

The latest [ISO 27000-series](#) international standards for information security management.

These international standards contain best practice guidance to help protect the confidentiality, integrity and availability of the information on which we all depend - information such as our bank accounts, health and defense data, all forms of intellectual property ... indeed even the very words you are reading right now.

- Does your organization gather, generate and/or release valuable information?
- Do you depend on computer systems and networks, or even card index systems and ledgers, to store and process important data?
- Could unauthorized disclosure, modification, insertion or loss of information cause problems for you, your work colleagues, customers, business partners, even the nation at large?

If you answered yes to any of those questions, then you *need* information security and the [ISO 27000 standards](#) are for you.

ISO has reserved the ISO/IEC 27000-series numbering for a range of information security management standards in similar fashion to the very successful ISO 9000-series quality assurance standards.

The following ISO 27000-series standards are either **published** or planned:

- [ISO 27000](#) - vocabulary and definitions (terminology for all of these standards)
- [ISO 27001](#) - **the main Information Security Management System requirements standard (specification) against which organizations are formally certified**
- [ISO 27002](#) (currently known as **ISO 17799** and formerly known as BS 7799 part 1) - this is the Code of Practice describing a comprehensive set of information security control objectives and a menu of best-practice security controls
- [ISO 27003](#) - will be an implementation guide
- [ISO 27004](#) - will be a new Information Security Management Metrics and Measurement standard to help measure the effectiveness of information security management system implementations.
- [ISO 27005](#) - will be a new Information Security Risk Management standard (will replace the recently issued **BS 7799 Part 3**)
- [ISO 27006](#) - may be a new standard: “Guidelines for information and communications technology disaster recovery services”, or possibly a guide to the accreditation process for certification bodies.

ISO 27000 will contain the **fundamentals and vocabulary** in other words the specialist definitions to be used throughout the ISO 27000-series standards.

Information security, like most technical subjects, is evolving a complex web of terminology. Few authors take the trouble to define precisely what they mean, but this is unacceptable in the standards arena as it leads to confusion and devalues formal assessment and certification.

ISO 27000 will presumably be similar to other vocabulary and definitions standards but will hopefully become a generally-accepted reference for information security terms amongst the information security profession. It will probably absorb guidelines such as **ISO/IEC Guide 2:1996 “Standardization and related activities – General vocabulary”** and **ISO/IEC Guide 73:2002 “Risk management – Vocabulary – Guidelines for use in standards”**.

We will of course pass on more information on ISO 27000 here as soon as we receive it ...