ISO 22301 – a walk in the park or an auditor's worst nightmare?

Hilary Estall explains how a new approach to planning and communication can help auditors navigate the new BCMS standard

When *ISO 22301 – Societal security – Business continuity management systems - Requirements* was finally published in May, organisations and certification bodies alike began pouring over it to determine how it differs from BS 25999-2. They wanted to know what changes will have to be made to existing business continuity management systems. So, what's the verdict?

I recently heard one certification body announce to a forum of consultants that ISO 22301 was very similar to BS 25999 and that the transition process would be simple for clients. My response was that for those of us who had been working closely with the British Standard and more recently the ISO standard, this comment may indeed hold some truth, but for the organisations trying to understand the impact of the new ISO standard, it may be a very different story. Assume nothing!

There are a number of differences between BS 25999-2 and ISO 22301 and it will take an auditor a number of 'read-throughs' as well as supportive training to become familiar with them. Here, we identify a few of the key variations to whet your appetite and send you running to your copy of ISO 22301 to read more!

Planning
With reference to the 'plan, do, check, act' model, four of the of the seven core BCMS clauses in ISO 22301 address planning requirements. From the development of the BCMS framework and the setting of policy and objectives through to establishing competent resource and an effective communication policy, planning is critical to a successful BCMS. Auditors should expect to see a greater involvement of top management and a more overt degree of leadership when it comes to business continuity management.

Top management
Management are now expected to really get behind the business continuity policy and use it as a mechanism for driving the business forward through clear direction and purpose. Gone are the days of an auditor accepting a signed piece of paper on the wall. Top management are also now expected to take more of a leadership role and retain overall responsibility for the BCMS and its effectiveness. As an auditor, how might you reasonably assess this and determine whether it's appropriate?

Interested parties
The organisation must now determine who the interested parties (formally referred to as stakeholders) are and identify their needs and expectations, whether expressed to the company or simply implied. Having achieved this, the organisation must then develop strong communication links with them on an on-going basis. Providing demonstrable evidence of this to the auditor will be more onerous and as an auditor you should be clear about what you expect to see.

Communication
Communication before, during and after an incident is a clear requirement. The organisation shall determine what BCMS communications is appropriate for both internal and external parties, and manage communications from interested parties. Methods of communication to be used during an incident also have to be identified and tested and could include alternatives not usually deployed by the organisation.

Performance evaluation
The need to identify and gather suitable performance metrics to assess the performance of the BCMS is new and takes performance review much further than BS 25999. Little steerage is offered in the standard and the organisation will have to determine what information should be included to evaluate the performance of its BCMS. This is an area where, as auditors, you will develop your knowledge through exposure to practices observed but you would do well to have some thoughts of your own, which could be obtained through training.

Summary
We all know that ISO standards have a habit of being less prescriptive than British Standards in order to appeal to a wider international audience. We also know that this leaves far greater scope for interpretation by the incumbent organisation, not to mention the auditor. Certification bodies have been frequently challenged on the competency of their BCMS auditors, so the question is: how should they now ensure that their business continuity auditors are able to demonstrate a pragmatic approach and are fit for purpose? As a starter for ten I would recommend deploying auditors with solid business experience and a good dose of common sense!

Hilary Estall SBCI and IRCA Lead BCMS auditor runs her own business continuity consultancy company, Perpetual Solutions. Her book, *Business Continuity Management Systems* (RRP £29.99), is a practical guide for organisations implementing a business continuity management system and certification in line with ISO 22301. As the only 'working tool' on the market, it includes self-assessment checklists, worksheets and top tips. A 15% discount is available with the code BCMS12 until 31 December 2012.