

BS 25999: KEY ISSUES TO ADDRESS FOR CERTIFICATION



AUTHOR: Malcolm Cornish, FCA, FBCI, operations director Continuity²

ABSTRACT: BS 25999-2 (Part 2 - the Specification) was issued in November 2007. Since that time many organizations have been certified and UKAS (the United Kingdom Accreditation Service) has been assessing the audits undertaken by certification bodies as part of its process towards accrediting these bodies in respect of BS 25999.

As a result of all these activities, BS 25999-2 is coming under the close scrutiny of organizations being certified, the certification bodies and UKAS. The overall consensus is that BS 25999-2 has been constructed to a very high standard and has generally been very well received by these three groups. As with any new standard, there are inevitably some areas of confusion and misunderstanding and there are aspects of the standard that are more difficult to comply with than others. In this paper, the author will address the following:

- Management system requirements
- Business impact analysis.

Detailed considerations

Management system requirements

There is a big difference between implementing business continuity management (BCM) and establishing a fully effective business continuity management system (BCMS). This became clear to BCM Committee Panel 2, which had been given the responsibility by the British Standards Institution to create BS 25999-2. As one of the ten or so actively involved in the panel, I quickly learnt that there were many aspects of a management system that are quite onerous and demand disciplines beyond the normal approach of BCM practitioners.

In particular, the aspects that seem to have caused the most difficulty relate to:

- Competency of personnel (BS 25999-2: Clause 3.2.4)
- Documentation and records (BS 25999-2: Clause 3.4)

Thankfully, we had experts in management systems who were able to combine and improve on the text from other management systems standards in order to set out precisely in BS 25999-2 what is needed. Close reading of the text is all that is required.

Competency of personnel

3.2.4 The organization shall ensure that all personnel who are assigned business continuity responsibilities are competent to perform the required tasks by:

- *determining the necessary competencies for such personnel;*
- *conducting training needs analysis on personnel being assigned BCM roles and responsibilities;*
- *providing training;*
- *ensuring that the necessary competence has been achieved; and*
- *maintaining records of education, training, skills, experience and qualifications.*

Documentation and records

There are a number of facets that need to be addressed. As well as identifying all the different documents that are required in respect of the work undertaken (all have a reference to relevant clauses) the standard also requires that:

3.4.1.2 Records be established, maintained and controlled to provide evidence of the effective operation of the BCMS

3.4.1.2 Documented procedures be established in order to identify the controls over BCMS documentation and records

For records:

3.4.2.1 Controls shall be established over BCMS records in order to:

- *ensure that they remain legible, readily identifiable and retrievable; and*
- *provide for their identification, storage, protection and retrieval.*

For documentation:

Controls shall be established over BCMS documentation to ensure that:

- documents are approved for adequacy prior to issue;
- documents are reviewed and updated as necessary and re-approved;
- changes and the current revision status of documents are identified;
- relevant versions of applicable documents are available at points of use;

- documents of external origin are identified and their distribution controlled; and
- the unintended use of obsolete documents is prevented and that such documents are suitably identified if they are retained for any purpose.

Business impact analysis

Before BS 25999-2 arrived, you could talk to thirty business continuity practitioners and get forty different explanations of what is meant by the term 'business impact analysis' (BIA). Thankfully BS 25999 (identically in both parts 1 and 2) sets out the definition of a BIA and identifies its fundamental requirements. However, there still appears to be confusion surrounding the BIA and it is rare to find examples of BIAs that have been conducted in full compliance with BS 25999-2.

Understanding of the terms MTPoD and RTO

There appears to be a great deal of confusion surrounding the newly introduced term 'maximum tolerable period of disruption (MTPoD)' as defined by the standard and its relationship to the term recovery time objective (RTO). Part of the confusion is of the standard's own making. In the terms and definitions, maximum tolerable period of disruption is defined as:

Duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed.

This suggests that MTPoD is attributable to the organization as a whole. In the body of the standard, there is, however, no reference to MTPoD in relation to the organization as a whole or individual products and services.

The next reference to MTPoD is in the definition of recovery time objective, which BS 25999 defines as:

Target time set for resumption of product, service or activity delivery after an incident

NOTE The recovery time objective has to be less than the maximum tolerable period of disruption.

This suggests that MTPoDs are applicable to products, services and activities. There is, however, no further reference in the standard to MTPoDs in respect of products and services.

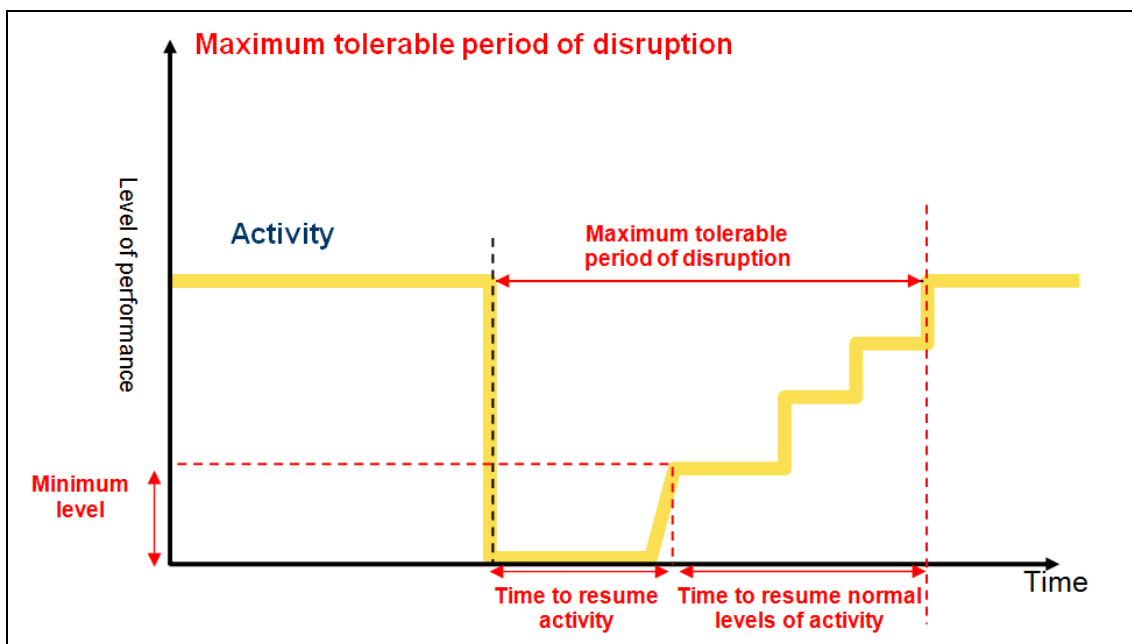
The only other reference to MTPoD is in relation to individual activities under the heading business impact analysis (clause 4.1.1), where the requirement is for the organization in relation to ALL activities to:

Establish the maximum tolerable period of disruption for each activity by identifying:

- the maximum time period after the start of a disruption within which each activity needs to be resumed;
- the minimum level at which each activity needs to be performed upon resumption; and
- the length of time within which normal levels of operation need to be resumed;

There is also a restatement that RTOs for critical activities must be within their MTPoDs.

The diagram below sets out my interpretation of MTPoD:



In order to determine the 'maximum time period after the start of a disruption within which each activity needs to be resumed', the standard requires the organization to:

Identify impacts resulting from the disruption to these activities, and determine how these vary over time

Based on my experience, it is very common for organizations not to do this. Many fall into the trap of setting a recovery time objective for each activity without full reference to impacts over time, and then call it the MTPoD without considering all the MTPoD components that the standard requires. The training material issued by the Business Continuity Institute in support of its five-day training course compounds the confusion by stating that the MTPoD is the point at which the activity needs to be resumed.

As well as determining the 'time to resume activity', some thought needs to be given to defining the level of performance at resumption (e.g. number of personnel, manufacturing throughput, invoices produced) and determining the time required to return to normal levels

of activity. My belief is that the standard is not looking for a scientific calculation of the latter (BCM is not a science) but is just looking for an indication from someone that understands the activity.

Steps required for full BIA

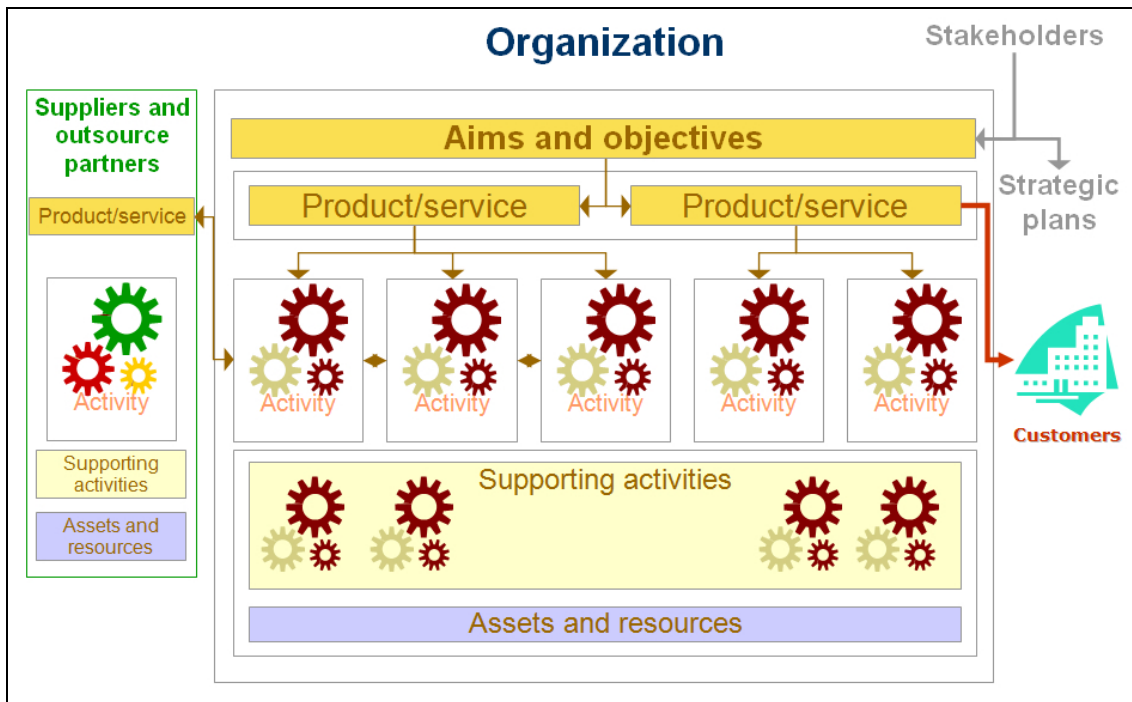
The standard is very specific as to all of the requirements of a BIA because of each requirement's individual significance to the validity of the BIA and consequently, the entire BCM process. As well as identifying critical activities, the BIA enables the organization to obtain consensus as to the order in which activities not identified as critical should be recovered in order to minimise the impact on the business. Failure to establish the MTPoD (including all its components) and use the information to prioritise all activities is likely to result in problems when a major incident occurs.

In essence, all the requirements of the BIA are linked in a chain. Failure of any of the links may jeopardise the validity of the BCM arrangements for critical activities and will almost certainly prevent the appropriate treatment of other activities during a major incident.

Because BCM arrangements and plans have to be put in place for critical activities, they come under closer scrutiny as the BCM process continues. The Standard does not, however, require further examination of the remaining activities, some of which may become 'critical' surprisingly quickly during an incident. If an organization does not use the BIA to gather key information, agree the impact implications and document them in an appropriate manner, the next opportunity will be when an incident occurs and there is not enough time to get it right.

Definition of RTO

In the terms and definitions of BS 25999-1 (which were intended to be identical in Part 2, apart from terms not used), the definition of RTOs extends to IT systems and applications. I would also contend that RTOs are required for all supporting elements required for the resumption of activities (supporting activities, products and services supplied by suppliers and outsource partners, assets and resources) as shown in the diagram below:



Conclusions

Management system requirements

The standard is very explicit and clear as to additional requirements of a management system. There is additional cost and effort involved in creating a BCMS and obtaining certification as opposed to just implementing effective BCM. Organizations should therefore make sure that there are sufficient benefits in achieving certification before embarking on that course of action.

Business impact analysis

The BIA requirements set out in BS 25999-2 are to my mind extremely sound and workable. There is considerable confusion surrounding the *maximum tolerable period of disruption* (MTPoD), so something needs to be done about it.

MTPoD could be retained as a term that relates to the organization as a whole or individual products and services. It is for example useful for management to express a view as to how sensitive the organization is to disruption and use this as an indicator of the level and extent of planning that would be expected. The difficulty is that I do not have a clear idea as to how it could reasonably be determined.

The 'activity' MTPoD (using my interpretation) is unnecessary. Its components are defined, so the requirement for a name is superfluous. Some may chose (as does the BCI) to use the term to describe the 'time to resume activity' in the MTPoD diagram above. The only other references to MTPoD are in relation to RTOs, which must be within it. If you go along with my explanation of MTPoD, this requirement is only saying that you must recover the activity within the time that you have determined it must be back to normal! All practitioners would I am sure agree that once you have determined on an 'impact over time' basis the latest time at which an activity must be resumed in order to avoid unacceptable impacts, you must set its RTO within that. The RTO will be influenced by other factors (e.g. dependencies, lead times for essential equipment, backlog issues) so could be significantly sooner than the time determined based on impacts.

The obvious conclusion is to define a new term TWWAMBRAULI being 'Time Within Which Activity Must Be Resumed to Avoid Unacceptable Levels of Impact'unless of course someone can come up with something snappier!

Author



*Malcolm Cornish, FCA, FBCI, operations director , Continuity²
malcolm.cornish@continuity2.com*

Malcolm has specialised in business continuity management for the past nineteen years dealing with all aspects of business continuity management in most business sectors. He is a Fellow of the Business Continuity Institute (FBCI) and has played an active role in the development of the institute from its inception. He is currently a member of the BCI Audit Committee and on the BCM committee of the BSI that is responsible for BS 25999. Malcolm develops and leads Continuity² training courses, is a regular conference presenter and has published many articles and papers to promote awareness and understanding of business continuity.