State-of-the-art information security management systems with ISO/IEC 27001:2005

by **Ted Humphreys**

The recent publication of ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements* [1] is a big event in the world of information security and one that has been eagerly awaited.

This is a revised and updated version of the hugely successful British Standard BS 7799, Part 2, and integrates the process-based approach of ISO 9001:2000 and ISO 14001:2004.

It specifies the requirements and processes to enable a business to establish, implement, review and monitor, manage and maintain effective information security. Like ISO 9001, it is built on the Plan-Do-Check-Act (PDCA) process cycle model *(see **Figure 1**, overleaf)*, and requirement for continual improvement.

ISO/IEC 27001:2005 has been developed by diverse organizations with a common interest – that of protecting their information assets, the "life-blood" of all businesses. These organizations have developed the information security management system (ISMS) standard to enable them to achieve cost-effective information security solutions to protect their business.

A risk management tool

Risk management is at the core of the ISO/IEC 27001 approach to achieving effective information security through continued use of risk methods, built into the PDCA process model, to monitor, maintain and improve such effectiveness. It provides a management framework to enable the best practice controls from ISO/IEC 17799:2005, *Information technology –Security techniques – Code of practice for information security management*, to be applied and managed as part of an organization's overall risk approach (see "Improved ISO/IEC 17799 heralds a new series on information security management systems", *IMS* September-October 2005).

ISO/IEC 27001:2005 provides the means to implement effective information security management in compliance with organizational objectives and business requirements. The

1) ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*, costs 124 Swiss francs and is available from ISO national member institutes (these are listed with full contact details on ISO's Web site : **www.iso.org**) and from ISO Central Secretariat (**sales@iso.org**).

***Ted Humphreys** serves as Convenor of the Joint Technical Committee, ISO/IEC JTC 1,* Information Technology, *Subcommittee 27,* IT Security techniques, *Working Group 1,* Requirements, services and guidelines. *He is also Director of XiSEC, a company specializing in information security management systems.*

Tel. + 44 1473 626615.
E-mail tedxisec@aol.com
Web www.xisec.com

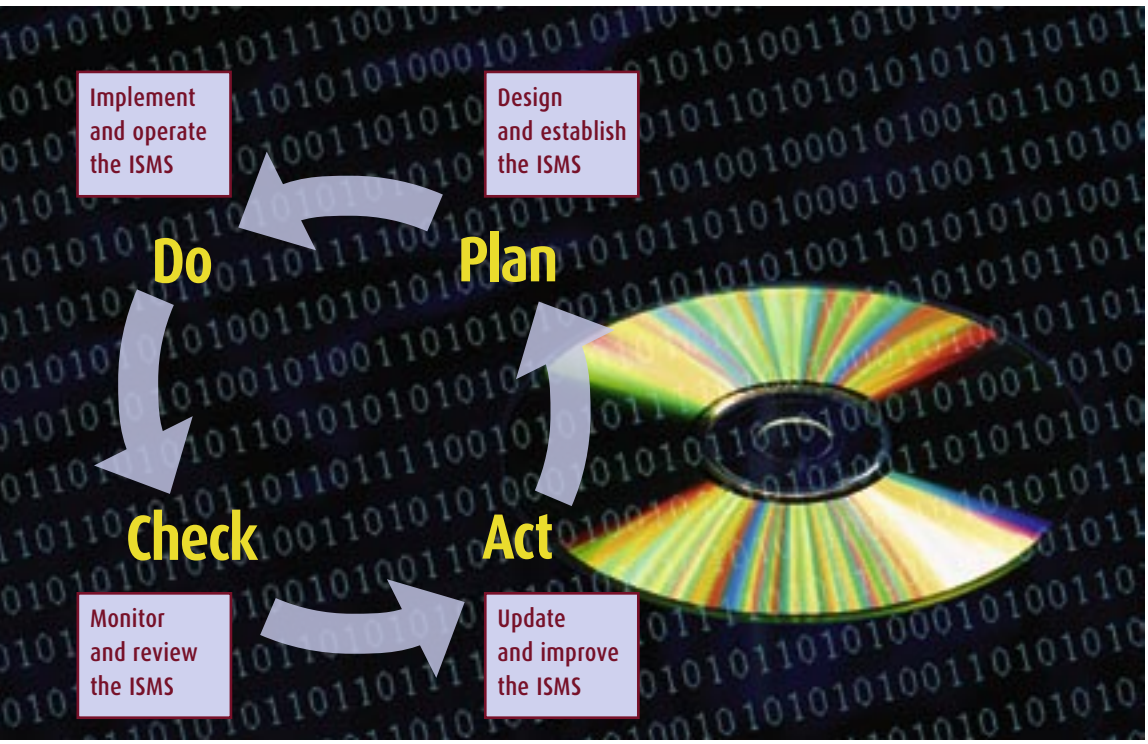

Figure 1: *The ISMS Plan-Do-Check-Act cycle*

standard is a risk-based specification designed to take care of the information security aspects of corporate governance, protection of information assets, legal and contractual obligations as well as the wide range of threats to an organization's information and communications technology (ICT) systems and business processes.

Risk management is at the core of the ISO/IEC 27001 approach

It also refers to the latest Organization for Economic Cooperation and Development (OECD) Security Principles which emphasize the need to engender a "security culture" within an organization. This is especially important in helping the organization fulfil its corporate social responsibilities, and for its overall well-being.

Business benefits

Gaining customer confidence is vital to business. An organization can assure customers by demonstrating that its processes and systems are "fit enough" to meet their needs in sharing and exchanging information, providing a range of services and transacting business online. Outsourcing, off-shoring and providing managed services all rely on achieving and maintaining customer confidence in the organization's business systems. Many organizations have reported the benefits of using these ISMS standards to give customers the assurance of services provided in a secure way.

They have also reported benefits in meeting contractual obligations, and being able to demonstrate this to business partners, customers and other interested business parties. Some have also claimed that applying the standards has helped protect them from numerous business risks while safeguarding critical tangible and non-tangible business assets.

Governments in many parts of the world are also applying ISMS standards to good effect as part of their e-government strategies and implementation roll-outs.

Applicable to all businesses

ISO/IEC 27001:2005 is applicable to small, medium and large organizations. It is practical and flexible enough to integrate with existing management systems and adaptable to any risk approach the organization might adopt. This view is well supported by organizations that have used BS 7799 Part 2 (the forerunner of ISO/IEC 27001) as part of their business strategy. Many have also certified to BS 7799 Part 2 to provide an independent confirmation of the effectiveness of their information security.

ISMS certification

Certification in compliance with BS 7799 Part 2 has increased rapidly in recent years, with more than 2 000 organizations from over 50 countries having done so to date. The International Register of Accredited Certifications at **www.ISO27001certificates.com** provides a list of all certified organizations by country. A further increase is expected with publication of ISO/IEC 27001:2005, although certification is not mandatory, nor is it referred to in the standard.

As the forerunner to ISO/IEC 27001, BS 7799 Part 2:2002 has proved its worth to the many organizations around the world that have certified using the same certification and auditing processes, guidelines and criteria as ISO 9001:2000 (e.g ISO/IEC Guide 62:1996, ISO 19011:2002 and EA 7/03[2]), and

(Continued on page 18)

2) ISO/IEC Guide 62:1996, *General requirements for bodies operating assessment and certification/registration of quality systems*; ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*; and EA 7/03 – (European Co-operation for Accreditation) *Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems*.

WHAT USERS THINK

Up to now, organizations that wished to have their ISMS certified have done so in conformity with the British Standard BS 7799 Part 2. This is now possible against International Standard ISO/IEC 27001:2005.

Here are some comments about the benefits of ISMS implementation and certification from organizations around the world.

Macquarie Telecom: 'Provides our customers with assurance'

"Being BS 7799 certified provides our customers with the assurance that we have all of the proven and correct resources, processes and procedures in place. We are seeing increased awareness and demand from our clients to consider security frameworks, especially as security issues and compliance is being raised at company board level. BS 7799 is just one of the ways we demonstrate our commitment."

Greg Thompson
Group Executive – Hosting and Security, Macquarie Telecom, Australia

Tectraxx: 'Has made a big difference'

"The fact that we announced we would establish a security management system according to BS 7799 Part 2 alone has made a big difference to our competitors. All our customers – from Nokia to Siemens – are very interested that their service provider fulfils this security standard."

Ernst Wiener
IS and QM Manager, Tectraxx, Wiener Neudorf, Vienna, Austria

Polaris Software: 'Enhanced customer confidence'

"BS 7799 Part 2 certification has brought in visible and improved information security awareness among our employees as well as senior management, leading to a high level of compliance, which in turn has enhanced our customer confidence."

S.Y. Amarnath
CISO – Information Security Group, Polaris Software Lab Limited, Chennai, India

Kapsch BusinessCom: 'Recognized on an international scale'

"Thanks to the independent verification performed by CIS, possible hidden deficiencies in our security system can be identified and eliminated. However, the primary goal of our certification is to offer our customers a safety standard recognized on an international scale."

Dr. Franz Semmernegg, CEO, Kapsch BusinessCom, Vienna, Austria

SPI Technologies: 'Winning clients' trust'

"BS 7799 Part 2 has really proven its worth in SPI Technologies' quest for business excellence. In this challenging time where information security is of utmost priority, the ISMS standard has become SPI's armour. It has played a big part in winning clients' trust and confidence in the company's services and capabilities. We believe that enhancing information security within the organization elevates SPI to higher grounds in the BPO* space a winning streak that will make SPI a cut above the rest."

Ian D. Bellord
Global Operations Support, SPI Technologies Inc, Philippines

*BPO = Business Process Outsourcing

BAE Systems Bofors: 'Vital to be certified'

"It is vital to be certified both for us and for our customers. Since we also deal with many international contacts, a worldwide certificate of this kind is essential."

Christina Larsson
Manager Information Security, BAE Systems Bofors AB, Sweden

Tata Steel: 'Reduced information security risks'

"By implementing BS7799 Part 2, we have been able to reduce information security risks, threats, and provide assurance to our stakeholders. It has helped us to build an environment of information security awareness and lay down a focused and structured approach towards security management. We look forward to ISO 27001:2005 which we hope will provide the framework for improving information security controls and their implementation."

Raghavendra Mathur
Head IT Infrastructure, Tata Steel, India

Siemens: 'A real competitive advantage'

"We have striven for certification because this standard offers a maximum of security. When making offers, we enclose the certificate according to BS 7799 Part 2. This spares us the necessity to furnish additional evidence on information security – a real competitive advantage."

Dr. Albert Felbauer
General Manager, Siemens Business Services GmbH, Vienna, Austria

Biznet Solutions: 'Distinguished in a busy market-place'

"Since obtaining the BS 7799 certificate in November 2004, Biznet Solutions has distinguished itself in a busy market-place. Our commitment to Information Security continually provides confidence not only for our customers, but employees and partners also. The certification has given our systems the strength and integrity to help us successfully compete with world class organizations on a global stage."

Gillian Esquivel
Biznet Solutions, Belfast, Northen Ireland

have reported many real and tangible business benefits as a result.

Typical benefits are expressed by a number of certified companies quoted here *(see box, "What users think")*. Similar benefits have been noted by organizations in most of the commercial and industrial market sectors including telecommunications, finance and insurance, utilities, retail and manufacturing, service providers, healthcare, police and emergency services, universities, government departments and agencies.

The new standard is is predicted to become **a best seller**

Consequently, with the publication of ISO/IEC 27001:2005, many organizations have already started preparing for the implementation/certification process – the aim being to achieve an internationally recognized stamp of approval.

The ISO/IEC 27000 family

ISO/IEC 27001:2005 is the first of a family of ISMS standards to be released over the next five years. It is planned to re-number ISO/IEC 17799 as ISO/IEC 27002 in April 2007 to allow existing users time to acclimatize to the new numbering scheme.

Under development is ISO/IEC 27003 which will provide additional guidelines for implementation, and ISO/IEC 27004 which will address the important topic of information security metrics and measurements. This will enable organizations to set performance targets and carry out benchmarking activities to measure the effectiveness of their information security.

Future developments will include ISO/IEC 27000, *Principles and vocabulary*, similar to ISO 9000:2000, and ISO/IEC 27005, a set of guidelines on risk management. Work is also underway on a set of telecoms requirements in collaboration with ITU-T, the standardization entity of the International Telecommunication Union. This is based entirely on ISO/IEC 27001 and defines additive telcoms requirements to the controls in ISO/IEC 27002 (ISO/IEC 17799) and is currently identified as the X.1051 ITU-T standard. It could become part of the ISO 27000 family of standards in the future e.g. as ISO/IEC 27051.

Best seller

ISO/IEC 27001:2005 will thus set the trend for a family of international ISMS standards that are expected to provide many benefits to business worldwide by enhancing information security in today's risk pervasive environment. The new standard is destined to follow the highly successful forerunner BS 7799 Part 2, and, like ISO/IEC 17799, is predicted to become a best seller across a broad spectrum of business markets and sectors. •