
International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

ISO/IEC 27002:2005 which can be found at <http://www.iso.org/iso/catalogue_detail?csnumber=50297>


Unlike ISO 27001, this standard is a list of recommendations and security considerations that deal with particular information security aspects. It is a code of practice containing general good practice guidance as opposed to prescriptive requirements.


This standard applies to all forms of data, documents, communications, conversations, messages, recordings, photographs, digital data, email, faxes and telephone conversations.

In total, there are eleven units covered by ISO/IEC 27005, and the standard specifies information security controls and their objectives for each of the units. The security controls provided are the best practice means to achieve the given objectives. Guidance is also provided for each of the controls. However, no specific controls are mandated because organisations are expected to undertake structured information security risk assessments to
determine their own specific requirements. The introduction section outlines a risk assessment process although there are more specific standards covering this area such as ISO/IEC 27005 Information Technology - Security Techniques - Information Security Risk Management. The units covered are:

1. **Security policy** - to build an information security program according to ISO 27002/2005, organisations must create, publish and maintain an information security policy for their security management system. Crucially, the policy needs to be reviewed.

2. **Organisation of information security** - this section details the governance of information security. Senior management should provide direction and roles and responsibilities should be clearly established.

3. **Asset management** - this covers the inventory and classification of information assets. Organisations are expected to establish responsibility for assets (IT hardware, software, data, system documentation, storage media and supporting assets) by compiling an inventory of organisational assets, appoint owners, establish rules, develop information classification guidelines and implement information handling and labelling procedures.

4. **Human resources security** - all security aspects relating to employees during the duration of their employment need managed. This applies to their joining, moving and leaving an organisation. Security roles and responsibilities should be defined prior to recruitment, new staff should be vetted and contracts be agreed to protect the organisation’s information. Training should be provided for existing employees and disciplinary processes for security breaches should be implemented. In advance of an employee leaving, systems should be in place to ensure assets are returned and information access rights are terminated.

5. **Physical and environmental security** - this extends to both the protecting of office facilities, perimeter security and natural/human threats in addition to securing the actual computer facilities. Consideration also is given to protecting offsite equipment and to how equipment is disposed and recycled.

6. **Communications and operations management** - fundamentally, this relates to the management of technical security controls in systems and networks. Procedures and responsibilities should be documented. This also extends to the managing of Third Party service delivery. Acceptance criteria and test plans should be produced in advance of system implementation. Procedures should be installed for backing up information and software. Network security controls and procedures should be established. Procedures for removable media need put in place. The disposal of media
also needs managed. All mechanisms for exchanging information should be
documented and safeguarded, including electronic commerce services.

7. Access control - this applies to the ability to permit or restrict the use of
a particular resource by a particular individual and applies to networks,
systems, applications, functions and data. Policies and procedures need
put in place and documented. This extends to passwords, privileges, clear
desk policy and to mobile and teleworking facilities.

8. Information systems acquisition, development and maintenance -
information security needs to be taken into account when specifying,
building/acquiring, testing, implementing and maintaining systems.
Purchased software should be tested for security weaknesses. Access to
system files and test data should be controlled. Formal change control
process should be performed.

9. Information security incident management - procedures for
anticipating and responding to information security breaches need
established with regard to reporting and investigation.

10. Business continuity management - continuity management needs put
in place to protect information for those occasions when business-critical
processes and systems are unavailable.

11. Compliance - complying with legal requirements requires all relevant
information security policies, standards, laws and regulations be identified
and protected. This includes intellectual property rights and the privacy of
personal data. Compliance reviews and information system audits should
be undertaken.

Next month

Next month we will look at PDF/A-1 (ISO 19005-1) a profile of the PDF file
format, which places restrictions on the use components to ensure
reproducability, stability and accessibility over time.

Stephen Scarth

Public Record Office of Northern Ireland