

Is ISO 27001 the Next Big Management System Standard?

At present, there are over 300 published standards relating to information security management programs that have been issued during the last fifteen years. The bodies having issued standards include:

American National Standards Institute,
American Society for Testing and Materials,
Alliance for Telecommunications Industry Solutions,
British Standards Institute,
Canadian Standards Institute,
U.S. Department of Defense, FAA and NASA,
International Organization for Standardization,
International Telecommunications Union, and
Japanese Industrial Standards.

Information, and the technologies that guard it, maintain it, and make it available, has become a central asset of many public and private organizations. The sharing of this information has become a vital lynchpin of commerce in the world today. Protecting information from accidental destruction, sabotage, and other potential attacks has become a major concern, and many companies have been implementing procedures to ensure that this asset is not compromised.

Companies that are interested in the ISO approach to developing standards of practice regarding managing IT security should be please to know that they can now be certified under the [newly released ISO/IEC 27001 standard](#). The new standard, released in October of 2005, is based on the British Standard (BS 7799:2002). The standard is intended to reassure customers and suppliers that information security is taken seriously within an organization, and that the organization has in place recognized processes to deal with information security threats and issues.

The basic objective of the standard is to help establish and maintain an effective information management system, using a continual improvement approach. The following process is used for implementing the ISO/IEC standard 27001.

- 1) Define an information security policy.
- 2) Define scope of the information security management system.
- 3) Perform a security risk assessment.
- 4) Manage the identified risk.
- 5) Select controls to be implemented and applied.
- 6) Prepare an SoA (a "statement of applicability").



The new standard provides a specification for ISMS and the foundation for third-party audit and certification. It is harmonized to work with other management system standards, such as ISO 9001 and ISO 14001, and can assist in the integration and operation of an organization's overall management system. It implements the Plan-Do-Check-Act (PDCA) model and reflects the principles of the 2002 OECD guidance on the security of information systems and networks.

At present, most of the companies adopting this standard are European, but there have been some U.S.-based companies that have recently been certified. The issuing body expects that this system will eventually become a dominant standard throughout the world.

The OH!Polymer Networker newsletter and associated service has been prepared solely for the purpose of providing helpful information to users of this service. The information has been compiled by Tech Resources, a contractor to OH!Polymer, however, no representation is made by either Tech Resources or OH!Polymer as to the completeness or accuracy of the information contained therein. In particular, some information may be incomplete, may contain errors or may be out of date. In addition, neither Tech Resources nor OH!Polymer endorses any product or service mentioned therein.