perpetual solutions

Getting the most from your BCMS audits

Are you responsible for auditing your company's business continuity management system? Do you struggle to fit your audits in to your "day job" and do you wonder whether your audit report and its conclusions will make a difference to the robustness of your business continuity arrangements? This, it seems, is quite normal.

Hilary Estall, IRCA Lead BCMS Auditor and seasoned management system consultant offers a few ideas to help bring life back to your audits.

Whether you choose to conduct internal audits of your business continuity arrangements and/or management system (BCMS) to ensure they continue to meet business needs or whether this is a mandatory activity because you are certified to ISO 22301 (or similar Standard), internal audits are an invaluable source of information and opportunity to find out what's working well and what could be improved. It's a business opportunity. In turn, with greater emphasis now put on leadership and management commitment in management system standards, your directors should be jumping at the chance at getting an insight into how the business continuity plans will work, if used for real, as well as supporting the audit process.

With everyone's time being so precious, you need to find the best way of developing an audit programme which, over time, assesses both compliance and effectiveness of your arrangements. Compliance comes with being certified to, or aligned with, a Standard such as ISO 22301, but all too often, takes over the focus and attention of an audit and prevents the auditor from thinking outside the box. Ideally, you need two hats when auditing.

Compliance versus Effectiveness

Whilst assessing compliance is straight forward; something either meets a requirement or it doesn't, determining the effectiveness of an activity or process and how the business might respond, is less straight forward. But it doesn't have to be. If you, as the auditor, have a good understanding of how the business operates, its strategy and governing principles, what you identify during an audit should be able to be translated into "effectiveness" based on company expectations and established business continuity principles.

How you, as the auditor, respond to compliance issues can make or break the company's faith in the audit process and once broken, is very difficult to regain peoples' trust and faith in the process. If you identify a non-compliance or nonconformity, you should assess its severity and impact on the BCMS and the business, overall. Don't over react when you find a single instance of, for example, a Business Impact Analysis having missed its review date, but look at the bigger picture; what controls are in place to ensure the review programme is properly established and followed and was this a single lapse or might it direct you to a more

significant problem? Only delving a little deeper will you be able to assess the true position. Of course, if it turns out to be a more serious issue, you should formally raise your findings. Be pragmatic in your assessment of the evidence.

Determining the effectiveness of your BCMS requires a little more consideration. No nonconformities doesn't necessarily mean the system is operating effectively. It simply demonstrates compliance with whatever standard you are assessing it against. What will give you the assurance the Plans will work if invoked and how can you be sure staff know what is expected of them during an incident? You need to be able to interpret outcomes. For example:

- Was the exercise programme sufficiently challenging and far reaching? Did it indicate a suitable level of awareness of plans, or strategies which seem appropriate to meet business objectives?
- Is the mechanism for identifying and managing risks appropriate? Is there a process which encourages staff to raise issues within their part of the business and be considered through a systematic assessment process?
- Does the Executive Team have a role in reviewing the performance of the BCMS and take steps to ensure issues identified are dealt with swiftly and appropriately? Is it working?

Assessing effectiveness is about challenging audit findings and determining to what extent business activities are being achieved and therefore supporting the achievement strategic objectives.

Audit Programmes

Do you find yourself re-running last years' audit schedule and adopting a similar approach to each audit? It's quick and easy and keeps the external auditors at bay.
We know audits should be planned based on business risks, the priority of processes and of course, results of previous audits. However, do you approach each new audit schedule with a fresh pair of eyes, considering the current status of the business and even its current strategic objectives? This is where you should start each audit schedule. Businesses are forever changing and responding to new challenges so surely it would be helpful if your internal audits focused on these new aspects, as well as the old chestnuts, of course. Think laterally and if nothing else, ditch any thought of auditing by clause number!

Auditing Skills

Mention has already been made of approaching audits in a pragmatic way. Whether you audit on a regular basis or only once or twice a year, it's good to take a moment to think about how you come across to an auditee and to re-assess how your audits are received. Here are a few tips for keeping your audits on track:

- Engage the auditee in conversation and keep your questions mostly open and definitely non-confrontational. Retain eye contact and show interest in what the auditee is saying;
- Listen out for subtle pieces of evidence offered up during the audit, consider their impact and utilise as appropriate;
- Rather than decide what questions to ask in advance, allow your questions to develop organically during the audit, whilst retaining control over the audit scope; and
- Be decisive with the information offered and dig deeper if you think necessary but equally, be able to move forward without labouring an issue of no material consequence.

Reporting your Findings

Providing prompt feedback to auditees and their line managers is important. Ideally, you should convene a formal meeting to do this. There shouldn't be any surprises at this stage, having discussed issues as they arise during the audit. Try and balance your feedback. Start with your overall conclusion of the audit and the general status of the BCMS followed by any positive findings. It's too easy to go straight into discussing the negative issues and not offer praise for what is being done well. You can then discuss specific findings and agree a suitable action plan.

A written report should follow within a reasonable timeframe (to retain engagement and focus). Your language should be neutral and the report itself should be factual. Any corrective action discussed at the closing meeting would be included and where appropriate, arrangements made for a follow up review of the action taken to determine effectiveness and to close out the audit. Leaving a follow up review until the next audit risks the action being overlooked or ignored.

Engaging with Directors

Ideally, your directors will already be showing interest in the outcome of audits but if not, it's important they are given the opportunity to review the findings and drive improvements. Provide them with useful information, not just headline numbers of nonconformities and how many remain open. Dig deeper and provide trend analysis and point to any areas of particular concern and seek their input into solutions.

As the auditor, you are the eyes and ears of the business and have a responsibility to ensure the business leaders understand whether the BCMS is working well or is in need of additional support. After all, directors need to be confident the business can robustly combat the impact of a disruptive incident.

Conclusion

For most people, conducting internal audits are an add-on to an already busy schedule. If you can view them as an opportunity to identify improvement to your business activities and even respond in a smarter way to an incident, you will be delivering a huge benefit to your company and that has to be good for your job satisfaction!

Hilary Estall MBCI, IRCA Lead BCMS Auditor and Director of Perpetual Solutions.

If you would like to explore any of the aspects discussed in this article, help with re-energising your audit programme or formally train as an auditor, please contact Hilary at enquiries@pslinfo.co.uk or via www.pslinfo.co.uk