navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

search
Go Search

interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

toolbox
- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link
- Cite this page

languages
- Deutsch
- Español
- Français
- Bahasa Indonesia
- 日本語
- Nederlands
- Português
- Русский
- Svenska

ISO/IEC 27002

From Wikipedia, the free encyclopedia
(Redirected from ISO 17799)

ISO/IEC 27002 part of a growing family of ISO/IEC ISMS standards, the 'ISO/IEC 27000 series' is an information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as **ISO/IEC 17799:2005** and subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards. It is entitled *Information technology - Security techniques - Code of practice for information security management*. The current standard is a revision of the version first published by ISO/IEC in 2000, which was a word-for-word copy of the British Standard (BS) 7799-1:1999.

ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad:

> *the preservation of confidentiality (ensuring that information is accessible only to those authorised to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorised users have access to information and associated assets when required).*

Contents

Outline of the Standard [edit]

After the introductory sections, the standard contains the following twelve main sections:

1. Risk assessment
2. Security policy - management direction
3. Organization of information security - governance of information security
4. Asset management - inventory and classification of information assets
5. Human resources security - security aspects for employees joining, moving and leaving an organization
6. Physical and environmental security - protection of the computer facilities
7. Communications and operations management - management of technical security controls in systems and networks
8. Access control - restriction of access rights to networks, systems, applications, functions and data
9. Information systems acquisition, development and maintenance - building security into applications
10. Information security incident management - anticipating and responding appropriately to information security breaches
11. Business continuity management - protecting, maintaining and recovering business-critical processes and systems
12. Compliance - ensuring conformance with information security policies, standards, laws and regulations

Within each section, information security controls and their objectives are specified and outlined. The information security controls are generally regarded as best practice means of achieving those objectives. For each of the controls, implementation guidance is provided. Specific controls are not mandated since:

1. Each organization is expected to undertake a structured information security risk assessment process to determine its specific requirements before selecting controls that are appropriate to its particular circumstances. The introduction section outlines a risk assessment process although there are more specific standards covering this area such as ISO/IEC 27005.
2. It is practically impossible to list all conceivable controls in a general purpose standard. Industry-specific implementation guidelines for ISO/IEC 27001 and '27002 are anticipated to give advice tailored to organizations in the telecomms, financial services, healthcare and other industries.

National Equivalent Standards [edit]

ISO/IEC 27002 has directly equivalent national standards in several countries. Translation and local publication often results in several months' delay after the main ISO/IEC standard is revised and released, but the national standard bodies go to great lengths to ensure that the translated content accurately and completely reflects ISO/IEC 27002.

Countries	Equivalent Standard
Australia New Zealand	AS/NZS ISO/IEC 17799:2006
Brazil	ISO/IEC NBR 17799/2007 - 27002
Denmark	DS484:2005
Estonia	EVS-ISO/IEC 17799:2003, 2005 version in translation
Japan	JIS Q 27002
Lithuania	LST ISO/IEC 17799:2005
Netherlands	NEN-ISO/IEC 17799:2002 nl, 2005 version in translation

Poland	PN-ISO/IEC 17799:2007, based on ISO/IEC 17799:2005
Peru	NTP-ISO/IEC 17799:2007
Spain	UNE 71501
Sweden	SS 627799
United Kingdom	BS ISO/IEC 27002:2005
Uruguay	UNIT/ISO 17799:2005

Certification [edit]

ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*) specifies a number of requirements for establishing, implementing, maintaining and improving an information security management system consistent with the best practices outlined in ISO/IEC 27002.

See also [edit]

- ISO/IEC_27000-series
- BS 7799, the original British Standard from which ISO/IEC 17799 and then ISO/IEC 27002 was derived
- List of ISO standards
- Standard of Good Practice published by the Information Security Forum
- IT baseline protection

External links [edit]

- The ISO 17799 Newsletter

Categories: ISO standards | IEC standards | Computer security standards