# ISO 22301 – BCMS audit results and what they tell us

*Hilary Estall MBCI, IRCA BCMS Lead Auditor takes a look at how organisations are faring with their BCMS audits and what, if any, trends are appearing.*

## Introduction

ISO 22301 has been in circulation for approaching two years but the uptake for third party certification remains at a steady crawl. Why is this? As with many other management system standards, there will be some organisations keen to be amongst the first to obtain certification and maximise the associated benefits, but for most, there will need to be an external factor to influence the decision whether to seek formal certification. ISO 22301 is no different.

That said, a number of organisations have taken the initiative and now benefit from a business continuity management system which not only stands up to the scrutiny of an independent auditor (which let's face it can vary in its worth) but more importantly, offers assurance that should the worst happen, the business (or part covered by BC arrangements) stands in good stead for riding the storm.

So, what can we learn from those who have already dipped their corporate toes into the water, otherwise known as ISO 22301? This article draws on my personal experience both as an auditor (one of the tough ones!) and a BCMS consultant and tries to get underneath what might be holding your BCMS back.

## Top Trends

Whilst ISO 22301 may have been out for a while it takes time for meaningful trends to be identified. Most certified companies will be audited by its certification body once a year (not the six monthly cycle undertaken for a number of other management system standards). We are therefore only seeing the early birds go through their first surveillance audit, following transition from BS 25999 or initial certification. Never the less, certain tendencies are showing themselves. Here are the most frequent ones I have come across.

## 1. Increased focus on Planning has not materialised

Taking the familiar Plan Do Check Act (PDCA) model, it appears to have escaped people's notice that ISO 22301 is made up of seven core requirement clauses, *four* of which (or 57% for those of you who like statistics) relate to the Plan phase. This is no coincidence. Following the introduction of Annex SL (the realignment of management system standard requirements and terminology), emphasis on planning your management system is considered key to its success. So, why aren't we seeing this in the development of a BCMS?

Whether it’s understanding where your organisation sits within its industry or marketplace (referred to as “context”), developing meaningful business continuity objectives, supplying adequate and appropriate resources for the BCMS or considering what might prevent your BCMS from meeting its objectives (these are different from your BC objectives), your BCM team should be spending significant time considering each of these points (as well as the others specified in the standard). How else will your business fully appreciate why it’s developing a business continuity management system and what might throw it off course?

## 2. Presenting the information

The introduction of new requirements and terminology is causing some confusion about how to present this information. It also sometimes begs the question; who is this being written for: The business or the external auditor? For the purposes of making this point, I recommend you ignore the auditor and their expectations!

At this stage I think it would be helpful to remind readers of three terms and their definitions used in ISO 22301;

**Document –** information and its supporting medium (can include paper, electronic or photograph)

**Documented Information –** information required to be controlled and maintained by an organisation and the medium on which it is contained (can be in any format or on any media)

**Procedure –** specified way to carry out an activity or a process

*Source BS ISO 22301:2012*

**Documented Procedure –** whilst not formally defined, it’s used in the standard and its meaning (and expected application) needs to be understood. An example is the business continuity plan being described as a documented procedure. Remember, not all procedures have to be “documented”.

I have already mentioned “context of the organisation” and I’m going to again as it’s a good example of where implementers struggle to know how best to present this information and still meet the requirements of the standard.

Firstly, the standard expects you to “document” this information. It’s not asking for a procedure and can be presented in any way you consider appropriate. My advice is to consider a pictorial description. After all, the word *context* means a framework or perspective of something. As long as you can also verbally describe your “picture” it’s more likely to strike a chord with staff and help them understand where your business sits in the grander scheme of things. So, have a go at unleashing your creative side and see what you come up with! I’ve seen some great illustrative interpretations as well as some dire written explanations.

Another example of where implementers can struggle is identifying the most suitable method of demonstrating how they have considered "actions to address risks and opportunities" of the BCMS. The standard merely expects they will *determine* this information and then put arrangements in place to address issues identified. How should you demonstrate your musings; Meeting minute?  Brain storming flip chart? It doesn't matter as long as you follow it through with ACTION (and the ability to demonstrate this action).

## 3. Demonstrating Leadership

We are used to the expression "management commitment" in management system standards. Typically seen as the nominated senior manager trying hard to convince the auditor (and less so the staff), that they are committed to the XYZ management system and all the good things it will do for the business. A cynical view point of mine but after more than 16 years auditing, it's a valid one! So, why has *leadership* been introduced via Annex SL and does it expect anything different from the management team? I'd like to believe it adds an extra layer of support to a management system but evidence to date does not back this up.

We often read about what makes a good leader? I might suggest the following traits; being supportive of others and the ability to permit others to take ownership and responsibility for something. To invest and believe in someone's ability to do a good job. How could this manifest itself in the context of a BCMS? As an auditor I would be looking for the provision of suitable and adequate resource to implement and maintain the BCMS and to allow that resource sufficient "space" in which to develop their role and function. Other examples of leadership might include owning a particular BC objective (leading by example) or actively participating in an exercise or test (this is actually stated in the standard now, which is great). Effective leadership should be assessed in its entirety during an audit (internal or external) and a conclusion drawn at the end of the audit.

## 4. Setting SMART Business Continuity Objectives

The expectation that BC objectives will be useful to the organisation has been raised significantly. Not only do these objectives have to be meaningful and relevant they now have to be allocated to an individual/function or team (however you deem most appropriate) and actually measured and reported on. Gone are the days when you could indicate something to do with the BCMS was important and then go on to completely ignore it. BS 25999 didn't go far enough in terms of follow through and accountability.

This requirement is found in the Planning clause and will feature in all revised and new management system standards working to Annex SL principles. If you can master the art of developing SMART objectives for your BCMS, they should easily follow for other standard/s you work to. (SMART stands for **S**pecific, **M**easurable, **A**chievable, **R**ealistic and **T**imely).

Evidence is showing me that organisations are struggling to do two things;

a) set meaningful and measurable BC objectives and
b) assess whether the objectives have been met

I believe that some are over thinking this requirement and therefore tying themselves up in knots. You don’t need to. I suggest you take a step back and consider why you are doing all this work. For example, is it to achieve certification by a certain date (SMART), is it to win a specific contract or to enter into a particular sector and position the business as a lead contender for future contracts? (SMART) or is it to meet certain regulatory requirements bestowed upon the company? (SMART). You are best placed to judge the reasons and expected outcomes of implementing your BCMS so please set original and meaningful objectives.

Once you have identified your BC objectives, you then need to decide who will be responsible for them and a method of measuring whether they have been achieved (and what should be done if they have not).

You are expected to retain *documented information* on your BC objectives and in my opinion it makes sense to develop a straight forward table or similar configuration through which objectives are clearly identified and the what, how, when and who information is there for all to see. You may also choose to include them within your BC Policy (or simply refer to their existence elsewhere).

Time will tell how well BC objectives are measured and followed through but early indications are this is an area which requires more attention to be both useful to the organisation as well as meet the requirements of ISO 22301.

## 5. Understanding Recovery and determining the level of information required

Do you remember the “Incident Timeline” diagram in BS 25999 Part 1? (Code of Practice) It helpfully depicted the various stages following an incident. Essentially these were split into three phases; Incident response, business continuity and recovery/resumption (otherwise known as back to normal). Timelines were also suggested as part of the diagram. However, the nature of business continuity and in particular associated standards seem to draw us to focus on the immediate/short term aftermath of an incident. Getting back to normal (whatever that might look like after an incident) takes a back seat.
We now have ISO 22313:2012 (BCMS Guidance Document) and this is a subject where the document adds particular value and provides examples of what *recovery* might include. To quote a few direct from ISO 22313:

- Restore damaged facilities
- Salvage equipment in damaged facilities
- Make claims against existing insurance policies

- Recover lost documented information
- Normalise operations at the restored facilities

All these (and many more) actions may be relevant and need to be undertaken as the business gets back to normal. Some may go on for months (or longer), depending on the severity of the incident.

ISO 22301 expects to see a *documented procedure* describing how the organisation would go about the recovery phase. What it doesn't expect is chapter and verse on every conceivable piece of work which might be required but neither does it expect a single sentence suggesting "recovery" will be considered following the incident. It requires thought and appropriate strategies to be outlined which will serve a useful purpose, if ever required. I recommend implementers read the relevant section in ISO 22313 to gain a better appreciation of what might constitute recovery and how your organisation may approach it.

## 6. Evaluating the performance of your BCMS

Traditionally this has been covered by internal audit and management review meetings and still can be, to some extent. However, wider consideration of how the management system is performing is now required. *Performance metrics* are now expected. Despite the fact I have seen BC firms offering training courses on developing performance metrics (!), this is another area where the organisation needs to take a step back, think carefully about what it is trying to achieve and identify "yardsticks" by which to measure its accomplishment. The yardsticks you choose are very important as you need to be selective. Too many will require a full time job to measure them and too few won't give the level of information and analysis the business needs in order to determine how the BCMS is performing.

Typical metrics might include;

- Internal and external audit findings/trends
- Exercise outcomes and test results
- Incident management success/meeting recovery time objectives
- Staff feedback following an incident or exercise
- Quality of Incident Management Team response during and following an incident/exercise
- Measurement of BC objective achievement

Once you have chosen your metrics you need to develop a systematic method for collating and reviewing the information and agreeing informed actions to further improve your BCMS. The results need to be retained as evidence so decide how best to do this.

It's fair to say that it is still very early days to see meaningful BCMS performance evaluation. You will have decided how frequently you review the information and how you report on it but I'm afraid I haven't seen many organisations approaching this requirement in a structured and effective way. Auditors should be demanding to see this as part of their audits (internal and external) otherwise what's the point of having a BCMS?

## General advice

I hope this article has offered you an insight into some of the issues being identified during the audit process. It's early days for ISO 22301 and many readers may still be thinking about whether to go for certification or stick with "alignment" (whatever that means!) In any event, my advice to anyone going down the ISO 22301 route is **make your BCMS your own**. Don't trawl the internet for examples of "this template" and "that report format". You'll rarely find an exact match for your needs and will end up redesigning it anyway. Be creative, involve a variety of individuals and work experience and develop a BCMS which reflects your business culture and requirements. If you can meet the specifications of ISO 22301 as well, even better.

*Hilary Estall is Managing Director of Perpetual Solutions and works with organisations seeking support and advice as they develop and maintain their BCMS. Applying her practical approach to management systems, Hilary's first book Business Continuity Management Systems; Implementation and Certification to ISO 22301 was published in 2012 and continues to receive much praise for its pragmatic look at ISO 22301. For further information please visit www.pslinfo.co.uk*

perpetual solutions