

TICK BOX MANAGEMENT OF BUSINESS CONTINUITY PLANS



'Tick, tick, tick' is the sound every BCM Manager dreads most.

Is this the sound of a bomb waiting to go off so that the BCP has to be invoked? No, it is the sound of Audit responding to their pre-set questions or completing standardised spreadsheets.

Too often either an Internal or External Auditor will ask

1. Have you done a BIA?
2. Are systems backed up?
3. Have these backups been tested?
4. Do you have a BCP?
5. Has the BCP been tested?

Business Continuity is about ensuring that the critical aspects of a business are essentially continuous, regardless of disruptions and disasters. This requires an understanding of what the business does normally and what the business needs to do in a disaster, so that its revenue, reputation and regulatory standing can be protected. Invariably, it is also necessary to assess which systems are critical, and how quickly they will be needed, as very little business in the modern world can operate effectively without its accompanying IT.

A Business Impact Assessment (BIA) is a tool used by the BCM Manager to help set priorities, so that effort can be targeted where disruption has the most disastrous effect. However, when working for a large organisation it is often necessary to set the parameters carefully.

- Is one considering the impact to the organisation as a whole, the particular business line or the particular location?
- Should only the impact on the individual area be considered or should the impact on dependent areas also be factored in?
- Will the latter result in double counting or is it the only way to assess internal service divisions?

In other words the BIA is not a standardised document, but one that has to be tailored to the specific situation, i.e. to set priorities for the company, the business line, the location or as required by any framework. The Auditor should be looking whether a suitable BIA has been conducted, whether the appropriate people participated and whether the responses are meaningful. Too often the diligent BCM Manager will be penalised when he regards a BIA that is more than 12 months out of date as invalid, whereas a less diligent one will present these old ones and get the box ticked by Audit.

Many organisations have central BCM functions, with limited resources. Ideally these resources should be focused on putting in place adequate contingency for the critical processes in major business centres. A high level, organisation-wide BIA should then be used to demonstrate where the key business centres are located, and which processes

are critical. However, an Auditor will often go to a small overseas office and highlight that it has no BCP, without regard to whether this will have any significant impact. The limited BCM resources may then be redirected from their critical activities to resolve this Audit point.

It is difficult to underestimate what a diversion an audit can be. An investment bank, employing several thousand people in each of the key financial locations, once concentrated all its European BCP activity for two to three weeks on a small overseas office with little financial risk. The overseas office was responsible for two of the three outstanding audit points relating to BCP: infrequent tape back-ups and the location of the recovery site. However, the third audit point was the complete absence of workable BCP in one of their major financial centres!

“ Ideally an Auditor should check that the plan is readable, workable and effective, and not just 'tick the box' ”

In some financial organisations this distortion of business priorities is made worse by a reward system that links the size of support staff bonuses to the number of outstanding audit points. One of the great failings of this tick-box mentality is that appropriateness (i.e. sensible weighting) is often forgotten.

APPROPRIATE MEASURES

Another area where a tick-box approach can distort priorities is when considering which systems should have rapid recovery in place. Too often, the question is "is this system backed up?", rather than "should this system be backed up and, if so, how quickly must it be operational again?" A non-critical system, which an organisation can survive without for a week or more, may not need a backup. It may be sufficient to put in place a replacement if and when a disaster occurs. Whereas for an essential system, backup may be insufficient, it may need full real time replication.

For example, a Market Research company who maintained huge historic databases, was diligently making daily tape backups of all the data, and taking these tapes off-site. Unfortunately when a fire kept them out of their building they realised that they did not have a server to which these tapes could be restored. Once a server was found it took many days to restore the data, and yet more days to catch up the lost historic data. Clients, who depend on these databases for their own reports, are now questioning whether the large annual subscription to this Market Research Company is justified. Perhaps the worst thing however, was that this Company had recently paid a large fee to an Auditor, who amongst other things had just ticked the box that backup was in place.

Jillian Simms, FBCI



Jillian Simms, FBCI, is a director of Cornwood Risk Management, a consultancy specialising in Business Continuity Management in the investment banking sector. She is a former bond arbitrage trader and European Marketing Director of the Chicago Board of Trade, the world's oldest futures exchange.

Similarly the question whether backup has been tested needs to be clarified. What is a test? Do you need to shut down all main systems and run the business from backup systems? Or is it sufficient to look at each DR system one at a time, leaving the main systems running? The answer is that the testing should be sufficient to give comfort that, if and when needed, the DR systems will work, within the timescales necessary. Where there is full replication and load balancing, ideally the business should be run sometimes from one and sometimes from the other. Where there are backup tapes to restore, go through the restoration process on a regular basis and check it works. If the system is to be acquired if and when needed, check the delivery and installation times, and consider a service level agreement.

Audits should review whether the testing is adequate and whether it would really work in a disaster. For example, a major clearing bank was set a regulatory requirement of an Auditor signing off, on a quarterly basis, that the backup of the Liquidity system was operational. So sure enough, once a quarter the Auditor went down to the Contingency site turned on the backup liquidity system and confirmed the data was accessible from this location. Unfortunately, no one bothered to tell the Auditor that the backup liquidity system was running off a feed from the main site, and so would not work if the main site was not operational.

A Business Continuity Plan (BCP) essentially explains how you hear of a disaster, where you go in a disaster, what you will expect to find when you get there, and what you should do. However, no two organisations will have exactly the same arrangements and so the BCPs should suit the organisation. Some will need to explain invocation procedures, crisis management team responsibilities and management of relationships with regulators. For large organisations, giving everyone company-wide documentation would be unwieldy. It may be more appropriate for each department to hold only their own procedures, with only a central co-ordinating team holding a plan setting out how it all fits together. For small organisations, it may be 'all hands to the deck' and everyone needs to know everything.

“ Audits should review whether the testing is adequate and whether it would really work in a disaster

READABLE, WORKABLE, EFFECTIVE ...

Ideally an Auditor should check that the plan is readable, workable and effective, and not just 'tick the box' that a plan exists. It is unlikely that a single plan template will suit all the people, all the time. A few key people may need to rush to a Contingency site, where their systems are live and fully replicated, and they will be required to continue business. Others may wait in an evacuation location until the contingency site is operational. Yet more people may be sent home to wait for further developments. Furthermore, large international organisations employ a number of other valid contingency strategies; dispersal of staff to overseas locations, passing of business activities to other offices, reciprocal agreements with other organisations and suspension of non-critical activities.

The BCP handed to individual employees should be appropriate to their required response, and not standard for everyone. For example a major insurance company call centre handed all employees a large book showing the location and layout of their contingency site, together with detailed maps and transport arrangements. This was regarded as the BCP, but there was no information as to whether the individual would be required at the contingency site in a disaster. Also, the contingency site accommodated only 300 of the 950 staff, and so would rapidly deteriorate into chaos if everyone turned up. Furthermore the book didn't state who was responsible for invoking the site, so the people would turn up and no one would have told the third party supplier they were coming.

Testing of BCPs is usually the final point on an Auditors checklist. What does this mean? Should users of the Contingency site have an awareness visit? Should people who are to be dispersed to another location check that their systems work from that location? Should people who are expected to work from home check that their remote access capabilities work when the main site is not operational? All these are necessary tests, but the key thing to remember is that a valid test requires the contingency to operate without resources from the main site.

Following a recent Audit assessment of the Hong Kong office of a major stockbroking house, the box was ticked confirming a tested BCP. However, the BCM team was less convinced, and set out to test the validity of the stated arrangement, namely that the traders would relocate to Singapore if the Hong Kong office had a disaster. It was soon discovered that the interface with the Hong Kong Stockmarket was based solely in the Hong Kong office, and although traders often execute deals from Singapore, they were doing this via a network link in the Hong Kong office. So for the BCP to work, a second interface to the Hong Kong market had to be installed in the Singapore office, and permission had to be obtained from the Hong Kong Stock Exchange that business may be transacted remotely. In effect the Auditor had checked there was a plan, but had not checked that it would work in a disaster.

INTELLIGENT USE OF BCM

In summary, an Auditor needs to check that due process has been followed and suitable, tested Contingency is in place. Checking for BIAs, backup systems and BCPs should only be milestones, not the whole story. Even these need to be assessed for their adequacy and validity, and there is no such thing as a standard template for all organisations, in all situations. Effective Auditors are the favourite partners of BCM managers, they help focus business attention and help prioritise BCM within an organisation.

We recommend that all BCM Managers should work together to encourage the intelligent use of BCM tools. We should get away from the search for the 'one fits all' requests for the standard BIA template, the standard level of testing and the standard BCP. If BCM Managers also move to a tick-box approach to BCP, what hope is there that organisations will have working contingency, adequate for their needs?