perpetual solutions

So you think you’re an auditor?

You are implementing a business continuity management system (BCMS) for the first time and you discover that one of the requirements is to conduct “internal audits”. What do you do? Who should be the auditor? Do they need to be trained? All valid questions (along with scores of others which you will doubtless ask yourself) which invariably will be rushed through without much thought into what is trying to be achieved (apart from a tick in the BCMS/certification box).

Done well, audits are an excellent way for your business to learn what’s working and what needs to be improved but done badly they soon become robotic and worse, potentially divisive. Internal audits are a requirement of any management system standard so if you are committed to implementing a meaningful BCMS you might as well do it properly from the outset.

Who should read this article?

Whether you are responsible for identifying and training the soon to be in post auditor or you have just found out that your role has been extended to include internal audits then this article is written with you in mind. Over and over again I come across situations where internal audits have been tagged onto someone’s existing job description (for a variety of reasons) and after a few days on a training course the “internal auditor” has been let loose on the company. A terrifying prospect for most first time auditors and a very naive approach by management.

If you haven’t already guessed it, this is a subject close to my heart and with the recent publication of ISO 22301 and renewed thoughts of BCMS implementation on many organisations’ agenda, a timely reminder that there is more to internal BCMS audits than simply attending a training course.

What is an audit and why do we conduct them?

An audit (in the eyes of management systems) is defined as a **systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.** This definition is taken from BS EN ISO 9000:2005 Quality management systems - Fundamentals and vocabulary and used in ISO 22301 amongst other management system standards (MSS) and why not? It’s succinct (for a MSS definition) and is understood across a number of MSS disciplines. I could write paragraphs on what an audit should look like but taking this definition literally we understand that;

- It must be *systematic*, in other words, repeatable in form. This will provide a consistent approach to auditing and ensure that whoever conducts the audit, the approach used will be constant.

- It must be *independent*. To be of use, the auditor must be impartial and have no direct link to the area being audited. Independence also extends to being unbiased and fair in judgement.

- And finally, the audit must be *documented.* To be a complete process the documentation starts with the planning phase (agreeing the scope of the audit), continues with the evidence obtained during the audit and does not complete its documentary obligation until the actions from the final (documented) report have been carried out, reviewed and closed by the auditor, at some predetermined date in the future. Thereafter, we are told that the audit evidence must be *evaluated objectively* in order to *determine whether the requirements of the standard* (audit criteria) *have been met.* Taken literally, you will agree, the internal auditor is being given responsibility for assessing the performance of the business and taking a tactical stance in operational improvement. Not something assigned to an individual without careful thought, you would hope.

The fundamentals of a well executed audit

Conducting an audit requires having a clear brief (audit scope) as well as asking pertinent questions in the right way. Planning the audit and communicating its scope and intent to the auditor beforehand is crucial if they are to understand what it is they are expected to assess; this doesn't mean having a checklist of pre prepared questions which must be rattled off as quickly as possible.

The auditor must be given the authority to ask searching questions of those who may be senior to them. In turn, the auditor must be confident to do this as well as judge whether the response (and supporting evidence) meets the audit criteria and where it doesn't, to raise the issue in the appropriate manner. Having asked a question the auditor must wait for a response. They shouldn't be tempted to fill silences with suggested answers or move on to the next question until the respondent has had both time to think or the question asked of them in a different way, if necessary. In short, it is down to the auditor to look and listen and ensure that the auditee understands what is being asked of them. Misunderstandings are a common cause of nonconformities and subsequent bad feeling between parties and are easily avoidable.

The extent to which an auditor should sample an activity comes with experience. Never continue sampling on the pretext that sooner or later you'll find something wrong. Judge what seems to be a fair sample and form an opinion from there. A competent auditor will soon know whether a problem exists.

Communication between auditor and auditee is vital. I've already said that misunderstandings can result in the raising of unnecessary nonconformities and the auditor needs to be able to communicate their expectations to the person they are auditing in a clear and non confrontational way. If they can see the auditee is struggling they have a duty to ask the question in a different way, not simply mark it down as a failure. The same goes for feeding back audit findings afterwards. Not only should these be backed up by specific examples but they should be accepted by the auditee and communicated to relevant management. Commitment to taking appropriate corrective action is necessary and should be agreed between parties before the audit is concluded.

Timely review of actions remains the responsibility of the auditor, even if this is several weeks or months after the original audit. This can be a challenge when fitting audits in around other workloads but should not be left until the next audit, which could be a year away. Ongoing focus and importance placed on audit actions will make sure appropriate commitment and ownership is maintained.

Core competencies of a management system auditor

The competency requirements of an internal auditor are no more or less relevant when determining BCMS competencies, required by ISO 22301 (and BS 25999-2) but it's surprising how often this role is overlooked by organisations. It's up to the business to determine such competencies but you can see from what I've said in this article, that there are certain "soft" skills which are as necessary (and sometimes more so) than a knowledge of auditing or BCM specifically.

Whilst the size and complexity of the organisation might dictate, in part, the competency requirements of the auditor, this is not an excuse to hold back on making sure the best person is allocated the role. Setting aside for a moment professional training requirements, personal qualities indicating a potential candidate include a tendency towards diplomacy, pragmatism, decisiveness and having an open mind to what is being discussed. Many more exist but to some extent these may be driven by the culture of the organisation.

As for professional training, the organisation (and prospective auditor) should be clear what it is they wish to gain from this. So often new auditors are sent on the wrong training course and come away bewildered, demoralised or simply unclear how they will translate what they have been taught into practical auditing skills. How many auditors have heard of, let alone read, BS EN ISO 19011:2011 Guidelines for auditing management systems? It should be on the pre course reading list of every auditor course but it's not!

The International Register of Certificated Auditors (IRCA) is where every professional auditor should aim to be professionally approved. It's the only independent assessment process for auditors, be they internal auditors, auditors or lead auditors and demands an ongoing commitment by the individual to develop their auditing skills through continual practice and professional development. Membership of IRCA means you can be taken seriously as an auditor, and not before, in my opinion.

Does ISO 22301 demand more from the audit process?

Those of you already familiar with ISO 22301 will know that greater emphasis is placed on managing the results of internal audits than in BS 25999-2. As with other new or revised requirements in the international standard, the weight of a BCMS now focuses more on the effectiveness and relevance of it both in terms of meetings the organisation's objectives as well as the needs and expectations of interested parties. What better way of determining this than by conducting your own internal assessment of your performance? Any third party auditor worth their salt should be assessing an organisation's internal audit capability in a slightly different light, going forward.

Are you getting what you want from your third party auditor?

Talking of external auditors, those jolly people who turn up to audit your management systems from certification bodies (I am one of them), have a lot to live up to. Since the launch of BS 25999-2 there have been several "issues" between client and auditor with expectations not being met. Many third party auditors do not conduct BCMS audits very often, are not business continuity professionals (understandably) and can come across as indifferent to the nuances that every BCMS displays. They too would do well to read this article!

If you only take one message away from reading this it should be; make sure you know what you want from your internal audits and you have the best people carrying them out for *your* business.

This is just the tip of the auditing iceberg. If you think you could be getting more from your BCMS audits Hilary Estall SBCI of Perpetual Solutions Limited will be pleased to carry out an Audit Health Check on your auditing arrangements and work with you to maximise the benefits of internal audits on your BCMS.

For more information or to find out where you can buy a copy of Hilary's "practical and insightful" book Business Continuity Management Systems; Implementation and Certification to ISO 22301

contact Hilary at hilary.estall@pslinfo.co.uk or www.pslinfo.co.uk perpetual solutions

Hilary is an IRCA registered BCMS Lead Auditor. For more information about becoming a certificated auditor visit www.irca.org