The Essentials of BCP

Business Continuity Planning as a Process

Presentation to British Universities Finance Directors London Group
25th November 2005

by

Philip Cassidy

Flux Risk Services S.A.

Website:www.fluxrisk.com **e-mail:** cassidy.philip@fluxrisk.com

1. The pitfalls of BCP

My own experience in advising clients is largely confined to the financial and insurance sectors, but I believe that there are some underlying principles which should apply to planning for those occasions when our normal risk management disciplines have failed and we have to move out of our operational comfort zone.

It seems to me that there are a number of common pitfalls into which some organisations can fall when approaching Business Continuity. Amongst these are:

- Confining BCP to one-off exercises which produce sterile documents which are seldom looked at again
- Plans which address many scenarios but only offer one solution (e.g. switch over to the backup servers and move to the recovery site)
- Leaving the whole business to a committee of risk, IT and FM managers, the minutes of whose meetings are never read
- Never testing plans in a thorough and systematic way
- To these perhaps we can add the considerable scope for confusion and worry produced by the burgeoning Business Continuity industry.

2. BCP is distinct from Disaster Recovery

As we know, crisis management, disaster recovery and business continuity are not new concepts, but they have been especially pressing topics since 9/11 and were given renewed impetus by the appalling events of last July, which Susan Wilkinson talked about from a fascinating first hand perspective.

It is undoubtedly vital to have well prepared plans to cope with such calamitous events, which may even devastate an enterprise to the extent of it being left with no fixed assets, virtually no personnel and little left except a depleted balance sheet and an insurance claim, as some businesses in New York found in 2001.

However, it is important not to be fixated with Doomsday scenarios, since there are many events which do not necessarily involve such drama and tragedy, but which can have dire consequences for an enterprise of any type. Those of us with memories of the three day week of the early 1970's may contemplate the implications of potential energy shortages this winter rather uneasily.

3. The difference between planning and plans

It is a well known military axiom that no plan survives first contact with the enemy. Like all such truisms, the saying has a certain superficial validity, but conceals the fact that a well-trained army which has marshalled its forces, studied the enemy and thoroughly reconnoitred the battlefield stands a better chance of attaining its objectives, regardless of obstacles and setbacks.

I think that this analogy illustrates the important difference between planning and plans. Frequently too much emphasis is placed upon the production of impressive and well (or not so well)-crafted documents designed to address a narrow range of disaster scenarios rather than the creation of a resilient process which will prepare an organisation to respond robustly and flexibly to a broad spectrum of mishap or calamity.

This distinction is important, both as an organisational approach to BCP and when drafting the documents which are undoubtedly important to structure the actions to be initiated and to record the necessary information to be accessed.

A document, or collection of documents do not of themselves constitute a plan: they should merely represent the outcome of a comprehensive process encompassing the whole organisation.

Later in this talk I would like briefly to outline how such a process might be created and operated, the elements to be incorporated, and the essential documentation.

4. Resilient for a broad range of scenarios, effects not causes

Before talking about process, I would like to run the risk in an academic gathering of standing conventional scientific and philosophical wisdom on its head by saying that here, effect should precede cause.

There is plenty of scope for an organisation to tie itself in knots considering all the obvious, not so obvious and downright bizarre things that might go wrong or happen unexpectedly. Whilst such speculation does have a place and can be as interesting as it is alarming (the same cannot be said about much else in this field), it does tend to obscure the fact that the effects will usually fall into one or more limited categories and that it is much easier to plan for those effects than to second guess the vagaries of fate. See Appendix (A) for a table relating effects to cause.

I would categorise those effects as follows**,** being the loss of, wholly or partially, temporarily or permanently:

- **Personnel**
- **Buildings**
- **Other Fixed assets**, such as computer equipment or infrastructure
- **Intangible and information assets**, such as data, goodwill or vital records
- **Services from third parties**, such as utilities, supplies, outsourced services.

I believe that most disruptions to the continuity of business can be resolved into their effects on any of these categories.

5. Blueprints for your business

I believe that the first essential step for an organisation in the planning process is to answer in detail ten fundamental, and apparently simple questions:

- Who are we?
- What do we do?
- Why do we do it?
- Whom do we do it for?

- How do we do it?
- When do we do it?
- Where do we do it?
- What do we need to do it?
- What does it cost us to do it?
- Who does what for us in order to enable us to do it?

Unless organisations have that information at their fingertips they cannot say what business it is whose continuity they are trying to protect, nor can they set about planning for it. Essentially we need that information as the basic blueprint for our enterprise: without blueprints one cannot successfully rebuild. It is surprising how many organisations will struggle to answer these questions in a structured, accurate, and succinct way.

A discontinuity of business will mean that the answers to some of those questions will have changed: an outbreak of severe avian flu or SARS, or a industrial action by key staff, might make the "who" equation: ***X* minus 50%**; a severe fire will change the "where" – no laboratories; the insolvency of the catering supplier might mean that your staff and students have nothing to eat or drink on campus; and so on.

I would suggest that the Business Continuity Planning process has to start with the definition of the current state by answering those questions, and thereby drawing up the blueprint of the business.

6. A structured planning process

It should then proceed to considering the implications if any event or series of events have changed any of those answers. As I am sure you are aware, this is commonly referred to as the business impact analysis. The changes can be referred to as outages and their effects over time (by days, weeks, months even years) can be scored according to the likely effects financially and non-financially e.g. diminished service levels, loss of reputation and customer confidence, loss of competitive position, legal or regulatory penalties, and so on. A specimen Business Impact Analysis form is attached as Appendix (B).

The scorecards thus generated will provide a clearer risk overview and provide a platform to devise a suite of responses appropriate and proportionate to the outages, according to the organisation's cost/ benefit analyses for making decisions about resources.

7. A structured management process

As important, or indeed more important than the methodology of the BC planning process is the way it is managed. I said earlier that BCP is often seen as an irritant, an unwelcome additional task for hard pressed managers and staff, distracting them from the existing burdens of managing business as usual (BAU).

There is no denying this: the demands of the here and now will always seem more pressing than the abstract and hypothetical subject of BCP. That is until disaster strikes and the improbable and remote becomes all too real, as happened on 7th July. Quite simply it has to be done to protect our businesses, just as we buy insurance but would rather invest in something more obviously productive.

In addition, it is vital that BCP is seen as a central management responsibility, not a sideline to be attended to during non-existent managerial spare time. Neither should it be shuffled off entirely to teams, committees or task forces of marginal importance without the necessary authority (although these do have their place). If line mangers are responsible for BAU activities, why should they not be accountable for the effectiveness of their departments when business is no longer as usual? The process must of course start from the top.

8. Everyone must be involved

What is true for management should, to some extent, apply to every member of the organisation. Each stakeholder in a plan needs to know of its existence and their role in it. To take ownership of that role they need to be made aware, to understand, to be trained and above all to participate.

This can be achieved for example by holding workshops, with "What if?" brainstorming exercises, or by tasking individuals with assembling and maintaining particular pieces of information such as contact lists, equipment inventories, process maps, and so on. Blueprinting is a significant task and needs to be dispersed.

Within the parameters of policy guidelines and structured brainstorming exercises, very useful insights can be gained and plan flaws more easily identified. Unsurprisingly, the information gleaned from such exercises can be highly useful in understanding and reappraising how the organisation operates day to day, never mind in contingency mode.

Staff should be asked how they could perform their duties if circumstances were different, for example, if a particular system were inaccessible, or what their individual practical needs are, such as a specific type of equipment. Sometimes there will no practical alternative solutions and expectations should not be unrealistically raised, but it is important to be aware of these limitations so that account may be taken of them. The devil is very much in the detail.

9. How prescriptive should management be?

As always, there is a difficult balance to be struck here between an excessively bureaucratic, top-down approach to laying down guidelines as to the methods and content of BCP, and a more laissez-faire approach of encouraging people to develop their own plans.

I have just mentioned the importance and benefits of involving all members of the organisation and encouraging active contributions to the process. However, this does need to be within a clear framework of fairly detailed policy guidelines and internal compliance.

Business Continuity Planning is intended to safeguard the capacity of an organisation to function effectively in abnormal and sub-optimal circumstances, so it is essential for senior management clearly to set out the following: what the overarching plans should be; the objectives in terms of minimum recovery times and longer-term restoration; the resources available; the duties of management and staff; and how a satisfactory level of preparedness should be maintained.

Above all they should make sure that everyone sees the big picture: there is no room for office politics, internal rivalries or turf wars. Since much of the planning process will revolve around prioritisation of tasks and the allocation of limited resources, these issues need to be resolved at a high level and not left to inter-departmental negotiations, or even worse, squabbling.

Mechanisms will need to be devised to ensure that the mosaic of departmental plans fit together as a coherent whole, and make sense in the broader context by mapping into a top level master plan.

10. Identifying dependencies, internal & external

Lift the lid off most organisations and one will find an intricate network of dependencies, both between different units within the organisation and with the outside world.

It is important during the blueprinting process to identify these dependencies and to analyse how they might be affected during a contingency. For example, are suppliers and outsource providers contractually obliged to provide the same services at the backup site? Has any thought been given to notifying them during an emergency? Would we need to have security at our building even if a fire had made it a smoking ruin? Would we need to scale certain supplies, up or down?

This in turn leads us to ask about the suppliers' own BCP's: do they have adequate contingency plans which would safeguard some service crucial to our own operations?

What about our own contractual or charter obligations to our customers or supervising authorities? Are we in a position to invoke force majeure or Act of God to get us off the hook if some disaster brings our operations to a standstill?

I am not suggesting that every contract might need to be rewritten, which is obviously unrealistic , but I would suggest that such vulnerabilities should be identified and opportunities taken to modify or clarify them when for example agreements are reviewed or pricing levels are changed. This is a longer term aspect of the planning process, but does need to be addressed by procurement and legal departments, amongst others.

11. Producing practical documents: policies, plans, templates and lists

Having talked about the planning process, it is now time to talk about the actual product to be generated by these exercises in the form of usable documentation.

I believe that the first thing to avoid is to consolidate everything, from strategic policy and business impact analyses, to equipment inventories and call trees into one document and call it the BCP for general distribution to all and sundry. This would create a huge unwieldy volume, which would gather dust on shelves, be out of date in a couple of months, and next to useless in an emergency for 95% of the staff.

At all times the audience being addressed and the purpose of the documents should be borne in mind.

To this end I would suggest that, once again remembering the distinction between planning and plans, the following suite of BCP documents might be created:

- **A Policies & Procedures Manual** which clearly sets out BCP objectives and rationale of the organisation, as well as the practices and routines to be observed in constructing and maintaining plans; it should include a plan hierarchy aligning plans to the organisational structure; the P&P Manual should also include practical guidance including templates, standard forms etc. This document would be intended for observance by the whole organisation, but should be aimed mainly at managers

- **A Plan Template** to be adopted by each entity identified in the plan hierarchy and populated with fairly comprehensive information, following fairly strict format guidelines in order to avoid a plethora of dissimilar, free form documents, which make it almost impossible to review and monitor centrally – they should all look very much the same. This would serve as a reference document for managers and those actively involved in BCP in the department/unit/business group. It is one with which they should be very familiar.

- **A Short Form Plan Template** or **"Briefcase Plan"** to be adopted by each plan entity and populated only with information essential for the emergency phase of a contingency. This document would be directed at all members of staff, but especially those with a defined role during the crisis period.

- **A BCP Maintenance & Compliance Guide** consisting of checklists, internal reporting forms and a BCP task calendar, all designed to provide a short and clear set of aides memoire for managers and BCP specialists showing what BCP tasks they need to be performing throughout the year.

All these documents can be posted on the organisation's intranet at the appropriate security access levels. Version control and sign-off protocols are important to avoid a proliferation of drafts, obsolete versions and incomplete or stale data. To this end documents might be produced in PDF once adopted.

12. The key components

I have touched on most of the key elements which should go into the planning process and now it would be timely to summarise the subject headings for the content of plans themselves. Some of these headings speak for themselves, others may require a little bit of explanation. I will number them in order to differentiate them more clearly:

i) Crisis management and disaster recovery – These are self-explanatory.

ii) Risk scenarios & BIA – Notwithstanding the importance of emphasising effect rather than cause, some connection needs to be made between events and their main effects by reference to the five main effect categories: personnel, buildings, other fixed assets, intangible and information assets, and services. See Appendix (B)

iii) Core processes – the listing and description of the critical processes which are priorities to be maintained during a contingency.

iv) Physical resources and assets, logistics and finance (including loss mitigation & cost benefit analyses).

v) Human resources – organisation charts, staff listings and definitions of the contingency role of each individual.

vi) Dependencies – defining from an input/output perspective which core processes flow into and out of the organisation and each plan entity, the corresponding entities (internal and external) which generate or receive these processes; their contact details and the contractual/defined obligations which bind these processes, as indicated above.

vii) Recovery – the detailed plan for resuming operations and running in contingency mode after the immediate emergency has been contained.

viii) Information technology & communications infrastructure - ensuring that there are resilient back up systems and procedures to ensure that data is not lost and processing can be maintained or resumed quickly, and that effective communications can be maintained internally & externally during the contingency.

ix) Internal & external communications - I would include under this heading all elements of corporate communications (internal and external), including public relations: what do we tell our employees, our business partners, our customers and the rest of the world when we have to implement our plans?

x) Awareness, training and testing – this is perhaps the most important element of all. Each plan should be the subject of comprehensive awareness and training programmes, and subject to regular and rigorous testing in as realistic manner as possible. All these should be recorded, de-briefed and subject to remedial action when deficiencies are revealed.

xi) Documentation & vital records – in addition to plan related material and the procedures for updating and maintaining it, this will include archiving, secure document storage and vital record-keeping.

xii) Regulatory, legal & compliance – This is to ensure that relevant laws, the rules of regulatory oversight (to the extent that they apply) and internal compliance rules are observed and not completely ignored during the contingency.

To these might also be added **Restoration –** how to resume business as usual in an orderly and controlled manner once a contingency is coming to an end. This presupposes that a contingency is passing and is not therefore an urgent priority needing to be included in plans themselves.

Conclusion – What value do BCP's have?

The acid test for any plan is whether it will work in a real contingency. Most of us would like to know before then if our plans are any good and would give us any prospect of salvaging our enterprise from disaster. The fact is that BCP is an inexact science and we cannot know in advance if our plans will work.

What we can do is to ensure that the process is in place to keep our plans constantly up to date and under review, with BCP issues nearer the front of everyone's minds through regular training and awareness.

It is likely that when the ill-omened day does arrive, it will be at an inconvenient moment and in an unexpected form. It is quite unlikely that our plans will go exactly according to plan.

The best that we can hope for is that with the preparation and resources we do have we will have the means and the resilience to respond as effectively as we can with the confidence to improvise, which is probably the most useful skill of all.

Appendix (A) – Business Continuity Causes and Effects (Scenarios & Outages)

Outage categories	H	B	F	I	S
Scenarios	Loss of or injury to personnel to prevent them working	Loss, damage or denial of access to buildings	Loss, damage or disablement of other physical assets or infrastructure	Loss, damage or disablement of intangible or information assets	Loss, denial or disruption to critical third party assets or services
Natural disasters e.g. storm, flood, earthquake	X	X	X		X
War, terrorism, hostage taking, sabotage, organisational blackmail	X	X	X	X	X
Man-made catastrophes e.g. fire, gas explosion, chemical spillage	X	X	X		X
Utility failures e.g. power cuts, network carriers		X	X	X	X
Transportation strikes and breakdowns	X	X			X
Communications and postal disruptions				X	X
Hardware or software failures e.g. overloads, bugs				X	
Electronic attack e.g. virus infection, hackers, website highjack			X	X	X
Employee action e.g. strikes, mass walkout, protests, sabotage	X	X	X	X	X
Civil disorder e.g. riots, vandalism, disruptive protests	X	X	X	X	X
Vendor failures e.g. contractual disputes, insolvency, crashes			X	X	X
Theft, fraud, embezzlement, extortion, blackmail of staff				X	X
Security compromised through error e.g. building left insecure		X	X	X	
Failures of internal predecessor, successor operations, supports	X		X	X	
Management failures e.g. damaging actions by rogue managers	X			X	X

Appendix (B) – Specimen Business Impact Analysis

		Outage event duration																					
Outage Categories	CORE PROCESSES IMPACTED	< 1 hour	< 1 day	< 1 week					< 1 month					< 9 months					> 9 months				
		ANY	ANY	F	S	C	P	R	F	S	C	P	R	F	S	C	P	R	F	S	C	P	R
H (human)																							
B (buildings)																							
F (fixed assets)																							
I (information assets)																							
S (services)																							

KEY:

F – Financial impact - rating scale:

1 - < £ 5k	**2 - £5k - £20k**	**3 - £20k- £50k**	**4 - £50k-£100k**	**5 - £100k-250k**
6 - £250k-500k	**7 - £500k-£1m**	**8 - £1m-£5m**	**9 - £5m-£10m**	**10 – Above £10m**

Non-financial impacts:
S – Service levels (internal)
C – Loss of customer confidence
P – Loss of competitive position
R – Regulatory and Legal

0 – not applicable (no risk)
1 – minor negative impact
2 – moderate negative impact
3 – high negative impact
4 – critical negative impact