

Standard Wire

Edition 3 - September 2002



IN THIS ISSUE

TOP OF THE LIST

United States National Committee to Hold Constituency Workshop

CONSULTANT CORNER

ISO 17799 or BS 7799 Pt. 2

STANDARD NEWS

- *ISO updates ISO 14000 brochure for World Summit on Sustainable Development*
- *A Few Small Miracles Give Birth to an ISO Quality: Management Systems Standard For the Automotive*
- *Security Still Pays*
- *OSHA Invites Comments On First Set of Ergonomics Guidelines*

DID YOU KNOW?

Global ISO 14001 Certificate Boom, 60% Increase in 2001

HOW TO...

Risky Business

TOP OF THE LIST

United States National Committee to Hold Constituency Workshop

The United States National Committee (USNC) of the International Electrotechnical Commission (IEC) announced today that a USNC Constituency Workshop has been scheduled for Monday, September 23rd at Edison Electric Institute in Washington, DC.

Open to USNC technical advisors, deputy technical advisors, USNC Technical Advisory Group (TAG) administrators, IEC Technical Committee (TC) or Subcommittee (SC) secretaries and IEC TC/SC chairmen, the workshop will focus on issues and topics identified during a survey of TATAG information needs conducted earlier this year.

Attention will be given to issues such as the global relevance of IEC standards; regional and international cooperation and coordination; intellectual property (copyright) issues; the adoption of standards at both the national and international levels; implementation of the U.S. National Standards Strategy; and various conformity assessment activities. Focus areas will also include a review of successes achieved following the USNC's structural reorganization that was implemented in January 2001 and a report on the current financial status of both the IEC and the USNC.

Read full article:

http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=256

Newsletter Sponsor



GET THE MOST OUT OF
MANAGEMENT SYSTEMS
WITH BSI



BSI Management Systems is the world's leading management systems registrar, helping companies to improve quality and manage risk. BSI Management Systems has registered over 40,000 companies worldwide to ISO 9000, QS-9000, ISO/TS 16949, ISO 14001, OHSAS 18001, and many other management systems. Other services include CE Marking, standards, publications and training courses.

Here are some of the documents we have to help you Get The Most out of Management Systems registration available to download at: <http://www.bsiamericas.com/getthemost>

ISO 9000

- What is ISO 9001:2000?
- Glossary of ISO 9000 Terms
- 10 Top Tips for Transition to ISO 9001:2000
- 10 Tips for Selection and Use of a QMS Consultant
- Transition to ISO 9001:2000 the BSI way
- 10 Tips for Internal Auditing

QS-9000 and ISO/TS 16949

Comparison Matrix of QS-9000 and ISO/TS 16949

OHSAS 18001

Case Study of the Benefits of OHSAS 18001

ISO 14001

What is ISO 14001?

CONSULTANT CORNER

ISO 17799 or BS 7799?

A Two-Part Introduction to the Information Security Management System Standard

by Benny Cheung, Vintara Consultant

PART 2

Question and answer time.

"I don't care which number is for what. Just tell me what an information security management standard is about."

The BS 7799-2:1999 standard has two key sections. The first section describes a six-step framework to establish an Information Security Management System (ISMS). The steps include:

Step 1. Define the Policy: To define an organization's shared vision, commitment and direction in information security.

Step 2. Define the Scope: To determine the boundaries of the ISMS by the characteristics of the organization such as its location, assets and technologies.

Step 3. Undertake a Risk Assessment: To evaluate the risk and threats to the information system and their respective impacts to the organization.

Step 4. Managing the Risk: To determine the organization's approach to risk management and the degree of assurance required.

Step 5. Select Control Objectives: To determine the controls and control objectives which are applicable to the organization and identify any additional controls that are not included in the standard.

Step 6. Prepare Statement of Applicability: To state the reasons for the selection and exclusion of certain controls.

The framework is supported by other common management system components such as effective implementation and document and record control.

The second key section details the requirements of the 10 controls and control objectives. Not all the controls are required. An organization should select the appropriate ones for implementation. The 10 controls are:

- Security policy
- Security organization
- Asset classification and control
- Personal security
- Physical and environmental security
- Communication and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

The standard has given detailed requirements for each of the controls. Your organization is required to select those that are applicable for implementation.

"OK, I can see that it is a useful model, but tell me how it will help my business."

There are plenty of benefits of an ISMS. It improves data integrity and enhances the privacy practices while safeguarding the company's confidential information. A tight ISMS reduces the chances of being attacked and causing damages by malicious users and the loss associated with these attacks. Under such a threat or a disaster, a company is more likely able to contain the problem and restore its operations faster. All of these benefits will contribute to building a higher confidence level with employees, suppliers, customers and shareholders.

Regarding all these benefits, there is a question hanging before committing resources. "Should my company begin information security or should I wait at this time?" Before banging your head too hard on a wall for the correct answer, you should at least know that no company has an information security system that is entirely secure. On the other hand, no one company processes an information system that is entirely open for anyone.

On the spectrum of zero security to perfectly secure, every company is somewhere between the two ends. It would be difficult to find a company that is at the very extreme. That means every company has committed some resources for doing something on information security already. So the question is not whether you should, but whether the current system needs were well thought out and whether the resources are well spent. How do you tell? If your answer is no to either of the questions or you do not know, then you should probably employ the ISMS model to guide you through a structured information assessment and use it to build an information security model. Do it as soon as possible. If you can answer the question confidently that you have a well designed information security system and the resources are well implemented and used, first, congratulations, you are one of the few lucky companies. Although the ISMS standard may still be useful to be a reference, most likely, your company has already complied with all the relevant requirements.

"Now I have heard enough, give me a 20 second summary."

An Information Security Management System (ISMS) is a management system standard that has fundamental components similar to ISO 9000 or ISO 14000. Examples of the common components are policy, document control, audit, record requirements, etc. The same principles "Say what you do, do what you say, and show evidence" basically applies to BS 7799 too.

Unlike ISO 9001 and ISO 14001, however, the international demand for BS 7799 certification has not been picking up much. However, the demand for its compliance is growing. The Center for Internet Security, a consortium of more than 100 organizations including Intel Corporation, VISA, Chevron, Lucent Technologies and Stanford University, has adopted BS 7799 as a foundational standard. A newer version of the BS 7799 will be released in September 2002. Both signs could represent the growing opportunities of the information security management system standards. As a decision maker, you are in the best position to consider the benefits of an ISMS and make a sound decision for information security to your management.

Read more about ISO 17799:

<http://www.iso17.com/information/index.html>

STANDARD NEWS

ENVIRONMENTAL

ISO updates ISO 14000 brochure for World Summit on Sustainable Development

ISO (International Organization for Standardization) has just published a new version of its free brochure on the ISO 14000 family of environmental management standards, specially updated in time for distribution at the forthcoming World Summit on Sustainable Development (26 August-4 September 2002, Johannesburg, South Africa).

Written by experts participating in ISO technical committee ISO/TC 207, the brochure, which updates a 1998 version, is entitled Environmental Management - The ISO 14000 Family of International Standards 2002. It provides an overview of the 25 published standards, technical reports and guides developed by the committee since it was established in 1993, as well as documents in progress, and other ISO 14000-related publications by ISO.

Read full article:

<http://www.iso.org/iso/en/commcentre/pressreleases/2002/Ref831.html>

QUALITY

A Few Small Miracles Give Birth to an ISO Quality Management Systems Standard For the Automotive

The potential for using ISO standards as a basis for alignment of customer requirements in global industries was established with the publication of ISO/TS (Technical Specification) 16949:2002. This standard, "Quality management systems -- Particular requirements for the application of ISO 9001:2000 for automotive production and relevant service part organizations," represents a significant advance to support the global automotive manufacturing industry.

Read full article:

<http://www.iso.org/iso/en/commcentre/isobulletin/articles/2002/pdf/automotiveind02-08.pdf>

INFORMATION SECURITY

Security Still Pays

Tight budgets, hiring freezes and layoffs haven't stopped employers from continuing to invest in security professionals with the right stuff.

It's no secret that the listless economy has forced profound changes on almost everything under the IT umbrella. The soaring salaries and enormous bonus incentives used to lure IT pros at the height of the dot-com boom have plummeted as quickly as they shot up.

Except in security.

Infosec compensation has shown astonishing staying power, based on this year's annual Foote Partners' review for Information Security. The review, compiled from questionnaires and direct interviews conducted quarterly with nearly 30,000 public and private sector IT professionals in the U.S. and Canada, shows a marked divergence between security jobs and the rest of IT in nearly every compensation statistic.

Base salary, certification premium pay and bonus pay for security professionals continued to climb--albeit more slowly--while compensation for almost all other IT categories sank.

The bottom line: With above-average pay performance in security-related jobs posted for a second straight year, and an enormous upside potential for long-term career advancement, many of IT's best and brightest will gravitate to the field as it evolves and expands.

Read full article:

<http://www.infosecuritymag.com/2002/aug/securitymarket.shtml>

OCCUPATIONAL HEALTH & SAFETY

OSHA Invites Comments On First Set of Ergonomics Guidelines

WASHINGTON, Aug 29, 2002 (U.S. Newswire via COMTEX) -- The Occupational Safety and Health Administration is scheduled to announce in tomorrow's Federal Register a notice informing the public that the first set of industry-specific ergonomic guidelines -- Guidelines for Nursing Homes -- is available for public comment. The guidelines will be available August 30 on OSHA's website at www.osha.gov/ergonomics (select "guidelines").

"These guidelines are the result of an extensive and cooperative process involving a wide-ranging, inclusive review of both scientific information and existing ergonomic practices and programs in the nursing home," said OSHA Administrator John Henshaw. "We also conducted one-on-one meetings with major stakeholder groups to gather information on best practices that have been successfully used in the nursing home industry to ensure we are recommending practical solutions that will work in the real world."

The guidelines are in three parts, with a reference list at the end:

- Management Practices discusses the importance of management commitment and employee participation in ergonomics training, occupational health management of musculoskeletal disorders, and ergonomics program evaluation;
- Worksite Analysis discusses assessment of resident handling tasks and activities other than resident handling; and
- Control Methods contains illustrations that demonstrate various methods to control common ergonomic stressors.

The guidelines are intended to provide practical solutions for reducing ergonomic-related injuries and illnesses in nursing homes. They will not be used for enforcement purposes. Draft guidelines are being developed for other industries and will also be available for comment.

DID YOU KNOW?

Global ISO 14001 Certificate Boom, 60 Percent Increase in 2001

International ISO 14000 certificate growth exploded in 2001 with an unprecedented increase of 60.57 percent, according to The ISO Survey Eleventh Cycle. "Up to the end of 2001, at least 36,765 ISO 14000 certificates had been awarded in 112 countries, an increase of 13,868 certificates (+ 60.57 percent) over the end of December 2000 when the total stood at 22,879 in 98 countries. This is by far the highest increase recorded in the seven cycles of the survey in which ISO 14000 has been included starting with the results at the end of December 1995," the survey reports.

Courtesy of The Environmental Management Report

HOW TO...

Risky Business: Standards Like ISO 9004, ISO 14001 and OHSAS 18001 Can Help Organizations Manage Risk

Recent news events have focused business leaders on the importance of looking after all their stakeholders. Although profit is fundamental to business success, it's no longer acceptable to drive businesses exclusively through financial controls. Other factors must be considered to ensure that the business of business remains successful during the medium term. Customers, employees, legislation, litigation, and local and worldwide opinions can all significantly affect the health and prosperity of any organization.

Will your company be the next one to hit the headlines? Consider the following leads from July 2002 issues of the Financial Times:

- U.S. regulators are underfunded and pulled in dozens of directions in their efforts to restore investor confidence.
- Sony became the latest victim of investor concern.
- Tyco shares dropped sharply after a Goldman Sachs analysis.
- China's insatiable demand for coal has precipitated a series of terrifying underground explosions.
- The World Health Organization yesterday released the draft text of a groundbreaking international tobacco control treaty.
- Farmers and residents are protesting the planned seizure of their land to build a new international airport for Mexico City.

Governments in North America, Europe and Asia are increasingly focusing on corporate governance and internal controls. As a result, organizations will have to demonstrate that they have structured management systems in place to review and prioritize all their stakeholders' needs as well as manage the business risks they face. Many view these issues as related initiatives that must be adopted as additional business functions.

How can organizations juggle the conflicting requirements of high financial returns, fair salaries, decent working conditions, low prices, excellent service and minimal impact on the environment?

Read full article:

http://www.qualitydigest.com/sept02/articles/03_article.shtml



Vintara is the leading provider of Web-based process management solutions and services. Founded in 1997, Vintara has a proven track record of helping the enterprise successfully prepare for and cost-effectively maintain compliance with a range of domestic and internationally recognized standards. Our customers come from a variety of industries, with a diverse range of needs. In every case, Vintara has created solutions that meet and exceed their growing business needs.

Combining innovative technology with training and consulting services, our brands – ISO9, ISO14, ISO17 and OHS18 – deliver the solutions that help the enterprise manage their key business processes setting the path to continual improvement.

For more information on Vintara, click on the URL: www.vintara.com

FEEDBACK

Is there something we're missing that you'd like to see in a future edition? We'd love to hear from you. Let us know what you think about Standard Wire by writing us at standardwire@vintara.com. Visit us today at www.vintara.com or call 1.866.321.4769 for more information.

SUBSCRIPTION

1. Change your email address: Please reply to this message with the words CHANGE EMAIL in the subject field.
2. Tell a friend: If this email has been forwarded to you and you would like to be added to the distribution list, send an email to standardwire@vintara.com with SUBSCRIBE in the subject line.
3. Cancel your subscription: Your privacy is important to us. If you do not wish to receive future communications from standardwire@vintara.com, please reply to this message with the word UNSUBSCRIBE in the subject line.

CONTACT

- For a guided demo of any Vintara brand solutions, please contact sales@vintara.com
- Send news items to pr@vintara.com
- Send questions, complaints or service queries to info@vintara.com
- Send advertising inquiries to info@vintara.com