Getting your house in order

Since the publication of BS25999:2 by the British Standards Institution in November 2007, the business continuity standard has sold faster than any other British standard to date. When one considers other well known standards, this is highly impressive and goes some way to demonstrating that business continuity is gaining greater recognition and credibility across the globe.

So, what can this level of interest be attributed to? Is it world events such as 9/11, environmental disasters like Hurricane Katrina or the 2007 floods in the UK, or is it just that our level of expectation for continuity of service and lifestyle is driving up this requirement? Well in truth, it's all of these and there is nothing to suggest that this interest in BCM is likely to dissipate any time soon. Governments and organisations alike are looking for a medium to instil a recognised and evaluated level of control over what they expect from their businesses and their suppliers.

To date, approximately 50 organisations in the UK and a further 50 in the rest of the world have become certified to BS25999:2. Whilst this is only a tiny proportion of the overall level of interest in the standard and representative of the initial flurry of interest that is seen with all new standards, it is significant in its own way.

The findings so far

Based on the assessments carried out on those organisations seeking compliance or certification under the standard, we have witnessed some interesting trends emerging. For example, there has been a tendency to focus more on the technical areas of business continuity (clause 4) rather than ensuring that all the elements of the management system have been fully implemented. Under-estimating the importance of determining what the necessary competencies are for BCM personnel has also been a recurring issue. Furthermore, in some instances there have been difficulties in ensuring that there is a meaningful link between the organisation's business objectives and their business continuity objectives and these are traceable through the business impact analysis and business continuity strategies.

At the core of every business continuity management system is the Plan-Do-Check-Act (PDCA) cycle, which all organisations must get to grips with if their plans are to be effective. This was added to BS25999: 2 in an attempt to be consistent with other management systems such as IS0 9001:2008, but to some the addition of the PDCA cycle simply adds an unnecessary layer of confusion to what for many is their first foray into the world of management systems. By linking it with the BCM Lifecycle it goes to show that there is an evolving cycle to the business continuity management system by following the phases of establishing, implementing, monitoring, reviewing, maintaining and improving business continuity.

The classic mistakes

So, what are the classic assumptions being made and pitfalls when dealing with compliance or certification and how can we overcome these?

- *Top heavy on documentation* – For those people who don't have experience of other management systems there may be a tendency to over-produce materials such as manuals, procedures, process maps and other documentation in the belief that this is what the auditor wants to see. Whilst documentation is a source of auditable evidence, BS25999 is very clear in stating what it expects. Where an organisation has a particular desire to produce more than what is required, this should be limited to practical materials. Business continuity plans have been known to run in to hundreds of pages (each!) and clearly are of limited practical use in the event of a disruption.

- *Why do we have to have written procedures?* – To ensure consistency of approach, some management system processes are required to be documented in the form of procedures. These tend to be along similar lines for each management system and for BS25999-2 are stipulated for just five elements: control of BCMS documentation and records (this may be combined into one procedure); internal audit; preventive action and corrective action. These procedures should be written in line with the requirements of the standard (in full) and be readily accessible for staff to read in particular should they be required to undertake any related BCMS activities.

- *The provision of BCM resources and determining competencies* – All being well, senior management will have identified what roles are required and who will fill them. This may be from existing staff or from a recruitment initiative, but either way there will need to be clear evidence of how this selection process took place and what competencies, skills and knowledge were considered appropriate for each role. These roles and responsibilities may be added to an existing job description or be added in an appendix. It is not sufficient to blame the HR department on "not getting around to updating the job descriptions" come the time of the assessment. And don't forget about defining individual authorities too, which is a classic mistake.

- *Auditing your own work* – If you work on a particular aspect of the business continuity management system on a regular basis, it stands to reason that you shouldn't be auditing your own work. Make sure that there is a clear line of independence throughout the audit process. You could call upon colleagues who audit another management system within the organisation, or, if not applicable, utilise others who are involved with business continuity but not the area which is to be audited. Just remember that you need to be able to demonstrate how you have selected this resource.

- *Avoiding confusion over what is BCM and what is BCMS* – BS25999-2 attempts to make a clear distinction between implementing business continuity arrangements (BCM) and a business continuity management system (BCMS). The one time that it is often confused is with the requirement to review the BCM arrangements through self assessment or audit (clause 4.4.3.3). This is not the same as the internal audit of the management system (clause 5.1) and an organisation must be able to demonstrate that it is reviewing both elements of the standard.

- *The need for action plans* – There are a number of different events that will require an action plan. Perhaps the most notable events are: a management review meeting; after an exercise or a real life incident; or an internal audit. Remember, preparing an action plan is only the start of the process. You need to monitor activities to ensure that actions are completed, chase if necessary and then review the actions taken and determine whether they have been effective or not. This takes you into the corrective and preventive action requirements of the standard as well as being very credible evidence of continual improvement.

- *Applying for certification too soon* – Understandably, organisations are keen to invite the auditors in as soon as the ink is dry on the BIA and the BCPs. However, it is important to remember that to qualify for BS25999-2 certification you have to be able to demonstrate that your business continuity management system is fit for purpose. This means not only ensuring that have all of the requirements have been met, but also that the management system has been sufficiently embedded into the organisation to give the certification body confidence in it. Typical evidence of embedding would include: internal audit results; management review meeting minutes; exercises and experiences learnt from any real life incidents.

- *Scoping your BCMS* – It is surprising how many organisations enter into their BS25999-2 preparations without having clearly identified the scope of their business continuity management system. Should they include all of their products and services? Are only some of them considered 'key' and is there any benefit from phasing implementation based on some form of business prioritisation? Experience shows that for larger organisations which may have multiple sites, possibly over different continents, a phased implementation is the best way to proceed, possibly by identifying a particular product line or service. For smaller companies with only one or two sites located in the same region, the decision may be taken to adopt a 'big bang' approach to certification. There is no right or wrong approach, but it is important to be mindful of the resources at your disposal and what the business drivers are for certification.

Top 10 tips for implementing BS25999-2

1. Obtain a copy of BS25999 Parts 1 and 2 and read them (yes, really!)
2. Implement your management system alongside your business continuity arrangements and select the best way of communicating it to staff
3. Appoint a BC sponsor at the outset and gain top management commitment to implementing BS25999 within the organisation (and the resources to do so)
4. Consider the scope of your BCMS carefully and clearly define the boundaries
5. Determine BCM competencies adequately
6. Make sure that the extent of the BIA is appropriate to the size and complexity of the organisation
7. Ensure that risk assessments are based on threats specific to the organisation and its critical activities as well as universal threats such as fire and flood
8. Follow the management review inputs and outputs in the standard rather than making up your own agenda
9. Ensure that the BCM culture is sufficiently embedded into the organisation before inviting the auditors in
10. Remember, BS25999-2 is about continual improvement. Rome wasn't built in a day

And finally, consider the benefits of undergoing a gap analysis before formal certification to BS25999-2. It's an ideal way of identifying any shortfalls in your system and by addressing them at this stage it should make the certification process significantly smoother.