ISO 9001 and ISO 14001 White Papers

I am sure that you are all aware of the recent revisions of the ISO 9001 and ISO 14001 standards and in our last newsletter we provided links to a range of support material. The CQI and IRQA have both been heavily involved in these revisions and they have also produced two white papers that give you their insights in to the main changes. You can download these white papers at:
http://www.thecqi.org/Knowledge-Hub/Management-system-standards/CQI-Resources/ISO-White-Papers/ISO-90012015-and-140012015/
http://www.thecqi.org/Knowledge-Hub/Management-system-standards/CQI-Resources/ISO-White-Papers/ISO-90012015-and-140012015/

The BSI have also produced a white paper highlighting the changes and providing practical advice on how small businesses can implement the standard. You can download it for free from:

http://shop.bsigroup.com/forms/ISO-9001-white-paper/?utm_source=Pardot&utm_medium=Newsletter&utm_term=Bodytext&utm_campaign=SM-STAN-NEWS-QM-QualityNewsletter-BUYS-1511

Following on from the ISO 14001:2015 publication last year, the revision of the complementary standard ISO 14004 has reached its final draft stage. The key focus of the revised ISO 14004 is reflected in its new title "Environmental management systems – General guidelines on implementation". ISO 14001:2016 aims to provide guidance on the establishment, implementation, maintenance and improvement of an effective EMS. It is intended to help organisations manage their environmental responsibilities in a systematic manner, thereby contributing to sustainability. It will align with the changes made to the recently revised ISO 14001:2015.

Per Arne Syrrist, Convener of the working group that revised ISO 14004, said: "The 2016 version of the standard will be a useful guidance document, both for those organisations that are yet to implement an EMS, and those with EMS experience that want to develop it further to cope with future environmental challenges."

ISO 14004:2016 is due to be published in March 2016. For further information visit www.iso.org

Chartered Quality Institute's Conference

The 2016 CQI Conference will take place on 13 April at The King's Fund London. It will build on the 2015 theme "The future of business excellence" and look at how quality management is changing.

According to the CQI, attendees can expect:

- Thought provoking content sessions
- Collaborative approaches to implementing quality
- To be inspired in a series of case studies and "interactive workshop sessions"
- Networking with more than 250 professionals
- Insight from more than 15 industry and revolutionary quality practitioners

Speakers include; Tim Coultard, Head of Communications and Marketing at the CQI, Gerald Ashley, Risk and behaviour expert and Managing Director at St Mawgan & Co Limited, and Tim Harford, the Undercover Economist Author and Financial Times columnist. For further information and to book visit www.thecqi.org

Competency-based Interviews

Are you looking to change your job in 2016? You might find using the STAR approach will help you to communicate your skills and abilities to the interviewer more clearly. It is designed to enable you to provide a meaningful and complete answer to questions asking for specific examples and at the same time, simple enough to be applied easily.

STAR stands for Situation – Task – Action – Result

S – Situation. Describe the situation that you were confronted with where the task had to take place. This sets the context for the task. It needs to be concise and informative and focus on what is useful to the story.

T – Task. Explain the task that you had to complete. Again keep it simple and focused.

A – Action. This is where you must demonstrate and highlight the skills and personal attributes that the interviewer's questions are testing. You have set the context of the example and now you must explain what you did. Key points to remember are:

- Keep it about you – not what the rest of your team did
- Include relevant details – do not assume that they will guess what you mean
- Steer clear of technical details unless it is crucial to understand the story
- Explain what you did, how you did it and why you did it

Your answer should help the interviewer understand the skills and abilities you have in dealing with the example situation. They should understand what drove your actions and reinforce the feeling that you consider the consequences of your actions and retain full control of the situation.

R – Result. Explain the results of your actions. Use the opportunity to describe what you accomplished and what you learnt from the situation. This helps you make the answer personal and enables you to highlight further skills.

For further information visit http://www.interview-skills.co.uk/competency-based-interviews-STAR.aspx

Legal Admissibility of Electronic Information

One of the benefits of a Quality Management System is that it can provide you with helpful documentary evidence should you need it to fight a legal case. However, much of that evidence is now electronic, can it still be used? BS 10008: *Evidential weight and legal admissibility of electronic information – Specification* has now been revised to keep pace with the expanding reliance on IT systems. It describes how information should be managed to ensure that the evidential weight is maximised and is demonstrably trustworthy. BS 10008 describes:

- How to deal with structured data
- Recognise recent changes in how information is managed as an asset
- Cover stewardship of electronic information as an organisational activity
- Alignment with the ISO management system standards structure

For further details visit www.bsigroup.com

Emergency and Damage Management

Organisations coping with the extensive flooding that the north and west of Britain have experienced over the last few weeks may find a recent standard from the BSI helpful. *BS 12999:2015: Damage management – Code of practice for the organisation and management of the stabilisation, mitigation and restoration of properties, contents, facilities and assets following incident damage*; provides recommendations for the organisation and management of the initial response, stabilisation, and restoration of properties, contents and assets following incident damage. The new standard includes:

- Best practices to stabilise, mitigate, remediate and restore damage
- A simple method to establish whether these activities have been conducted well
- A guide to communication between parties who should be aware of an incident's status

It has been developed in line with good risk management practice and insurance principles; and it aims to provide recommendations to individual damage management practitioners and organisations. It is also relevant to anyone who might be affected by damaging incidents – including property owners, emergency responders, insurers, facilities management, and those in government departments and local authorities. For further information and to buy the standard, please visit www.bsigroup.com

Further, two recently published ISO standards could also be helpful in dealing with emergency situations that put people at risk. ISO 22322:2015, *Societal security – Emergency management – Guidelines for public warning*, gives guidelines for developing, managing and implementing public warning before, during and after incidents occur; and ISO 22324:2015, *Societal security – Emergency management – Guidelines for colour-coded alerts*, gives guidelines for the use of colour codes to inform people at risk, as well as first-response personnel, about danger and to express the severity of a situation.

ISO 22324 describes how colours should be used e.g.

Red is associated with danger and should be used to notify people at risk to take appropriate safety actions immediately. Yellow is associated with caution and should be used to notify people at risk to prepare to take appropriate safety actions. Green is associated with a safe status and should be used to notify people at risk that no action is required. In addition, black, purple, blue and grey may be used to provide additional messages, such as fatal danger, supplementary information, or when no information is available. For further information, visit www.iso.org

Cyber Security

One of the key changes in the revised ISO 9001 standard is the increased focus on risk management. One of the greatest risks that many organisations face is cyber-attack. The ISO/IEC 27000 series on security techniques for information technology has been updated to provide organisations with standards and systems that should help them keep their information safe.

Prof. Edward Humphreys, Convener of the working group responsible for ISO's information security management systems (ISMS) standards, emphasizes, "To ensure security in today's digital landscape, all organisations, irrespective of size, should put in place a management framework as a starting point to manage cyber risks. ISO/IEC 27001 was designed to help organisations do just that. The standard is the world's 'common language' when it comes to assessing, treating and managing information-related risks."

There are some new additions to the ISO 2700 series:

A new code of practice for information security controls for cloud services, ISO/IEC 27017, has just been published. The cloud is one of the most widely used innovations now being used by commerce and business. Users demand assurances that data stored and processed in the cloud is safe. The marketplace for cloud services is global, with providers located across wide geographical areas, and data is routinely transferred across national boundaries. International guidance is therefore key.

ISO/IEC 27013 offers a systematic approach to facilitate the integration of an information security management system with a service management system, which results in lower implementation costs and avoids duplication efforts as only one audit, instead of two, is needed when seeking certification.

ISO/IEC 27010 is a sector-specific addition to the ISO/IEC 27000 toolbox, which guides the initiation, implementation, maintenance and improvement of information security in inter-organisational and inter-sector communications. It includes general principles on how to meet these requirements using established messaging and other technical methods. The standard is expected to encourage the growth of global information-sharing communities.

ISO/IEC 27039 gives guidelines to prepare and deploy an Intrusion Detection and Prevention Systems (IDPS), covering such crucial aspects as selection, deployment and operation. The standard is particularly useful in today's market where there are many commercially available and open-source IDPS products and services based on different technologies and approaches. ISO/IEC 27039 will guide organisations throughout the process.

More and more organisations are turning to third-party certification audits to demonstrate that they have in place a solid information security management system (ISMS) that conforms to the requirements of ISO/IEC 27001. ISO/IEC 27006 gives the requirements that certification and registration bodies need to meet to be accredited, so they can offer ISO/IEC 27001 certification services. For more information on the standard, please visit www.iso.org