



Typical Stages of a Business Continuity Plan

1. Scope

This is a very important stage of your plan. In smaller organisations one plan may cover all the functions undertaken, in larger ones several plans may exist (for each business unit or geographical area for example). The key is to ensure that whatever areas are covered they are the ones that are vital to the survival of the organisation should an incident occur.

2. Who will do what?

In smaller organisations one person can be the BCP Manager for example ideally this should be someone who is fully conversant with the operation of the organisation and understands what makes it tick. They should also have a high level of people management ability as this is invaluable during a disruptive time.

In larger organisations a response team will be formed where each member will have responsibility for a specific area such as people, finance, media and systems. Temporary authority may be given for emergency expenditure etc.

3. Invocation

A very important stage a plan that is wrongly invoked or invoked too late can have dire consequences. Many incidents can be dealt with without invoking a plan at all. A well written and maintained Plan can act as an operational guide on how to deal with threats that present themselves. Partial invocation can also take place for example Public Relations responses can be detailed in the plan but invoked independently using proven methods.

If a plan is invoked then it is important that everyone knows what their role is in keeping the organisation alive.

4. Key Components

There are two crucial components of any BCP

Risk assessment

Your organisation may already have a risk register where you have identified risks that may put it under threat. This can be amended and used as the basis of assessing risk. There are normally three actions you can take with risk **address**, **mitigate** or **ignore**.

However well you address risk incidents will happen and you need to be ready to deal with these.

Business Impact Analysis (BIA)

Once you have analysed the risk the organisation faces it's time to look at the actual impact these could have on people and process. Each potential risk is then examined further in terms of the impact its failure could have on the ability of the organisation to survive.

Steps will be identified on how you will address each area of potential impact with the aim of protecting people, property, revenue etc. Not to be forgotten is the interdependency between each process as one failure may lead to a domino effect.

5. Communication

Who an incident might affect has to be carefully considered employees, clients, suppliers the general public may all have some involvement with your company. Investors will need to know an Incident will affect their investment, employees need to be kept as safe as possible both physically and mentally.

The key is that you have discussed this and planned a communication method(s) prior to the incident not during it as stakeholders will be under enough pressure as it is.

Internal and external communication can be very different an interview to the press is very different in nature to a personal phone call to a distressed employee each will have where possible the best person and best communication method assigned to it

6. Documentation and Version Control

Creating a workable Business Continuity Plan is challenging enough maybe an even greater challenge is keeping it up to date. An out of date plan could have a catastrophic affect in an incident scenario. Whether paper or software based these documents, processes and procedures must be kept current.

Reviews of the current risk/impact climate must be done regularly and changes made accurately and quickly. Key here is old or obsolete documents must be archived and taken out of use. A suitable member of staff should be selected for this role having the required attention to detail.

7. Test, Test, Test

You don't want to find out that your BCP plan has serious flaws during a serious incident testing regularly will increase your protection level. In the Business Continuity World three tests are utilised.

Table-top exercise

Key actors in a potential scenario read the plan look for gaps and collectively revise it to bring it up to date. This method is essentially aimed at smaller organisations who have a plan that is managed by an individual

Walkthrough

Typically for larger organisations this is one step further where each member of an Incident Management Team for example rehearse a scenario and practice their responses to it. Lessons learned are recorded and procedures, processes and documents updated accordingly. Activities can be split over several days if availability is at a premium

Full Simulation

Mainly aimed at larger organisations to fully test readiness in the event of a serious incident. Companies have switched off main communication links for example to test function of back up circuits. Transactional organisations such as banks and large on-line stores have elaborate contingency plans to stop loss of revenue.

Any organisation can use any of these effective tests depending on budget available and applicability the key is to test as often as possible as the environment and risk profile is forever changing.