



Business Continuity Planning

Many factors are now combining to bring home the realisation to organisations that planning for business interruption is essential. 'Business Continuity' has evolved as a discipline and prepares the organisation for a 'business interruption' aiming to minimise consequential loss and damage. Fire and flood are less rare than most realise. In 2001, 30,000 commercial buildings in England alone were affected by fire. 75% of companies that have a serious fire go out of business within 3 years. Companies are becoming increasingly dependent on IT at a time when IT infrastructures are under pressure and virus and Internet hacker activity is at its peak. 57% of business 'disasters' are IT related, 44 % of UK businesses suffered at least one malicious security breach in 2001, twice as many as in 2000.

Accountancy Age estimates that 1 in 5 companies will suffer a crisis within the next 5 years. Without a plan 90% of those companies will not survive beyond 12 months. In addition there are mounting pressures from corporate governance and insurers, whilst at the same time customers are demanding sound plans are produced to enable speedy and effective recovery from a crisis. It is now recognised that all businesses are vulnerable to failure should they suffer denial of access to data, offices or both.

So what is the best way to go about Business Continuity Planning?

The potential downside of a major business interruption in terms of loss of revenue, dissatisfied customers and damaged confidence is considerable, even fatal. Crisis Management Planning helps to significantly reduce the duration of business interruption caused by a crisis because it reduces the time taken to work out how to recover from it.

Business Continuity Planning is a business-wide issue, NOT just an IT issue and the first step is to create an effective company-wide Crisis Management Plan.

Draw up how your business works, what the business areas are and which each area needs to function correctly. Don't overlook non-IT issues such as buildings, desks, documentation and staff. Then look at the measures already in place to cope with problems, if any and whether they are enough. Lastly try to understand the cost of an area not being able to do its job within a certain amount of time. This information will drive everything else.

The BCP process is expanded on overleaf and can be assisted by the use of BCP tools, which support the team through the process of developing the plan. These tools also accumulate the output of the planning process and provide an efficient and reliable method of maintaining the plan and in some cases support its use in an active situation where the plan has to be used.

From the BCP project point of view, the tools are normally of greatest assistance to the project team members as it provides them with a consistent structure within which to approach the exercise. Their other main advantage is the ability to manage the maintenance of the plan and support its use when necessary.

This was a particularly powerful feature of the tool Shadow-Planner which Scott-Moncrieff recently evaluated. Scott-Moncrieff currently recommends the Shadow-Planner tool, which we ourselves use for our own Business Continuity Planning requirements.

An evaluation of the benefits to the team of deploying such a tool should be considered at an early stage in the project.



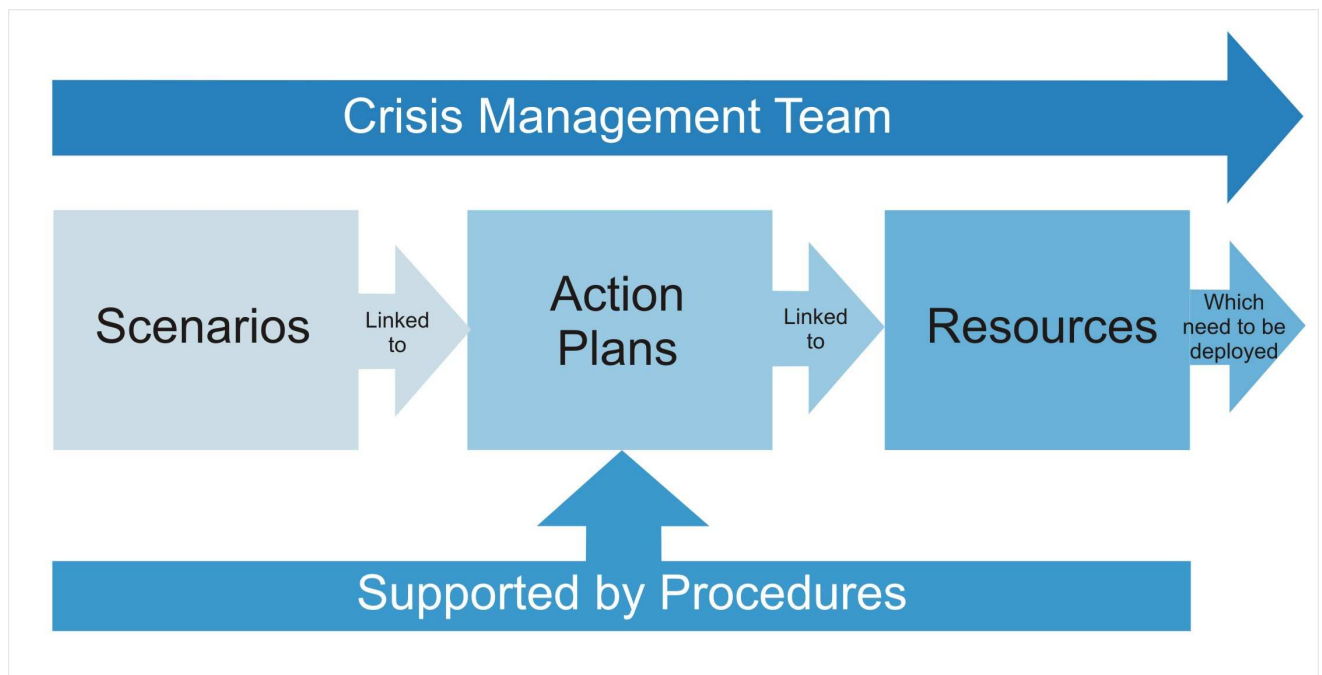
Business Continuity Planning

The first step in the process should be the completion of a Threat and Vulnerability Matrix. On completion select from the threats with the highest likelihood and develop typical scenarios of how the threats might materialise. It is also useful to quantify the scale of impact and identify who should be responsible or accountable for dealing with each situation.

The idea is that the scenario provides a realistic and sensible interpretation of the type of situation which could have a significant impact on the day to day business of the organisation. Once the Scenarios had been defined the approach is then to develop action plans capable of responding to these likely scenarios.

The action plans for each scenario are then linked to the relevant resources, be they people, facilities or infrastructure, which are required to perform the planned actions. Ideally the majority of these actions would be supported by procedures setting out how a particular task is to be performed. These could be anything, from contacting staff to notifying a supplier or any of the other myriad tasks which would need to be carried out.

The entire process would be co-ordinated by a Crisis Management Team who have the authority to make decisions. The diagram below illustrates the relationship between these processes.



BCP workshops are used to start the process of compiling action plans for a number of the scenarios identified in the Threat and Vulnerability Matrix. This approach produces both a tangible product from the workshop and also provides the attendees with the experience of actually performing the process of working through the development of an action plan.