QM&T Winter 2011_2012` Newsletter
© Quality Management & Training Limited - website www.qmt.co.uk

Happy New Year to all our Readers

Auditing Information Security Controls

A new Technical Report (TR) has been released by ISO that provides guidance and information for auditors when assessing security techniques. *ISO/IEC TR 27008:2011, Information technology – Security techniques – Guidelines for auditors on information security controls* hopes to provide confidence in the controls within an organisation's information security system.

Edward Humphreys, leader of the working group that developed the report said, "The business environment is constantly changing – along with threats to a company's survival. Organisations need to be ahead of the game and an excellence defence can be built around audit of the controls used to support information security. ISO/IEC TR 27008:2011 supports a rigorous organisational security audit and review programme for information security controls, to enable the organisation to have confidence that their controls have been appropriately implemented and operated and their information security is fit for purpose."

Further information on the report can be found at www.iso.org

Dealing with Management System Records

Two new standards have been released by ISO to assist organisation on dealing with their management system records. The standards are compatible with other management system standards such as ISO 9001 and ISO 14001. *ISO 30300:2011, Information and documentation – Management systems for records – Fundamentals and vocabulary,* and *ISO 30301:2011, Information and documentation – Management systems for records – Requirements* also incorporate the experience gained in the implementation of ISO 15489 on records management that was published 10 years ago.

Judith Ellis and Carlota Bustelo, leaders of the working groups that developed the standards, have said, "The ISO 30300 series offers the methodology for a systematic approach to the creation and management of records, aligned with organisational objectives and strategies. Managing records using a management system standard supports cost-effective operational processes, such as storage, informational retrieval, information re-use, litigation and due diligence."

Further information on these standards can be found at www.iso.org.

Help in a Crisis

The ISO and BSI have both recently issued standards that aim to help organisations deal with disasters.

ISO 22320:2001, Societal security – Emergency management – Requirement for incident response, aims to minimise the impact of disasters, terrorist attacks and other major incidents. The standard outlines Best Practice for implementing command and control structures and procedures, decision support, traceability and information management that are required for a successful response.

Prof E-P Dobbling, Convenor of the working group that developed the standard, said, "Any response following an incident might include the participation of both public and private organisations working at international, regional or national levels. Harmonised international guidance is needed to coordinate efforts and ensure effective action. ISO 22320 is a valuable tool that all types of organisations can use to improve their capabilities in handling incident response in any crisis. In addition to its many benefits, we hope that the information and communication requirements outlined in the standard can promote the development of innovative technical solutions enabling maximal interoperability for communication, which in an emergency can be the key element for success or failure."

For further information, please visit www.iso.org

The British Standards Institute (BSI) have released a *Publically Available Specification (PAS) 200:2011, Crisis management – Guidance and good practice* that is designed to help organisations take practical steps to improve their ability to deal with crises. It provides a framework to help organisations identify potential crises, mitigate the risks and avoid potentially damaging results.

Please visit www.bsi-global.com for further information.

Anti Bribery support

The UK Bribery Act makes it an offence if "adequate measures" are not in place to prevent corrupt practices from happening. The British Standards Institute (BSI) released a standard at the end of 2011 that could help organisations demonstrate that they have done everything that they could to comply with the Act.

BS 10500:2011 Specification for an anti-bribery management system (ABMS) provides a framework for a systematic approach for putting in place procedures and controls that will make sure that you have 'adequate measures' in place.

BS 10500 is a complete management system that includes guidance and easy to follow checklists to help an organisation put processes in place to stop any bribery and corruption.

For further information, pleas visit www.bsi-global.com

Popularity of ISO Standards

The ISO have released information on the use of ISO standards in 2010. ISO 9001 remains the most popular standard with over 1 million certificates issued in 178 countries. China is top of the table for total number of certificates, with Italy second and Russia third. China also showed the highest growth in number of certificates.

Over quarter of million ISO 14001 certificates have been issued in 155 countries, with again China heading the table for number of certificates, with Japan second and Spain third. However, the UK was in the top three for annual growth.

The biggest increases in certification are to the sector-specific ISO22000:2005 food safety management system standard which is up by 34% and the issue-specific ISO/IEC 27001:2005 information security management system standard which has risen by 21%.

Rob Steele, ISO Secretary-General said, “Indicating nearly a million and a half users at the end of 2010, these figures illustrate the continuing attraction of the ISO management system model pioneered by ISO 9001 for quality management and since extended to meet other challenges faced by public and private sector organisations.”

The principle findings of the survey are available free of charge from the ISO Website www.iso.org.

New Auditing Standard

A new version of the ISO 19011 auditing standard was released at the end of 2011 by ISO. The 2002 version only applied to ISO 9001 and ISO 14001, whereas the new version has been expanded to cover the complexities of auditing multiple management system standards. It provides the guidance on how to carry out internal or external management system audits as well as how to manage audit programmes.

Alistair Dalrymple, convenor of the team that updated the standard, said, “ISO 19011:2011 has been revised to provide auditors, organisations implementing management systems and organisations needing to conduct audits of management systems an opportunity to re-assess their own practices and identify improvement opportunities. Compared to the 2002 version, the standard adds the concept of risk and recognises more explicitly the competence of the audit team and individual auditors. Also, the use of technology in remote auditing is acknowledged, for example conducting remote interviews and reviewing records remotely”.

For further information, please visit www.iso.org

Environmental Support

The British Standard Institute (BSI) have recently released a revised edition of PAS 2050 – their standard for calculating the carbon footprint of goods and services. This can help organisations identify their environmental impact beyond their own activities as it can be used to look at the ‘carbon footprint’ of the entire supply chain.

PAS 2050 can be downloaded free from the BSI website www.bsi-global.com

The BSI have also released *BIP 2178:2011 Climate Change Adaptation: Adapting to climate risks using ISO 9001, ISO 14001, BS 25999 and BS 31100* as a guide to a logical and cost-effective approach to identifying future climate risks and embedding management of those risks in an existing management system.

Further information can be found from the same BSI website.