

What is ISO 27001 after all?

By Rosângela Caubit – May, 2006

ISO/IEC 27001:2005 is an evolution on British Standard BS 7799-2:2002, which addresses the definition of requirements for information security management systems. The standard was incorporated by the International Organization for Standardization (ISO), an association based in Switzerland which establishes international certification standards in several fields. As a result of its strong tradition in standardizing activities which goes back to the days of the Industrial Revolution, the United Kingdom is a large provider of rules and standards. Some examples of British Standards that have been incorporated by ISO are BS5750, which later became ISO 9000 (Quality) and BS7550, which later become ISO14000 (environment).

ISO 27001:2005 is a revised form of the BS7799-2:2002 standard, with improvements and adaptations. It addresses the PDCA improvement cycle and the process view absorbed by management system standards. The standard was revised by an international technical committee formed by ISO and by the International Electrotechnical Commission (IEC) and the ISO/IEC JTC 1, subcommittee SC 27, which as of 2000 conjointly took on the task of performing the alterations. These changes are a compilation of several suggestions put forth by the members of the committee in meetings, discussions and presentations held in several countries through to the first half of 2005.

Below we present a brief history of how the standard evolved to become ISO 27001:

- **1995:** the first version of BS 7799-1 was published (BS 7799-1:1995 - Information Technology - practice code for information security management)
- **1998:** the first version of BS 7799-2 was published (BS 7799-2:1998 - information security management system - specifications and user guide)
- **1999:** a review of BS 7799-1 was published (BS 7799-1:1999 - Information Technology - practice code for information security management)
- **2000:** the first version of the ISO/IEC 17799 standard was published (ISO/IEC 17799:2000 - Information Technology - practice code for information security management, also referenced as BS ISO/IEC 17799:2000)
- **2001:** the first version of the standard was published in Brazil, NBR ISO/IEC 17799 (NBR ISO/IEC 17799:2001 - Information Technology - practice code for information security management)
- **2002:** a review of the standard BS 7799 part 2 was published (BS7799-2:2002 - Information Security Management System - Specifications and User Guide)
- **August/2005:** the second version of the standard was published in Brazil, NBR ISO/IEC 17799 (NBR ISO/IEC 17799:2005 - Information Technology - practice code for information security management)
- **October/2005:** the ISO 27001 standard was published (ISO/IEC 27001:2005 - Information Technology - Security Techniques - Information Security Management System - Requirements)

The evolution presented above shows that the ISO/IEC 17799, which is an evolution of BS7799-1 incorporated by ISO in 2000, was also revised, and both standards - ISO/IEC 27001 and ISO/IEC 17799 - have been aligned. The next step will be to convert ISO/IEC 17799:2005 into ISO/IEC 27002. This is expected to happen in 2007 and will form the ISO/IEC 27000 family, which will address wider information security aspects.

The most relevant changes occurred during the migration to the ISO/IEC 27001 standard were made to the SGSI structure (information security management system), where internal audit aspects are emphasized, together with security management system performance indicators. Annex A has also suffered several changes and has 11 sections in ISO/IEC 27001, since a section on Information Security Incident Management has been included. It now contains:

1. Information Security Policy
2. Organizing Information Security
- 3 Assets Management
4. Human Resources Security
5. Physical and Environmental Security
6. Operations Management and Communications
7. Access Control
8. Acquisition, Development, and Maintenance of Information Systems
9. Information Security Incidents Management
10. Business Continuity Management
11. Conformity

According to the certifying bodies, companies that have the BS7799-2:2002 certification will be given time to adjust to the new ISO/IEC 27001. The average time granted is eighteen months, by which all companies intending to keep their certifications should have revised their systems and pass a recertification audit prior to migration into ISO/IEC 27001. The natural course is that companies start seeking compliance with the new standard. And given the augmented acceptance of the ISO standard, the number of certifications should also rise throughout the world.