

Main Focus



Managing information security

Protecting information a critical and essential business asset

Professor Edward (Ted) Humphreys, ISO/IEC JTC 1/SC 27/WG 1 Convenor, ISMS Standards, Visiting Professor of ISMS Studies and Research at Korea University, Seoul, South Korea

The world has become a far more risky place for business. The Internet is being used for on-line business continues to grow, more businesses are outsourcing and using third party services, supply chains are getting larger and computer fraud is on the increase all risk areas to business. Also business dependence on IT, networks, wireless and mobile communications again raises the risk levels.

The driving force for a successful business is to have the right information at the right time in order to make well-informed decisions. Not only is information the key to business success but the protection of this information is equally important.

ISO/IEC 17799 renumbered as ISO/IEC 27002

In the interest of consistent numbering of the ISO/IEC 27000 series, ISO/IEC 17799 is being renumbered as ISO/IEC 27002 although the content remains unchanged.

Information security is the key. The ISO/IEC 27000 family of International Standards on information technology, security techniques and information security management systems were developed to address the topic of information security management.

The family will cover the following subjects:

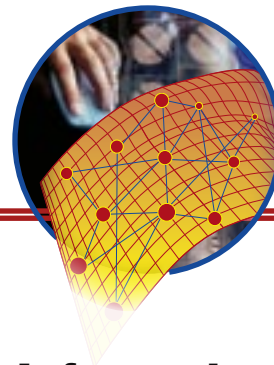
- Information security management system (ISMS) requirements (ISO/IEC 27001:2005);
- Information security management code of practice (ISO/IEC 27002) – formerly designated ISO/IEC 17799, no change in content;
- ISMS implementation guide (ISO/IEC 27003) – under development;

About the author



Professor Ted Humphreys has been leading British activities regarding the ISO/IEC 27000 family of ISMS standards and the British standards BS 7799 Parts 1

and 2 (which later became ISO/IEC 27001:2005 and will become ISO/IEC 27002) since 1990. He is also responsible for many of the ISMS accreditation and certification activities as well as producing the standard EA 7/03. He is an ISMS consultant providing advice to organizations around the world. He is also Founder and Director of the ISMS International User Group, which promotes the global use of the ISO/IEC 27000 family for ISMS standards.



Information security controls and ISMS risk management

Dr Angelika Plate, AEXIS Germany, Secretariat of ISO/IEC JTC 1/SC 27/WG 1 and co-editor of ISO/IEC 27002

ISO/IEC 27002 (previously called ISO/IEC 17799:2005) will be a code of practice for information security management. This International Standard will support the Information Security Management System (ISMS) standard ISO/IEC 27001:2005, which is used world-wide for third party management system audits and certification.

ISO/IEC 27002 will contain helpful guidelines and advice for the security controls that are needed to initiate, implement, maintain and improve ISMS in an organization. However, it is important to understand that ISO/IEC 27002 will contain only guidance and will not be suitable for certification.

The holistic set of security controls in the code of practice will provide business with an important tool to manage its information security risks, to enhance its ability to manage its incidents and to support its business continuity capability.

The key objective of this future International Standard is to enable business to protect the confidentiality, integrity and availability of its sensitive and critical information. In addition, it will offer security controls in the following areas:

- Information security policy
- Organizing information security
- Asset management
- Human resources security
- Physical and environmental security

- Information security management measurements (ISO/IEC 27004) – under development;
- ISMS risk management (ISO/IEC 27005) – under development;
- ISMS accreditation requirements (ISO/IEC 27006:2007). ■

Risk management and ISO/IEC 27001 – A view from Australian business

John Snare, Editor of ISO/IEC 27001

Risk management has long been implicit in the way organizations make a wide variety of management decisions. Recently, there has been increasing recognition that risk management activities need to be formalized so that the management of organizations can make considered decisions concerning a portfolio of risks using a common set of concepts.

The ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*, provides definitions that form a common conceptual framework for considering different types of risk. ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*, uses this common conceptual framework and specifies a management system that can be used to ensure that information security risks can be well managed by organizations.

Using ISO/IEC 27001, information security risk management outcomes can be compared with outcomes of activities to manage other types of risk because it is based on the ISO/IEC Guide 73 definitions.

ISO/IEC 27001 recognizes that it is not possible to eliminate all information security risks. Instead, it allows

organizations to establish information security risk criteria that balance business opportunities, regulatory and contractual requirements, the costs of information security controls, and information security risks.

Using criteria that support organizational objectives, the ISMS requirements specified in ISO/IEC 27001 can be used to establish confidence that information security risks are managed to meet acceptability criteria on an ongoing basis, even if risks or business needs change over time.

“ISO/IEC 27001 allows organizations to establish information security risk criteria.”

ISO/IEC 27001 is unique in that it places requirements to understand information security risks into an operational context, where action is taken to ensure that actions found necessary by a risk assessment are actually taken and are effective. This differs from other information security risk management approaches that place great emphasis on risk assessment and producing a good risk management plan, but give little attention to follow-up to ensure that the plan is implemented and achieves the required outcomes. ■

About the author



John Snare is currently National Manager, DMO Security and Privacy in the Telstra Customer Solutions division. John's professional background includes

20 years working in Telstra's research laboratories and, more recently, 7 years managing aspects of security implementation in other Telstra divisions. He is currently chairman of the Standards Australia subcommittee IT/124 working on data security techniques.



About the author



Dr Angelika Plate runs the German based information security consulting company ÆXIS Security Consultants. She has been involved in ISO activities for

many years, as the editor of several International Standards, including being co-editor of the revised version of ISO/IEC 17799, and she also edited the new accreditation requirements standard ISO/IEC 27006. She is chairing the ISMS IUG Germany, which she founded in 2002, and has recently been appointed as the secretary and vice-chair of SC 27 WG 1.

- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance with legal requirements and security standards

The code of practice will use a risk-based approach, and the security controls in this International Standard should be selected and implemented to meet the requirements that have been identified by a risk assessment as per the requirements specified in ISO/IEC 27001.

Another International Standard under development in the ISO/IEC 27000

family will be ISO/IEC 27005, *Information technology — Information Security Risk Management*. This International Standard provides further explanation about how to carry out a risk assessment and how to successfully implement the resulting controls to achieve overall sound risk management.

It is expected to be published in 2007, and it is important to understand that this International Standard will only provide guidelines for an organization; it will not specify a particular methodology for information security risk management. It is the organization's responsibility to define an approach to risk management that is most suitable to their business. ■

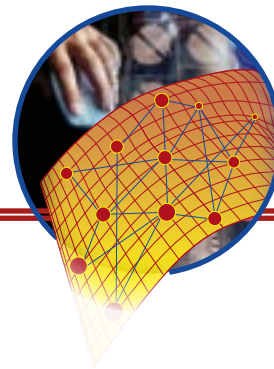
Significance of ISO/IEC 27006

by Toshio Takatori, Director, ISMS Promotion Office, Japan Information Processing Development Corporation, Japan

The International Standard ISO/IEC 27006:2007 *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*, specifies requirements for bodies providing certification of information security management systems. It is intended to ensure their credibility as well as their competence to perform audits.

As an accreditation body, especially in IT-related fields in Japan, the Japan Information Processing Development Corporation (JIPDEC) has operated the ISMS conformity assessment scheme since April 2002, with the aim to promote a high level of information security in Japan.

Under the scheme, JIPDEC accredits certification bodies based on ISMS accreditation criteria, which have been



developed based on ISO/IEC Guide 62, *General requirements for bodies operating assessment and certification/registration of quality systems*, and the European Standard EA 7/03, and those certification bodies conduct audits of organizations seeking ISMS certification.

These certified organizations are now in the process of transferring their certificates from ISO/IEC 17799 to ISO/IEC 27001:2005.

“The ISMS enables an organization to establish an effective framework for managing information security.”

The ISMS enables an organization to clarify its business processes, establish an effective framework for managing information security, and provide confidence to its customers. In addition, it helps the organization to raise its business competitiveness, and plays an important role in IT governance.

In Japan, both public and private sector organizations have increasingly recognized the importance and benefits of the ISMS, which has led to the increase in the number of certified organizations in our country.

In the future, it will be important for the sound development of the ISMS to ensure that the ISMS audits and certifications are internationally credible. As such, the issue of ISO/IEC 27006 will help the increase of ISMS implementation in many parts of the world. ■

About the author

Toshio Takatori is Director of the ISMS Promotion Office, Information Technology Management Center of the Japan Information Processing Development Corporation.

Applying ISO/IEC 27006

by *Eisaku Takeda, ISMS Lead Auditor, IS Certification Division, Japan Audit and Certification Organization for Information Security*

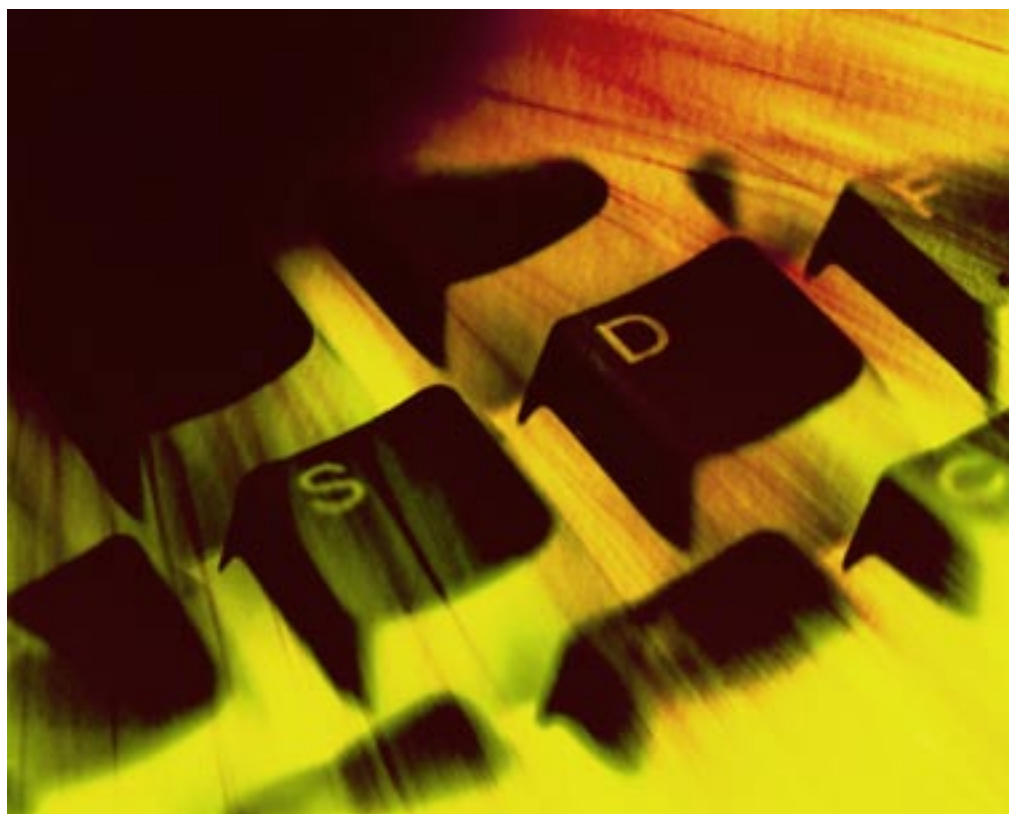
As a certification body with certification to ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*, the Japan Audit and Certification Organization for Information Security (JACO-IS) is also the first company to be accredited in Japan by The United Kingdom Accreditation Service (UKAS) with EA 7/03, Guide 62, *General requirements for bodies operating assessment and certification/registration of quality systems*, and International Accreditation Forum (IAF) guidance.

The new ISO/IEC 27006:2007, *Information technology — Security techniques — Requirements for bodies pro-*

viding audit and certification of information security management systems (the replacement for EA 7/03), important for ISMS certification bodies and auditors because it is easier to integrate with the existing management systems for certification and auditing (which were based on EA 7/03) and it is possible to simplify and refine the documentation.

The new International Standard establishes the foundation of ISMS certification and auditing method of ISO/IEC 27001. The biggest advantage of ISO/IEC 27006 is that it is an ISO/IEC standard; it is therefore recognized internationally and applied as the requirements and guidance for ISMS certification bodies and the auditing method. As EA 7/03 is a European standard for ISMS accreditation, there have been such cases that quality of certification and audit.

We are convinced that accreditation to the International Standard raises the profile of certification bodies, such as JACO-IS, and gives variable assurance to certification clients that the certification body is following the require-

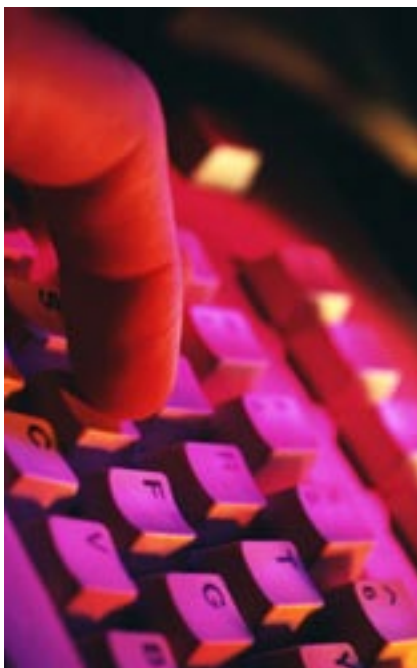


ments and best practice. Accreditation to ISO/IEC 27006:2007 is particularly important for international certification based on conformance to the requirements ISO/IEC 27001.

Finally, we look at sector specific requirement for ISO/IEC 27001 and the future ISO/IEC 27002, which is discussed in the next article on the telecommunications sector. Other sectors that JTC 1/SC 27 is considering are the automotive industry and the regulated domain of world lotteries. ■

About the author

Eisaku Takeda is the ISMS Lead Auditor of the Information Systems Certification Division of the Japan Audit and Certification Organization for Information Security. Previously he was the Manager of the Information Security Technology Department, of the Mitsubishi Electric Corporation, in the Research and Development Division. Mr. Takeda holds an MS in computer science from the University of Denver, US and a BS in mathematics from Hokkaido University.



Information security management for telecommunications

by Koji Nakao, Director of Information Security in KDDI Corporation, Leader of the Institute of National Information Communication Technology

Telecommunications organizations especially those that have participated in ITU-T have been interested in providing a requirements document on information security management for telecommunications since 2003.

In 2004, ITU-T decided to publish an initial Recommendation X.1051, *Requirements for Telecommunications of Information Security Management System (T-ISMS)*, based on BS 7799-2. ITU-T SG17, the group responsible for telecom security, decided to revise the existing Recommendation X.1051 to conform to the ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*, and ISO/IEC 27001