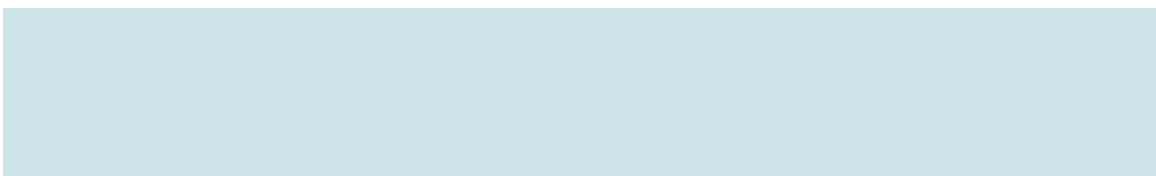




# Getting serious about business continuity

Carl Greiner

August 2006





## Getting serious about business continuity

***Many valuable lessons and improved best practices have evolved since 9/11. However, for the vast majority of IT organisations (ITOs), they have gone back to business as usual when challenged with limited budget dollars. The main purpose of this series of papers is not only to instil a sense of urgency in IT to more adequately address the lingering frailties within our infrastructures, but also to identify reasonable and achievable goals that allow the organisation to begin the process for real improvement. You need to know what to do, know how to do it, and be able to accomplish it and measure results. Business continuity is as much as (or more so) an operational and cultural challenge as a technology challenge.***

### Changing the focus

Traditionally ITOs and business leaders viewed business continuity (BC) as a necessary evil and focused primarily on disruption causes with instituted plans for facility evacuations, disaster preparedness and infrastructure recovery. The unfortunate events of the past few years have changed this view forever, with all enterprises realising they are vulnerable to unplanned business disruptions and that they must become more proactive about minimising corporate risk associated with any disruption. Therefore, now and going forward business continuity will be less about anticipating possible disasters and their unique recovery, but more about keeping the business running no matter the disruption. As a result, business continuity will have to adapt to increased scrutiny.

IT has a responsibility to assist the corporation in understanding what will be expected in the future, and to help get ahead and stay ahead of the curve. In MIT Professor Yossi Sheffi's book, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, he alerts organisations to multiple tiers of vulnerability created by our reliance on complex supply chains. This means one's complete business operations may come to a screeching halt due to a large or small – natural or manmade – issue with one of their suppliers, possibly half a world away. While certainly enough to cause one to pause, and important enough to include as an additional level of criteria/evaluation when selecting supply chain partners, we cannot begin to solve the entire problem all at once, especially since there can be many reasons for disruption. Even by restricting our attention to the scope of IT business continuity, we cannot



resolve the exposures for the entire chain until we have our own houses in order. You must also keep in mind that your enterprise can be a significant element of another corporation's supply chain, so at some point your most significant customers may be asking your company these same questions about your ability to survive.

### **How to promote change**

The age-old question is 'how do we get an organisation to do something they know they should do – but still have not yet done?' Sounds silly, but let's draw an analogy to something that we can all relate to on a daily basis – dealing with personal business communications.

Going way back to the days of the pink 'while you were out' message slips, to voice mail and email, and now non-stop email and voicemail via mobile phones with caller ID and Blackberry-like devices, we have dealt with the internal struggle of which message to respond to first. How does each individual establish a set of personal priorities? While it would be 'clean' to list a number of logical rules or methods (one executive claimed to have the self-discipline to address everything in chronological order, regardless of the source or importance of the issue), life is not a laboratory. We have good days and bad. Most times, others set our priorities. Regardless, much like the United States Marine Corps slogan, we improvise, adapt and overcome.

Human nature usually drives us to do the more enjoyable things first: return the call of your old classmate to catch up, email your client that you have tickets to the ballgame, and so on. Conversely, we postpone returning the message from the business unit head that is complaining (again) that the network is down, and wants to know what we are doing about it.

Many items warrant being addressed 'out of turn', so we have to struggle against our natural instincts to tackle distasteful tasks sooner rather than later. Certainly one of those is business continuity. Business continuity can be complex, expensive, and if you are *really* successful in your implementation, most people don't even realise what you have accomplished.

Whenever there is a natural or manmade threat, news items of lost back-up tapes, or other events that strike fear in the hearts of the IT professional, it generates a lot of material (both written and verbal). It reminds us of the need to take a closer look at our own situations. This is another one of those friendly wake-up calls – however, with a twist.

Instead of ranting about the impact on GNP, or threatening the basic economic fabric of a given geography, we will revisit the processes and actionable items organisations can address to begin the journey to



continuously improve the organisation's ability to provide appropriate levels of business continuity required by the company.

So let's take this back to the business. Firstly, ITOs need to think about business continuity as an ongoing responsibility within the organisation. It has been noted that many organisations assemble BC plans (many three-ring binders that sit on a shelf) and more often than not are infrequently or never tested or revisited. The business is given comfort by the fact that there are BC plans, yet in many cases no one is sure if they still work – or more importantly that the plans still map to dynamic business requirements.

Changing requirements are a constant. One area involves the dynamics of the business, ranging from mergers, acquisitions and high growth in one area to decline in another. A second is solution and technology evolution from basic price/performance, new media/capacities, replication technologies that enhance distance, communications or performance, and solutions such as continuous data protection. Both are important to maintaining the proper level of preparedness, and why an ongoing self-appraisal of your state of preparedness is a necessity.

## Business continuity success starts at the top

Business continuity is not just an IT organisation responsibility. Senior executive management sponsorship and ongoing business executive participation are required to build business continuity into an enterprise culture. The ultimate transformation is to integrate BC processes into the portfolio/lifecycle management of every project, and all business/IT processes and change management activities. Business continuity requires that disparate enterprise resources be assembled as an executive advisory team.

Members of the decision-making advisory team should include an executive from HR, facilities and real estate, each business line, IT, finance and legal. It is this group, in conjunction with the corporate board, that:

- sets the ultimate BC strategy
- establishes corporate risk thresholds
- establishes regulator and compliance requirements
- set objectives, governance and measurement metrics
- establishes priorities
- determines funding/budget allotments.

### **A dedicated BC group**

However, for continuity, budget management, integration tracking and accountability, there must be a focused and dedicated BC group (a



minimum of two, often four or more per geographic region) in conjunction with the executive advisory group. The full-time entity is responsible for:

- implementing policy, governance and reporting
- establishing and leveraging appropriate standards
- reporting on corporate preparedness
- communicating business continuity requirements and business requirement changes
- confirming all test results and works with auditors on corporate business risk evaluations.

The dedicated BC team is responsible for conducting the business impact analysis (BIA) to identify what the enterprise has at risk and which business processes are most critical, thereby informing the executive team so that they can prioritise risk management and recovery investments. The direct/indirect impact of business interruptions must be constantly reviewed with all primary business changes, new regulations, and business process or system/application changes, and include updated business impact analysis statements. The intent is to establish the business continuity plan and then keep it current through ongoing updates.

Without establishing a dedicated business continuity group, which should report to the CFO/COO (not the CIO), most efforts deliver limited success. Corporate and business buy-in/support is mandatory for a leveraged and cost-effective activity.

Assuming this level of buy-in, the next activity must be to ensure that whatever the level of authorised spending, it is spent in the right places and protects the most critical business processes. Again, the BIA identifies critical business processes and resources, internal and external dependencies against acceptable corporate risk, and is critical to the decision-making process.

## **A virtual team**

As with almost every other aspect of IT, one can think of IT business continuity as a 'virtual' team encompassing the entire ITO. Permanent members would have tracking, reporting and auditing responsibility and often be augmented by the virtual pool of IT resources, and would not necessarily take up 100% of their time. That said, all ITO personnel would have business continuity as part of their overall job description. Additional business representatives are likely to augment the core team at varying points in time, along with external specialists/consultants. The important considerations when developing the team are expertise, authority, operational awareness and the recognition of the importance of their charter. Do not be confused about this point. We are not suggesting a blue ribbon panel that meets for lunch twice a year. This issue warrants significant attention, and the likelihood that each of the team



members/representatives would take action items that would require additional staff to work in their primary organisations. Like any organisation, requirements will change over time, and some members will leave – and new ones will join. This is fundamental to the enhancement of the overall capabilities of the dedicated BC group.

## The ten steps of a business continuity solutions plan

What prevents most organisations from even beginning this effort is its sheer magnitude and dimension. Even the *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System* recognised that organisations need time to plan and budget appropriately to implement 'sound practices.' Achieving such a large goal can be made more manageable by breaking it down into smaller components.

The broader task can be broken up into categories – we suggest three:

- plan
- build
- manage.

Arguments can be made for more or less, yet these map well to a reasonable lifecycle approach. Within these areas there are additional discrete tasks.

### Plan

- Assess program/service levels.
- Define business requirements.
- Evaluate availability and recovery alternatives.
- Design infrastructure.
- Conduct implementation planning.

### Build

- Implement and test technologies.
- Develop recovery/failover plans.
- Conduct recovery testing.
- Redevelop/update program definition.

### Manage

- Manage resources, improvements and measurement, including program management and integration throughout the life of the initiative.



The subsequent papers in this four-note series will go into greater detail around these elements of the 'plan', 'build' and 'manage' approach. Again, our goal is to lay out an actionable plan that will allow for the definition, articulation and adaptability of the evolving business continuity needs of the organisation. This is not a project that will be finished in a few months or years, but a 'cultural change' for your organisation.

In the end, two things are constant: business requirements will continue to change, and BC technology will continue to change. Corporations must maintain the 'pulse' of both.



## Client re-use disclaimer

- This is a verbatim reproduction of independent material that has previously been published by Ovum within the last 6 months
- Ovum operates under an Independence Charter. For full details please see [www.ovum.com/about/charter.asp](http://www.ovum.com/about/charter.asp)
- Ovum may have been paid by the client for the right to re-use the material
- Ovum may have a deal with the client to supply research or consultancy. However, no other relationship exists between the 2 companies (e.g. shareholdings, loans, non-executive directorships etc)
- Ovum does not endorse companies or their products
- While we take every care to ensure the accuracy of the information contained in this material, the facts estimates and opinions stated are based on information and sources which, while we believe them to be reliable, are not guaranteed. In particular, it should not be relied upon as the sole source of reference in relation to the subject matter. No liability can be accepted by Ovum Limited, its directors or employees for any loss occasioned to any person or entity acting or failing to act as a result of anything contained in or omitted from the content of this material, or our conclusions as stated
- This material is the copyright of Ovum Europe Ltd.