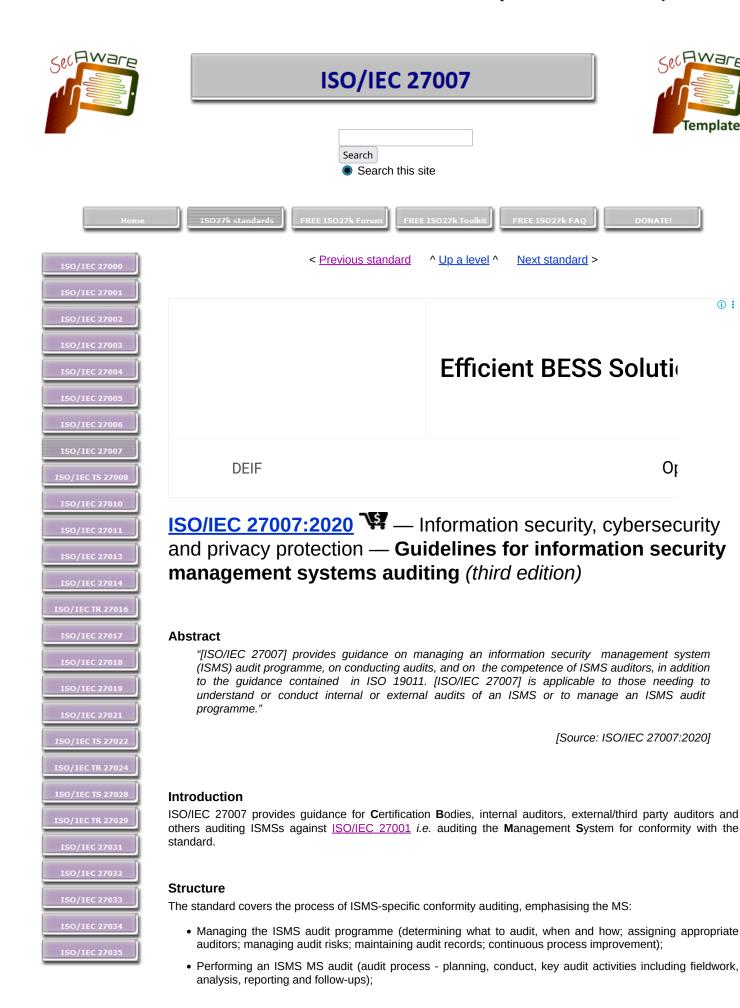
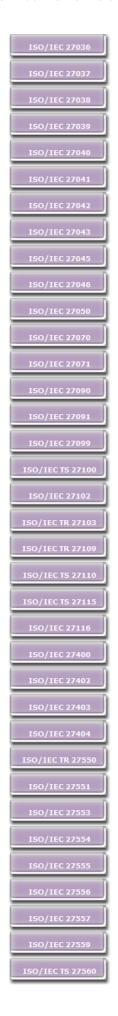
i

10



1 of 3 8/28/25, 21:27



• Managing ISMS auditors (competencies, skills, attributes, evaluation).

The main body of the standard mostly advises on the application of <u>ISO 19011</u> to the ISMS context, with a few not-terribly-helpful explanatory comments (e.g. audits are likely to involve sensitive proprietary or personal information, hence auditors may need to be security-cleared to the appropriate level before auditing, and secure audit evidence appropriately).

However the more valuable **annex** lays out in specific audit tests concerning the organisation's conformity with requirements in the main body of <u>ISO/IEC 27001</u>.

Other standards for ISMS auditing

ISO/IEC 27007 draws heavily on <u>ISO 19011</u>, the generic standard on auditing *management systems*, providing additional ISMS-specific guidance.

See also <u>ISO/IEC 27008</u> for advice on auditing *information security controls* and <u>ISO/IEC 27006-1</u> for the requirements of certification auditors.

Status of the standard

The first edition was published in 2011.

The second edition was published in 2017.

The third edition was published in 2020, having been updated to reflect ISO 19011:2018.

A fourth edition is being prepared, updating the third to reflect the 2022 release of ISO/IEC 27001 and the imminent 2025 release of ISO 19011.

The new version of '19011 will incorporate guidance on remote auditing, including remote auditing of virtual locations such as globally-distributed data centres providing cloud services, plus other editorial changes.

Publication of the fourth edition of '27007 is planned for 2027 - once again lagging two years behind the '19011 update. It is at first **W**orking **D**raft stage.

Personal comments

This standard primarily concerns **conformity/compliance auditing**, a particular form of auditing with a very specific goal: to determine whether the audited organisation's ISMS conforms with (*i.e.* fulfills all the mandatory management system requirements specified formally by) <u>ISO/IEC 27001</u>. Such audits are normally performed for certification purposes.

Other types of audits have different goals. *Please* don't make the mistake of assuming that all auditors are so-called "tick-and-bash" compliance/conformity auditors, or that all audits are compliance/conformity audits! Specifically in relation to information risk and security management, competent technology auditors might for instance:

- Evaluate the organisation's strategies and policies relating to information and privacy risk management, incident management, fraud *etc.* for aspects such as strategic fit, currency, relevance, readability, coverage, suitability and quality (fitness for purpose);
- Audit workers' conformity with organisational policies, procedures, directives, guidelines, employment contracts/agreements and so on, in the general area of information risk, information security and privacy;
- Delve into the root causes of ongoing issues and repetitive incidents, including near-misses and lesser events:
- Examine the governance arrangements in this area *e.g.* organisational structure, internal and external reporting relationships, information flows within and between management layers, accountabilities, roles and responsibilities ...;
- Audit the organisation's compliance/conformity with other relevant obligations and expectations, aside from ISO/IEC 27001 e.g. privacy and data protection laws, intellectual property protection, health and safety plus employment laws, fire codes and building standards, technical security standards, supplier, partner and customer agreements, industry guidelines, ethical codes ..., including the associated arrangements such as enforcement actions, and how the organisation ensures it remains up to date with changes;
- Audit the effectiveness and efficiency of the ISMS, including aspects such as the net value (benefits less
 costs) it generates for the business, and any unrealised potential;
- Examine 'assurance', 'integrity', 'confidentiality', 'availability', 'risk', 'information risk management', 'compliance', 'privacy' etc. in the broad, deliberately interpreting such words and phrases very widely to take in related aspects that are not usually considered in any depth;
- Review improvements made and explore further opportunities to improve the ISMS;
- · Examine the organisation's potential and actual exploitation of other standards, methods and frameworks

2 of 3 8/28/25, 21:27



relating to information risk and security management;

- Survey, compare and contrast various stakeholders' opinions, comments and suggestions on the ISMS, teasing-out the deeper, longstanding concerns that normally remain hidden/unspoken;
- Follow-up on previous ISMS audits, reviews, penetration tests, security assessments, post incident reports *etc.*, delving deeper into areas of concern or extending the scope, and examining the manner in which audits *etc.* are scoped, conducted, reported, actioned, closed off *etc.*;
- Explore the management aspects of business continuity and resilience;
- · Look into the integration and interoperability etc. of various management systems with the ISMS;
- Audit the organisation's information management as a whole, such as the integration of risk and security aspects with other business imperatives;
- Benchmark the ISMS against comparable organisations or business units, or against other operational management systems *e.g.* quality assurance, environmental protection;
- Measure and comment on the organisation's maturity in this area;
- Review the organisation's use of security metrics, reports, and management information.

Although that is not even a complete list, there are clearly *plenty* of creative possibilities here, in addition to the obvious 'conformity with the standard' approach. One of the best things about auditing is the chance to do something different for a change, making use of the auditors' independence, competence, experience, skills, focus, information access, rigorous methods *etc.* to delve into aspects that are rarely if ever addressed as part of routine management and operations - including those awkward politically-charged issues that are studiously avoided, and longstanding problems that seem set to remain forever.

Some pessimists see audits as information threats to be avoided or minimised: speaking as a former (lapsed? Reformed!) IT auditor and optimist (realist!), I see audits as valuable business opportunities to be exploited to the max.

< Previous standard ^ Up a level ^ Next standard >

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

Simula tu hipoteca

Compra tu vivienda sin ahorros. Simula tu hipoteca en menos de un minuto.

1

3 of 3 8/28/25, 21:27