

preparing for the unexpected

KEEPING BUSINESS GOING

None of us has to be reminded of the importance of preparing for the unexpected. Good Corporate Governance demands we be prepared, and the need to have contingency plans in place has been brought sharply into focus since the events of 9/11.

NOT EVERYTHING IS MISSION CRITICAL...

The first thing to do in working out a Business Continuity strategy is determine which of your systems are actually mission critical.

Payroll: If the payroll system were to go down, continuity may well be satisfied at minimal cost by having an arrangement with the bank to pay staff the same as last pay period, and make up for any differences later.

Transaction systems Any company that makes a living from processing electronic transactions would probably need to ensure that their continuity strategy involved duplicated systems, possibly located at different sites.



It is impossible to tell when a disaster will occur, but every organisation needs a strategy to cope with the unexpected.

DEVELOPING A BUSINESS CONTINUITY STRATEGY

- Secure Support from Senior Management — developing a Business Continuity Plan is not just an IT activity.
- Conduct a Risk Assessment— see adjacent table. An external consultant may be required.
- Assign Priorities to Operations — what is it that you can't survive without?
- Explore all Options for Disaster Recovery strategies — insurance, "cold", "warm" or "hot" backups.
- Collect objective data — from across the organisation: one person's gut-feel may be quite different to another's.
- Create a Comprehensive Written Plan — and have it approved by the sponsor (CEO, Board).
- Develop Test Procedures, and test/exercise the Plan on a regular basis.
- Maintain the Plan — regularly review the plan and link it to your change management processes to capture internal and external changes.

IDENTIFYING RISK

The first thing to do in coming up with a Business Continuity strategy is to create a list of systems used within an organisation, and assign 2 attributes to these systems:

- a *criticality* classification; and
- the likelihood of occurrence of an outage.

The product of these two numbers indicates the relative criticality of the system, indicated by the red area in the diagram below.

Classification \ Likelihood	Critical	High	Medium	Low	V Low
Almost Certain (>80%)	Red	Red	Red	Red	Red
Likely (> 60%)	Red	Red	Red	Red	Red
Medium (>40%)	Red	Red	Red	Red	Red
Unlikely (>20%)	Red	Red	Red	Red	Red
Very Unlikely (<20%)	Red	Red	Red	Red	Red

This Risk Matrix plots the criticality of systems against the likelihood of an 'outage'. Business Continuity strategies are needed for those systems in the top left.

MAKING PREPARATIONS

The following steps provide increasing levels of business continuity — with corresponding increases in cost:

Backups: Most organisations have routine backups in place, but you may like to review some aspects of the strategy — for instance, is it really wise to engage an off-site backup company that has its logo emblazoned on its vehicles? When was the last time a restore was tested?

Duplicated power rails: most data centres use racks which have dual power supply rails, supplied from different circuits. Computing equipment should also be supplied with twin power circuits to take advantage of this inherent redundancy.

Duplicated storage: Storage costs have reduced to such a stage that it may be quite economical to duplicate files on different storage units, and arrange for file updates to be made to both systems. In the event of a failure, the other unit can be brought on line reasonably quickly — more quickly than applying last night's backup tapes.

Duplicated hardware: if commodity hardware is involved, a complete backup system could exist alongside the production equipment, with manual changeover when required.

Clustered hardware: duplicated hardware can be clustered in a redundant fashion, so that the failure of one component automatically results in transfer to another.

A second site: backup systems can be located at a second data centre, which is served by different power and communications infrastructure to the primary data centre.

AC3 DATA CENTRES

ac3 provides a highly reliable and secure environment for hosting mission critical systems. The data centres feature:

- **power redundancy**
- **resilient UPS system**
- **dual circuit power rail racks**
- **environmental monitoring**, and are
- **professionally managed** — on a 24x7x365 basis.

ac3's second data centre in the Global Switch complex at Darling Harbour, on the fringe of the Sydney CBD, is:

- served by separate communications and power, **but**
- is close enough to be accessed easily in an extreme emergency.



ac3 data centre at the Australian Technology Park

AC3 AND BUSINESS CONTINUITY

ac3 is the primary data centre for a large number of corporate and government clients, and is increasingly being used as a secondary data centre for clients.

- We host and manage client equipment across 2 data centres;
- We work with clients in establishing DR plans;
- We work with clients in regularly testing DR plans.



ac3's second data centre is located within Global Switch, on the outskirts of the CBD.

ABOUT AC3

ac3 provides professional management services for computing and networking equipment to best practice standards. All equipment is housed in secure, fail-safe data centres at the Australian Technology Park and at Global Switch.

ac3 is a private company owned by the NSW Government and the universities of NSW. See www.ac3.com.au.