

Recertification of your Business Continuity Management System

In this article I demystify the process of recertification; the procedure undertaken by certification bodies every third year in the cycle of management system certification. I identify how an organisation should prepare and the process of recertification itself. Is it just another audit or is there more to it?

If your organisation has a certified business continuity management system (BCMS) you will know in order to retain it, your certification body will carry out periodical audits. You will also know that when you first achieved certification and were issued with your certificate, it had an expiry date on it, three years hence*. What are the implications of this expiry date and how should you prepare for “renewal”? For those of you who have held BCMS certification for some time, the chances are that you started out with BS 25999-2 certification, transitioned to ISO 22301 over the last year or so and have, or are approaching, your first, if not second, recertification audit.

Apart from the duration of the recertification audit being longer than a surveillance audit, most organisations don't seem to pay a great detail of attention to the significance of what they are about to go through. At best it's likened to going through the initial assessment again and at worst, it's just another audit. I believe if organisations had a clearer understanding of its intent, they might plan for recertification in a more structured and focused way. After all, achieving successful recertification is not a given and should be worked at.

Why is recertification important?

Recertification is the opportunity for the organisation to demonstrate to its certification body;

- Its BCMS is still functioning, in its' **entirety**, in the way it was originally intended, incorporates the products, services and locations (otherwise referred to as the “scope”) as initially assessed (or subsequently amended to)
- Its BCMS continues to be compliant and **effective**
- Its BCMS continues to **improve** in order to meet its the purpose
- Its BCMS continues to support the ongoing achievement of business objectives

It's also the chance for the organisation to review its BCMS and take stock of its ongoing relevance and accomplishment and communicate its findings to interested parties, as appropriate.

The method by which these requirements are assessed is two-fold. First the auditor will review past performance observed during surveillance/other audits and second, they will assess how the organisation sees the future of its BCMS and where this sits within the company's business strategy. It's for this reason that Senior Management should be involved with recertification in order to demonstrate ongoing support and commitment.

If we take each of the yardsticks stated above (in bold), it's important to understand exactly what is expected of the organisation. To assess whether a BCMS meets its purpose in its **entirety**, or as a whole, the auditor looks for comprehensive evidence that the system is functioning in a cohesive and efficient way. Do all parts of the system work together and feed in as one? Is it under control and producing the results and benefits originally anticipated? How does the organisation know whether this is the case? A broader review, every three years is an ideal opportunity for both internal and external parties to step back and take a rounded view of the system and if necessary, plan changes.

How do you assess the **effectiveness** of your BCMS? This has been made easier with the introduction of performance evaluation requirements but you still have to decide the best ways of measuring the BCMS. You establish the metrics you want to evaluate and then review the findings to determine whether the BCMS has achieved its purpose and objectives. This sounds straight forward (and it is) but the triennial review gives management the opportunity to step back and analyse performance and effectiveness. It might sound obvious but evidence of *ineffectiveness* is quite easy to spot, if you are only willing to look. Outstanding nonconformities, not identifying the root cause of problems, exercises not meeting set objective/s and repeated absenteeism from management review meetings by key individuals (to name but a few) would all give the auditor a sense that all was not well with the BCMS.

All management systems include the requirement for **improvement**. Easier said than done, perhaps. Improvement happens over time and unless it can be seen from results of a specific project, is best considered through the periodical review of processes and procedures and with a questioning mind. The three year recertification process is an ideal opportunity to remind yourself of the improvements achieved and to demonstrate to the auditor (and senior management team!) just how far your BCMS has developed and matured, in that time.

If, as part of the recertification process you are unable to demonstrate improvement, do you really deserve to retain your certificate? That's the view an auditor (should) take. To put this into context, if your organisation cannot realistically justify the recertification of its BCMS, it will be given time to address shortfalls and step up its game. This is no different to raising major nonconformities during an audit and as long as you can demonstrate genuine intent and corrective action, you should retain your certificate, but you can't afford to be complacent.

How should you prepare for recertification?

Get your BCMS house in order. This might include:

- Address and close outstanding nonconformities.
- Ensure your exercise programme is up to date and reports are complete.
- Check all internal audits have been fully closed and any follow up audits are complete.
- Where applicable, demonstrate you have learned from previous exercise and audit scheduling methods.
- Have you reviewed your BCM procedures in line with your documented timescales and is there evidence of maturity, over time?
- Ensure the last management review meeting you held considered the effectiveness of your BCMS and that the outcome of this discussion is clearly documented. (You should be going this anyway).
- Be in a position to demonstrate the improvements achieved both to the business and directly through the BCMS.
- Ensure staff have been given the tools and support to develop their understanding for the importance of the BCMS and its relevance to their role. Involvement in exercises and tests, will help with this.
- Make sure your Business Continuity Policy and Objectives are current and relevant. There's nothing worse than seeing a stated objective which was achieved some time ago. (For example, to achieve BS 25999 certification)!

How long does recertification take?

Generally speaking, you should assume a similar duration to your initial certification audit. This may vary if you have revised the scope during the three year period or have added or subtracted significant staff numbers from scope so it's best to check with your certification body before agreeing audit dates.

The audit will include a detailed plan of areas to be covered but very often, certification bodies will include a schedule of audit plans covering the entire three year audit cycle, as part of their surveillance audit reporting. Expect to be asked questions about how the BCMS has evolved over time and be prepared to demonstrate how staff and management have matured in their BCMS experience and familiarity with procedures. A system which may have originally been the domain of a handful of individuals needs to be fully owned and managed by a much broader collection of individuals/teams and if this cannot be shown to be the case, the auditor is well within their rights to ask why.

If shortfalls are identified the auditor will raise nonconformities in the usual way. If corrective action/ a follow up audit is required before recertification can be recommended, the onus will be on you to ensure the appropriate action is taken and evidence of this provided to the auditor. Because of this possibility, it is always wise to ensure your recertification audit is carried out in good time prior to expiry. Certification body audit

report reviews can take a number of weeks and recertification isn't confirmed until this review is complete and the new certificate issued.

Conclusion

Recertification audits, whilst taking longer than you may like, are a useful benchmarking exercise for your BCMS. It is the chance for you to take a good look at your procedures and (hopefully), communicate to the business that the BCMS remains fit for purpose and continues to meet the needs of the business. It's also an opportune time to go out to external interest parties and let them know that you have been recertified for another three years!

* This article is based on UKAS accredited certification body requirements. Non accredited bodies may operate different practices.

Hilary Estall, MBCI and IRCA BCMS Lead Auditor is Director of Perpetual Solutions Limited, a business continuity and management systems consultancy practice.

www.pslinfo.co.uk