ISO/IEC 27001:2013

From Wikipedia, the free encyclopedia

ISO/IEC 27001:2013 is an information security standard that was published on the 25th September 2013.[1] It supersedes ISO/IEC 27001:2005, and is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27.[2] It is a specification for an information security management system (ISMS). Organizations which meet the standard may be certified compliant by an independent and accredited certification body on successful completion of a formal compliance audit.

Contents

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 the structure of other new management standards such as ISO 22301 (business continuity management);[3] this helps organizations who aim to comply with multiple standards, to improve their IT from different perspectives.[4] Annexes B and C of 27001:2005 have been removed.[5]

Changes from the 2005 standard

The 2013 standard puts more emphasis on measuring and evaluating how well an organization's ISMS is performing,[6] and there is a new section on outsourcing, which reflects the fact that many organizations rely on third parties to provide some aspects of IT.[7] It does not emphasize the Plan-Do-Check-Act cycle that 27001:2005 did. Other continuous improvement processes like Six Sigma's DMAIC method can be implemented.[8] More attention is paid to the organizational context of information security, and risk assessment has changed.[9] Overall, 27001:2013 is designed to fit better alongside other management standards such as ISO 9000 and ISO/IEC 20000, and it has more in common with them.[10]

New controls:

- A.6.1.5 Information security in project management
- A.12.6.2 Restrictions on software installation
- A.14.2.1 Secure development policy
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.8 System security testing
- A.15.1.1 Information security policy for supplier relationships
- A.15.1.3 Information and communication technology supply chain
- A.16.1.4 Assessment of and decision on information security events
- A.16.1.5 Response to information security incidents
- A.17.2.1 Availability of information processing facilities

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 but little understood change in the new version of ISO27001 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 ISO27001 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 now 114 controls in 14 groups and 35 control objectives; the old standard had 133 controls in 11 groups.[11]

- 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 new and updated controls reflect changes to technology affecting many organizations - for instance, the Cloud - but as stated above it is possible to use and be certified to ISO27001:2013 and not use any of these controls.[4]

References

1. "ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements". International Organization for Standardization. Retrieved 27 January 2015.
2. "ISO - ISO Standards - ISO/IEC JTC 1/SC 27 - IT Security techniques". International Organization for Standardization. Retrieved 27 January 2015.
3. Zhou, James (March 2011). "ISO 27001 Information Security Management". Nanyang Technological University. Retrieved 27 January 2015.
4. Breslin, Paul (14 March 2014). "Security updates: The upcoming revision of ISO/IEC 27001". DNV Business Assurance. Retrieved 27 January 2015.
5. "ISO/IEC 27001:2013(en) Table of Contents". *ISO.org*. ISO. Retrieved 11 December 2015.
6. Herbert, Chantall (3 June 2014). "More changes ahead…..ISO 27001:2005 Information Security Management Standard". QSL. Retrieved 27 January 2015.
7. "ISO 27001 update is around the corner". British Assessment Bureau. 14 May 2013. Retrieved 27 January 2015.
8. "Update to ISO 27001 Planned for 2013". Dionach. 25 January 2011. Retrieved 27 January 2015.
9. "BS ISO/IEC DIS 27001 (Draft ISO27001 2013)". IT Governance. Archived from the original on 1 May 2013. Retrieved 2 July 2013.
10. Mackie, Ryan (2 April 2013). "ISO 27001:2013 – Understanding the New Standard". The Pragmatic Auditor. Retrieved 27 January 2015.
11. "The new versions of ISO/IEC 27001 and 27002 are now Final Draft International Standards". Gamma. Retrieved 27 January 2015.

Retrieved from "https://en.wikipedia.org/w/index.php?title=ISO/IEC_27001:2013&oldid=735662815"

Categories: Information assurance standards | ISO/IEC 27000-series