of information security controls, including checking of technical compliance, against an information security implementation standard, which is established by the organization. It does not intend to provide any specific guidance on compliance checking regarding measurement, risk assessment or audit of an ISMS as specified in ISO/IEC 27004, 27005 or 27007 respectively."

Technical compliance checking/auditing is explained as a process of examining 'technical' security controls, interviewing those associated with the controls (managers, technicians, users *etc.*), and testing the controls. The methods should be familiar to experienced IT auditors.

'Technical' controls, while not explicitly defined in the standard, appear to be what are commonly known as IT security or cybersecurity controls, in other words a *subset* of the information security controls described in ISO/IEC 27001 and especially 27002.

Status of the standard

The first edition was published in 2011 as ISO/IEC **TR** 27008:2011, a 'Type 2 Technical Report. Minor but numerous grammatical and technical errors in the standard, as well as its limited scope, may have hampered its adoption.

The second edition was **published in 2019** as ISO/IEC **TS** 27008:2019, a 'Technical Specification' reflecting the 2013 versions of ISO/IEC 27001 and 27002.

Personal comments

The title now refers to 'assessments' not 'audits', for some reason.

The 2019 version still includes the phrase "technical compliance checking of information system controls" without explaining what that means: it appears to imply that the new version remains myopically focused on 'technical controls' as noted above. Unless the organization understands and accepts the need to protect its valuable information against the huge variety of information risks, for business reasons, the ISMS and hence the specific technical security controls will remain largely irrelevant, and yet the standard does not address broader issues of that nature.

While this standard is *not* intended to be used by accredited ISMS certification bodies, some members of SC 27 are concerned about its potential impact on ISO/IEC 27001 certification audits. Certification against ISO/IEC 27001 requires certification auditors to assess the organization's ISMS as a whole for compliance with the standard, but not necessarily to delve into the information security controls themselves. They review the *management system* in much the same way that ISO 9000 auditors review an organization's *management system* for quality assurance. Some of us feel that this leaves an assurance gap: it is conceivable for an organization to implement an ISMS 'on paper' but to ignore significant elements of its security policies, standards, procedures and guidelines in practice, perhaps arbitrarily declaring a narrow ISMS scope and a minimalist Statement of Applicability, and declaring an *unreasonably* high risk tolerance simply to avoid making changes that any sane person would think appropriate. Others insist that certification auditors *do* normally substantiate the existence of information security controls as well as the management system controls, at least to some extent (how much being a moot point).

< Previous standard ^ Up a level ^ Next standard >