

# Key Elements to an Effective Business Continuity Plan

One of the biggest challenges in continuity planning is identifying and protecting essential elements. An effective plan must be departmentally broad, and consider the needs of the entire enterprise. The goal is to understand what is critical, and to encompass all of the necessary parts (personnel, network, platforms, applications and data) when evaluating the components that support critical processes. Good business continuity planning (BCP) needs to take a broad view, embracing people, human behavior, customers and other factors that lie outside the data center. It is also important to secure the vision (and endorsement) of executive management.

Effective planning includes a few basic steps: consider every part of the business, decide what is critical and determine how long individual departments can operate without some parts of their normal support systems. This prioritization is what should drive planning decisions. For example, if a function cannot be off-line for more than two hours, relocating people to a back-up data center will not be practical. What's needed is a secondary data center that can take on the additional load. The operational and financial cost of not having a critical function should also be considered. Without a failover call center, how much revenue would be lost if calls could not be forwarded in an emergency? How many customers would seek another supplier?

Planning for business continuity is similar to buying life insurance. When looking for a policy, the shopper must first decide how much insurance is needed. Only with a clear understanding of the need can a buyer make an informed decision about the purchase. The same principle applies to BCP – understand the fundamental requirements before evaluating potential strategies. Effective planning cannot begin without a clear understanding of the business functions that need to be supported, and the scope of what that support will entail.

Many BCP solutions are available, and the costs will vary. When considering budget in the planning process, keep in mind that faster recovery solutions tend to be more expensive because they usually involve pre-positioned assets.

### Don't Forget Security

Historically, business continuity plans have tended to focus on natural disasters: fires, floods, hurricanes and earthquakes. Security breaches must also be part of the overall plan. A virus-driven system failure could spread very quickly, compromising an entire world-wide enterprise. Any options proposed by a continuity plan should comply with existing production security standards and policies. Even if an enterprise is running in disaster mode, security procedures should not be compromised. Some minor disasters could even be engineered as way to gain entry to company systems and access to sensitive information.

### Developing the Plan

A key step in developing a plan is to establish the scope. This entails clarifying what is critical, and defining requirements for covering essential elements. In doing so, there are three useful metrics to keep in mind:

**Recovery Time Objective (RTO)** – The amount of time it will take to go from the point of disaster to the point of recovery. Simply put, the RTO indicates how long the business can be down.



**Recovery Point Objective (RPO)** – The amount of time between a disaster and the last full back-up. The RPO is a measure of how much data is at risk in the event of a disaster.



**Level of Service (LOS)** – This is a combination of throughput and functionality, and is an indicator of what services are essential. For example, a company might need the full functionality of its core financial systems, but not its analysis and forecasting systems.

By providing a general structure for its assembly, tools and templates can be helpful in developing a plan. However, key steps should still be followed, with or without a planning tool: set the scope, define the requirements, develop the plan and test. It's also a good idea to build the plan around a worse-case scenario, rather than planning for many graduated levels of disaster. If a plan can cover a "smoking hole scenario," it should not be difficult to adapt to less severe situations.

### Key Success Factors

While developing a Business Continuity Plan, there are four ingredients that will greatly influence its ultimate effectiveness: secure true executive sponsorship, establish a regular testing program, obtain sufficient funding and trust the people. These factors should be kept in mind throughout the planning process.

### Secure True Executive Sponsorship

Perhaps nothing is as important as engaging with upper management to clarify the big picture. Without executive guidance, planners tend to produce very expensive plans that cover every aspect of daily operations. The risk is these high-cost plans either may not be fully implemented, or may be put aside for later re-consideration. The company then

continues to remain at risk. One of the most challenging tasks in BCP is to establish executive consensus about:

- Which aspects of a company's business must stay operational in an emergency
- The exact level of protection that is necessary (RTO, RPO, LOS)

### Establish a Regular Testing Program

If a BCP is not tested, it may fail under the stress of a real disaster. The point of testing is to stress the plan, expose potential weaknesses and uncover what's missing. An efficient method to introduce testing is to look for ways it can be integrated with normal business operations. For example, servers need to be taken down for periodic maintenance. This is a perfect opportunity to conduct fail-over testing, without adding additional down time for systems.

### Obtain Sufficient Funding

Whether counting the cost of hardware, software or time, BCP is sometimes considered a good but non-essential practice. Surveys have shown that a surprising number of companies either do not engage in formal continuity planning, or believe their plans may not adequately address the problems of

a real disaster. An under-funded plan is a plan at risk. One option is to work BCP costs into whatever business cases are normally used to secure project funding. No project should be implemented if it does not include some budget to cover continuity issues.

### Trust the People

In an actual disaster, people can be incredibly inventive. They are more flexible than systems, especially in emergency situations. For example, in many companies, key work teams need little more than a laptop and an Internet connection to conduct business. These personnel could work from virtually anywhere, including: homes, alternate company locations, recovery centers or temporary office space. With systems, back-up strategies must be pre-programmed, with recovery destined to specific locations. In this situation, there are not many alternatives if recovery does not work, or if failover centers are also impacted.

Keeping these key factors in the foreground of the planning process will help ensure successful business continuity plans. A properly funded, well-prioritized continuity plan, combined with a regular program of testing and disaster recovery drills, will help to safeguard an organization.

**For more information on AT&T's Networking Exchange, visit [www.att.com/networkingexchange](http://www.att.com/networkingexchange).**



**at&t**

Your world. Delivered.