

ISO 27001 & 17799:2005 Information Security Standards Published

Information Security for the Interconnected World

With the publication of ISO 27001 in October 2005 companies now have an internationally recognized standard which, through ISO 9001-style audits, enables them to show

- *Customers* that confidential information will not be accidentally disclosed to competitors or the world at large, or be used in ways that contravene regulatory requirements;
- *Business partners* that computer network security will not be compromised by connecting computer networks;
- *Stakeholders* that risks such as business disruption, damage to reputation, fines, compensation, fraud, loss of confidential information and data corruption are reduced.

Information is Power

Information is power, ever more so in today's competitive, virtual world. Information security management applies to all kinds of information:

- Consumer information (credit, finances, health, etc)
- Company financial information
- Intellectual property (designs, patents, software, music and video recordings)
- Company confidential information (customer and contact lists, product plans)

In the USA, information security is vital to Sarbanes Oxley compliance and, for the medical industry, satisfying HIPAA regulations.

Information Security is More than Technology

It takes more than technology and a powerful IT department to protect information. It takes people, intelligence, and process.

- Only 50% of information security incidents will be detected by technology: the other 50% are "detected the harder way — by customers, colleagues or the news media alerting the company to a breach, or worse yet, to damages the event caused," according to [CIO's "State of Information Security Survey 2003"](#).
- According to Gartner, 60% of security breaches suffered by businesses will be financially or politically motivated, the work of insiders working alone or in collaboration with outsiders.

ISO 27001 – Independent Audits of Information Security Processes and Technology

ISO 27001 addresses the people and process issues as well as IT, bringing them all together into a comprehensive Information Security Management System (ISMS) which requires an organization to systematically assess and mitigate the information security threats it faces.

The new publication separates the requirements for auditing an ISMS from implementation guidance, by specifying for auditors the Requirements for an ISMS in ISO 27001.

Guidance on implementation was also recently revised as ISO 17799:2005, adding many state-of-the-art best practices which address the modern interconnected e-commerce environment with security arrangements for external businesses, outsourcing, software patch management, mobile devices, wireless technologies, mobile code on the Internet and so forth. (Prior to the publication of ISO 27001, companies registered their ISMS to ISO 17799. Henceforth, ISO 27001 is the audit standard for registration, and ISO 17799 is recommended as the implementation standard, in much the same way as ISO 9004 is the recommended implementation standard for ISO 9001 Quality Management Systems.)

ISO 27001 – Under the Hood

Since security risks change almost daily, as hackers and thieves devise new ways around renewed defenses, the heart of ISO 27001 is the requirement for a continual risk assessment process. Using a Plan-Do-Check-Act (PDCA) cycle, regular risk assessments drive continual revision of the Information Security Management System to meet changing threats and address new vulnerabilities.

The Requirements for an Information Security Management System follow the same PDCA framework as an ISO 9001 Quality Management System, comprising:

- General requirements (PDCA cycle based on systematic risk assessment)
- Control of documents and records
- Management responsibility (management commitment, resources, training)
- Internal ISMS audits
- Management review including review input and output
- Continual improvement of ISMS

One way of squeezing extra value from ISO 9001 audits would be to train internal auditors familiar with information security in ISO 27001, so that they can audit the people and process aspects of information security and complement the technological work of the IT department.

Managing Information Security with ISO 27001

The value of ISO 27001 lies in its “Controls”, over a hundred specific aspects of information security which must be controlled in a planned fashion. Supported with requirements like those of ISO 9001 for Documentation, Management Responsibility, Management Review and Continual Improvement, the standard is structured as follows:

1. Risk Assessment and Treatment – systematic identification and prioritization of information security risks and their treatment
2. Security Policy – management direction and support
3. Organization of Information Security – infrastructure, 3rd party access and controlling security of outsourced information processing
4. Asset Management – identifying and protecting assets and information
5. Human Resource Security – addressing roles and responsibilities, screening, training, disciplinary process, termination

Excel Partnership, an SAI Global Company
464 Heritage Road
Southbury, CT 06488 USA
(203)262-2200 / (800)374-3818
<http://www.xlp.com>
xlp@xlp.com

6. Physical and Environmental Security – managing physical access to prevent loss, damage, theft, compromise
7. Communications and Operations Management – ensuring correct and secure operations in computer and network systems, third party services, media (disks), exchange of information (electronic messaging), e-commerce, monitoring
8. Access Control – controlling access rights to information, enforced by controlling and monitoring access to networked devices, operating systems, applications, both directly on the organization’s network and via remote access
9. Information Systems Acquisition, Development and Maintenance – building security into information systems
10. Information Security Incident Management – damage control, reporting, collecting evidence
11. Business Continuity Management – counteracting interruptions and minimizing their impact
12. Compliance – avoiding breaches of law, statutory, regulatory or contractual requirements

ISO 27001 requires a company to define a systematic approach to risk management, to use as a basis for deciding which Controls to implement, and how much to invest in them.

Implementing ISO 27001 is a process familiar to anyone who has introduced an ISO 9001 management system. Start with a risk analysis against the requirements and controls, evaluate risks and the costs of mitigating them, plan and implement the controls necessary to mitigate unacceptable risks. Then monitor and improve the system, maintaining compliance with internal audits and corrective actions. To assure customers and business partners of compliance, engage a 3rd party auditor to certify the Information Security Management System to ISO 27001.

Patrick L Dey

Excel Partnership, an SAI Global Company
464 Heritage Road
Southbury, CT 06488 USA
(203)262-2200 / (800)374-3818
<http://www.xlp.com>
xlp@xlp.com