



Name: SRI Standards Update - ISO 27001:2005
Subject: ISO 27001 - Standard for Information Security
To: All Contacts
From: SRI Certification Department

Release: 2006

Client Update: **ISO 27001 Standard**

FOR: SRI Clients

SUBJECT: International Standard on Information Security Management Systems - ISO/IEC 27001:2005

ISO/IEC 27001:2005, a standard for Information Security Management Systems (ISMS), is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems. With acceptance of the international standard, organizations can now develop and implement a global framework for managing the security of their information.

The standard can be used by a broad range of organizations – small, medium and large – in most of the commercial and industrial market sectors: finance and insurance, telecommunications, utilities, retail and manufacturing sectors, various service industries, transportation sector, governments and many others. As information security continues to make headlines, more organizations are looking for a means to assess suppliers' and customers' commitment to the safety of vital business information.

ISO/IEC 27001:2005 specifies the processes to enable a business to establish, implement, review and monitor, manage and maintain an effective ISMS. The standard integrates the process-based approach of ISO's management system standards – ISO 9001:2000 and ISO 14001:2004 – including the Plan-Do-Check-Act cycle and requirement for continual improvement.

If you have any questions or are interested in ISO 27001 registration, please do not hesitate to contact the Certification department at SRI. More information is also available on our website, www.SRIRegistrar.com.

Sincerely,

SRI Certification Department
(724) 934-9000, x613
www.SRIRegistrar.com

Purchase a copy of the standard at:

http://webstore.ansi.org/ansidocstore/product.asp?sku=ISO%2FIEC+27001%3A2005&source=front_page

Full ANSI Abstract, ISO/IEC 27001:2005:

ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government

agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following: * use within organizations to formulate security requirements and objectives; * use within organizations as a way to ensure that security risks are cost effectively managed; * use within organizations to ensure compliance with laws and regulations; * use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met; * definition of new information security management processes; * identification and clarification of existing information security management processes; * use by the management of organizations to determine the status of information security management activities; * use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization; * use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons; * implementation of business-enabling information security; * use by organizations to provide relevant information about information security to customers.

Please Note:

This information has been established by SRI Quality System Registrar (www.sriregistrar.com), an internationally accredited registrar, as a service for SRI's customers and others that may benefit. All information is copyrighted year 2007 by SRI Quality System Registrar, and represents, solely, the opinions and understandings of the company, and is not intended to conflict with, or replace, any requirements of, or communications from ANAB or any other officially designated source or agent. Communications, inquiries, or any updates are invited – please contact us via email: info@sriregistrar.com, or 724-934-9000. SRI not only provides registration to ISO 9001, ISO 14001, AS9100, RC14001/RCMS, OHSAS 18001, ISO/TS 16949, ISO 13485, and ISO 27001, but also provides public training courses for individuals and organizations who want to update their staff's competency. © SRI Quality System Registrar, 2006. All rights reserved.