ISO/IEC 27001

ISO/IEC 27001 is an international standard on how to manage information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005[1] and then revised in 2013.[2] It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure.[3] A European update of the standard was published in 2017.[4] Organizations that meet the standard's requirements can choose to be certified by an accredited certification body following successful completion of an audit. The effectiveness of the ISO/IEC 27001 certification process and the overall standard has been addressed in a recent large-scale study.[5]

Contents

How the standard works

Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Security controls in operation typically address certain aspects of information technology (IT) or data security specifically; leaving non-IT information assets (such as paperwork and proprietary knowledge) less protected on the whole. Moreover, business continuity planning and physical security may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Note that ISO/IEC 27001 is designed to cover much more than just IT.

What controls will be tested as part of certification to ISO/IEC 27001 is dependent on the certification auditor. This can include any controls that the organisation has deemed to be within the scope of the ISMS and this testing can be to any depth or extent as assessed by the auditor as needed to test that the control has been implemented and is operating effectively.

Management determines the scope of the ISMS for certification purposes and may limit it to, say, a single business unit or location. The ISO/IEC 27001 certificate does not necessarily mean the remainder of the organization, outside the scoped area, has an adequate approach to information security management.

Other standards in the ISO/IEC 27000 family of standards provide additional guidance on certain aspects of designing, implementing and operating an ISMS, for example on information security risk management (ISO/IEC 27005).

History of ISO/IEC 27001

BS 7799 was a standard originally published by BSI Group[6] in 1995. It was written by the UK government's Department of Trade and Industry (DTI) and consisted of several parts.

The first part, containing the best practices for information security management, was revised in 1998; after a lengthy discussion in the worldwide standards bodies, it was eventually adopted by ISO as ISO/IEC 17799, "Information Technology - Code of practice for information security management." in 2000. ISO/IEC 17799 was then revised in June 2005 and finally incorporated in the ISO 27000 series of standards as ISO/IEC 27002 in July 2007.

The second part of BS7799 was first published by BSI in 1999, known as BS 7799 Part 2, titled "Information Security Management Systems - Specification with guidance for use." BS 7799-2 focused on how to implement an Information security management system (ISMS), referring to the information security management structure and controls identified in BS 7799-2. This later became ISO/IEC 27001:2005. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.

BS 7799 Part 3 was published in 2005, covering risk analysis and management. It aligns with ISO/IEC 27001:2005.

Very little reference or use is made to any of the BS standards in connection with ISO/IEC 27001.

Certification

An ISMS may be certified compliant with ISO/IEC 27001 by a number of Accredited Registrars worldwide.[7] Certification against any of the recognized national variants of ISO/IEC 27001 (e.g. JIS Q 27001, the Japanese version) by an accredited certification body is functionally equivalent to certification against ISO/IEC 27001 itself.

In some countries, the bodies that verify conformity of management systems to specified standards are called "certification bodies", while in others they are commonly referred to as "registration bodies", "assessment and registration bodies", "certification/ registration bodies", and sometimes "registrars".

The ISO/IEC 27001 certification,[8] like other ISO management system certifications, usually involves a three-stage external audit process defined by the ISO/IEC 17021[9] and ISO/IEC 27006[10] standards:

- **Stage 1** is a preliminary, informal review of the ISMS, for example checking the existence and completeness of key documentation such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the auditors with the organization and vice versa.
- **Stage 2** is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation (for example by confirming that a security committee or similar management body meets regularly to oversee the ISMS). Certification audits are usually conducted by ISO/IEC 27001 Lead Auditors. Passing this stage results in the ISMS being certified compliant with ISO/IEC 27001.
- **Ongoing** involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended. These should happen at least annually but (by agreement with management) are often conducted more frequently, particularly while the ISMS is still maturing.

Structure of the standard

The official title of the standard is "Information technology — Security techniques — Information security management systems — Requirements"

ISO/IEC 27001:2013 has ten short clauses, plus a long annex, which cover:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

Annex A: List of controls and their objectives

This structure mirrors other management standards such as ISO 22301 (business continuity management) and this helps organizations comply with multiple management systems standards if they wish. Annexes B and C of 27001:2005 have been removed.

Controls

Clause 6.1.3 describes how an organization can respond to risks with a risk treatment plan; an important part of this is choosing appropriate controls. A very important change in ISO/IEC 27001:2013 is that there is now no requirement to use the Annex A controls to manage the information security risks. The previous version insisted ("shall") that controls identified in the risk assessment to manage the risks must have been selected from Annex A. Thus almost every risk assessment ever completed under the old version of ISO/IEC 27001 used Annex A controls but an increasing number of risk assessments in the new version do

not use Annex A as the control set. This enables the risk assessment to be simpler and much more meaningful to the organization and helps considerably with establishing a proper sense of ownership of both the risks and controls. This is the main reason for this change in the new version.

There are 114 controls in 14 groups and 35 control categories:

A.5: Information security policies (2 controls)
A.6: Organization of information security (7 controls)
A.7: Human resource security - 6 controls that are applied before, during, or after employment
A.8: Asset management (10 controls)
A.9: Access control (14 controls)
A.10: Cryptography (2 controls)
A.11: Physical and environmental security (15 controls)
A.12: Operations security (14 controls)
A.13: Communications security (7 controls)
A.14: System acquisition, development and maintenance (13 controls)
A.15: Supplier relationships (5 controls)
A.16: Information security incident management (7 controls)
A.17: Information security aspects of business continuity management (4 controls)
A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

The controls reflect changes to technology affecting many organizations—for instance, cloud computing—but as stated above it is possible to use and be certified to ISO/IEC 27001:2013 and not use any of these controls.

See also

- ISO/IEC JTC 1/SC 27 - IT Security techniques
- ISO/IEC 27000-series
- ISO 9001
- BS 7799
- Cybersecurity standards
- International Organization for Standardization
- List of ISO standards

References

1. "ISO/IEC 27001 International Information Security Standard published" (https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/). *bsigroup.com*. BSI. Retrieved 21 August 2020.
2. Bird, Katie. "NEW VERSION OF ISO/IEC 27001 TO BETTER TACKLE IT SECURITY RISKS" (https://www.iso.org/news/2013/08/Ref1767.html). *iso.org*. ISO. Retrieved 21 August 2020.
3. "ISO/IEC 27001:2013" (https://www.iso.org/standard/54534.html). *ISO*. ISO. Retrieved 9 July 2020.
4. "BS EN ISO/IEC 27001:2017 – what has changed?" (https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/). *www.bsigroup.com*. BSI Group. Retrieved 29 March 2018.

5. Akinyemi, Iretioluwa; Schatz, Daniel; Bashroush, Rabih (2020). "SWOT analysis of information security management system ISO 27001" (https://repository.uel.ac.uk/item/88qx1). *International Journal of Services Operations and Informatics*. **10** (4): 305. doi:10.1504/ijsoi.2020.111297 (https://doi.org/10.1504%2Fijsoi.2020.111297). ISSN 1741-539X (https://www.worldcat.org/issn/1741-539X).
6. "Facts and figures" (http://www.bsigroup.com/en/About-BSI/News-Room/BSI-Fast-Facts2/). *bsigroup.com*.
7. Ferreira, Lindemberg Naffah; da Silva Constante, Silvana Maria; de Moraes Zebral, Alessandro Marcio; Braga, Rogerio Zupo; Alvarenga, Helenice; Ferreira, Soraya Naffah (October 2013). "ISO 27001 certification process of Electronic Invoice in the State of Minas Gerais" (https://ieeexplore.ieee.org/document/6922072/). *2013 47th International Carnahan Conference on Security Technology (ICCST)*. Medellin: IEEE: 1–4. doi:10.1109/CCST.2013.6922072 (https://doi.org/10.1109%2FCCST.2013.6922072). ISBN 978-1-4799-0889-9.
8. The ISO/IEC 27001 Certification Process (http://www.27000.org/ismsprocess.htm).
9. ISO/IEC 17021 (http://www.iso.org/iso/catalogue_detail?csnumber=59884).
10. ISO/IEC 27006 (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59144).

External links

- ISO website (https://www.iso.org/isoiec-27001-information-security.html)
