ISO 27001 vs ISO 22301: An On-Going Debate

There has been significant debate about the overlap of ISO 22301 (Business Continuity) and ISO 27001 (Information Security), and whether one standard or management system would provide reassurance for both disciplines and, more specifically, whether ISO 27001 ensures adequate Business Continuity, thereby negating the requirement for ISO 22301.

Requirements for Each Standard

ISO 22301 requires the implementation of a Business Continuity Management System (BCMS) which emphasises the importance of 'implementing and operating controls and measures for managing an organisation's overall capability to manage disruptive incidents', amongst other things.

Conversely, ISO 27001 requires the implementation of an Information Security Management System (ISMS) which 'preserves the confidentiality, integrity and availability of information'.

Both systems require the implementation of a Management System, closely linking to organisational objectives, and requiring explicit leadership and management commitment.

So What Does This Mean in Practice?

Taking aside the 'Management System' aspects, such as context, scope, leadership, internal audit, management review, etc, which are remarkably similar for each standard; each standard has a different approach, with ISO 22301 requiring the development of a Business impact Analysis and Risk Assessment, prior to the identification of suitable strategies, incident and business continuity response mechanisms, and a requirement for training and exercising. ISO 27001 requires an understanding of the risks, and then implementation of suitable risk treatments and plans, using the control objectives and controls detailed in Annex A of the standard. These control objectives are discussed in substantially more detail in ISO 27002.

ISO 27001 is much more prescriptive, with organisations required to choose which of the information security control objectives and controls should apply to their organisation and to justify any exclusions that they chose to adopt, and then deciding how they would implement any controls, with detailed guidance given in ISO 27002. Thus, there are some control objectives that may not apply to a particular business, eg if they are not dealing with cryptographic materials (A.10), so it would be sensible to opt out of this. However, I would expect the majority of businesses to have controls for the majority of these objectives. As an example, it is hard to see why a business would be able to choose exemption from the requirements of A.17 information security aspects of business continuity management

And What Does It Mean for Business Continuity?

To take a closer look at the requirements of A.17 Information Security, the following controls are specified:

- A.17.1.1 requires that an organisation 'determine its requirements for information security and the continuity of information security management in adverse situations, eg during a crisis or disaster';
- A.17.1.2 requires that an organisation shall 'establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation;'
- A.17.1.3 requires that an organisation 'shall verify the established and implemented information security controls at regular intervals in order to ensure that they are valid and effective during adverse situations'; and
- A.17.2.1 requires that information processing facilities 'shall be implemented with redundancy sufficient to meet availability requirements'.

We have already clarified that 'Information Security' requires the preservation of 'confidentiality, integrity and availability', but availability of what? Interestingly, neither ISO 27000 nor ISO 22301 define 'Information'. However, it is important to realise that this does not just pertain to digital data. Any organisation will have significant information assets; could this refer to paper, out-sourced activities, equipment or even people?

Reading the detailed guidance in ISO27002, it quickly becomes apparent that the organisation should ensure that 'information security is captured within its business continuity management process'. It further specifies that, where organisations do not have formal BC planning, then the organisation should 'assume the same information security requirements remain the same in adverse situations'. This then implies that separate processes are required for Information Security and business continuity, but that each should recognise the importance of the other, and should endeavour to include the requirements of the other.

So ISO 22301 or ISO 27001?

In summary, I would not suggest that either standard would give full reassurance for the other.

If you just want to go for the one certificate, then this would depend on the nature of your business, and the degree of reassurance that you want to give to your interested parties. If you deal with a lot of personal data, then ISO 27001 would probably be more of a priority, whereas, as a key supplier to Category One organisations (as defined by the Civil Contingencies Act 2004), you may find ISO 22301 more relevant.

Certainly, having ISO 27001 certification should provide reassurance that plans and procedures are in place to ensure the maintenance of Information Security during an adverse situation but the

extent to which this provides continuity would depend largely on what the organisation had defined as ‘Information’!

Conversely, having ISO 22301 in place will give some reassurance that Business Continuity is in place, but would not necessarily confirm that the maintenance of Information Security has been considered as part of this process.