ISO/IEC TS 27008

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

Abstract

"[ISO/IEC 27008] provides guidance on reviewing and assessing the implementation and operation of information security controls, including the technical assessment of information system controls, in compliance with an organisation's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organisation. [ISO/IEC 27008] offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001. It is applicable to all types and sizes of organisations, including public and private companies, government entities, and not-for-profit organisations conducting information security reviews and technical compliance checks."

[Source: ISO/IEC TS 27008:2019]

Introduction

This standard (strictly speaking a **T**echnical **S**pecification) 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 ISO/IEC 27007 concentrates on auditing the management system elements of the ISMS.

Scope

This standard provides guidance for all auditors/assessors regarding "information security management systems

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" [*sic*] selected through a risk-based approach (*e.g.* as presented in a **S**tatement **o**f **A**pplicability) 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 the organisation's required "ISMS controls" are implemented. Furthermore, it supports any organisation using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and as a strategic platform for information security governance.

Purpose and justification

This standard gives auditors background knowledge on the information security controls being managed through an **I**nformation **S**ecurity **M**anagement **S**ystem.

The standard:

- Is applicable to organisations of all types and sizes;
- 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 organisations, 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 27002:2013;
- 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 organisation and intangibles such as reputation and image of the organisation and privacy, skills and experience of people);
- Supports an ISMS-based assurance and information security governance approach and audit thereof [?? That strays from the standard's scope into the area of management systems auditing];
- Supports effective and efficient use of audit resources.

Whereas ISO/IEC 27007 focuses on auditing the *management system* elements of an ISMS as described in ISO/IEC 27001, ISO/IEC TS 27008 focuses on checking some of the *information security controls* themselves, such as (for example) those as described in ISO/IEC 27002:2013 and outlined in Annex A of ISO/IEC 27001:2013.

ISO/IEC TS 27008 "focuses on reviews of information security controls, including checking of technical compliance, against an information security implementation standard, which is established by the organisation. 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, ISO/IEC 27005 or ISO/IEC 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 ISO/IEC 27002.

Furthermore, the correct term here is conformity, not compliance, since it is discretionary. But I digress.

Status of the standard

The *first* edition was published in **2011** as ISO/IEC **TR** 27008:2011, a Type 2 **T**echnical **R**eport. It set out to provide "Guidelines for auditors on information security controls".

The *second* edition was published in **2019** as ISO/IEC **TS** 27008:2019, a **T**echnical **S**pecification reflecting the 2013 versions of ISO/IEC 27001 and ISO/IEC 27002. The title morphed into "Guidelines for the assessment of information security controls", dropping the explicit reference to auditing.

The *third* edition is currently in preparation, to reflect ISO/IEC 27002:2022. It *may* revert to a **T**echnical **R**eport. The title will reflect the committee's new name "*Information security, cybersecurity and privacy protection - Guidelines for the assessment of information security controls*" and a new abstract is likely:

> *"This Technical Report provides guidance for assessing the implementation of ISMS controls determined through a risk-based approach for information security management. It supports the information security risk management process and assessment of ISMS controls by explaining the relationship between the ISMS and its supporting controls."*
>
> *[Source: SC 27 Standing Document 11 (July 2022)]*

The *third* edition is at **C**ommittee **D**raft stage. A second CD ballot is planned so it is unlikely to emerge until late

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

2025, perhaps 2026.

Personal comments

Thanks to the liberal use of “technical” in phrases such as “technical compliance checking of information system controls”, “technical assessment” and “technical security controls”, this standard is patently concerned with **technology**, implying **IT** or **cyber**security, specifically, rather than **information** risk and security in general.

While this standard is *not* intended to be used for certification, it remains inconsistent and ambiguous (frankly, unclear and confusing) in the use of key terms such as: review, assessment, test, validation, check and audit. For example, are “information security auditors” the same as “certification auditors”, “IT auditors”, “internal auditors”, “ISMS internal auditors”, “compliance auditors”, “conformity auditors”, or something else? There are no (zero) definitions in the second edition since all terms are supposedly defined in ISO/IEC 27000: concerning that little list of terms, only “audit”, “information security” and “conformity” are defined, separately. “Risk assessment” is specifically defined but not “assessment” in general. So, conventional dictionary definitions presumably apply ... but don’t really help. For an international standard, it could hardly be more muddled.

Coupled with the ambiguous wording in ISO/IEC 27001 concerning the **S**tatement **o**f **A**pplicability and purpose of Annex A, the commonplace but erroneous perception that the Annex A security controls are mandatory and hence auditable requirements persists - even among some certification auditors - despite the committee’s repeated efforts to correct this misunderstanding.

Certification against ISO/IEC 27001 requires certification auditors to audit the organisation’s ISMS for conformity with the standard. If ISO/IEC 27001 *certification* - as opposed to protecting and exploiting information - is an overriding management objective, an organisation may conceivably implement an ISMS ‘on paper’, perhaps arbitrarily defining a narrow ISMS scope with a minimalist **S**tatement **o**f **A**pplicability, and declaring an *unreasonably* high risk tolerance. In practice, therefore, certification auditors generally *do* substantiate the existence, operation and suitability of information security controls as well as the [implicit] management system, management and governance controls, at least to some extent, primarily in accordance with ISO/IEC 27001 clause 4.4 that formally requires the ISMS to be ‘established, implemented, maintained and continually improved’.

< Previous standard ^ Up a level ^ Next standard >