

Avoiding Business Continuity Planning Pitfalls

Increased risks, complexities, and new federal regulations have escalated the urgency to have an effective Business Continuity Program (BCP) that extends beyond the information technology domain. A project of this magnitude entails a myriad of details that require extensive attention and documentation—and, of course, pitfalls. Here are some suggestions for avoiding eight of the most common pitfalls.

#1 Lack of Executive Sponsorship

Since senior management and the board of directors are responsible for continuing operations in a safe, sound manner, BCP merits board-level attention, especially to enlist the entire organization's support. This doesn't mean that they need to write the BCP. However, the board and senior management should:

- Allocate sufficient resources to develop the BCP
- Set policy by determining how your company will manage and control identified risks
- Review BCP test results
- Approve the BCP on an annual basis
- Ensure that the BCP is kept up-to-date and employees are trained and aware of their role in its implementation

#2 Lack of Ownership

Since most businesses don't have a VP of business continuity, the BCP hot potato seems to bounce between IT, Operations, Risk Management, Facilities and Finance, eventually landing in the lap of an administrative person who does not have the authority to demand that all departments keep the plan current. Consequently, the plan becomes outdated and essentially useless.

Senior management must allocate sufficient resources to ensure that the plan stays current, employees are prepared, and regulatory guidelines are met.

#3 BCP is Considered an IT-only Issue

IT is responsible for recovering critical data, systems and applications – not how the company will continue operations to serve customers in the wake of a disruption. BCP is an enterprise issue, requiring the involvement of all departments.

The BCP should document:

- Disaster declaration guidelines –conditions for invoking the BCP and who is authorized to declare a disaster
- Emergency/crisis response – how your company ensures the safety of employees and customers and how incidents should be handled
- Communication – message to be shared with customers, employees, and media when a disaster is declared and who should deliver it

- Continuity procedures – manual procedures for continuing critical business functions while systems are being restored
- IT recovery procedures – procedures on how to restore critical IT services in an acceptable timeframe. This should be written with sufficient detail that a qualified IT person could recover the environment if key personnel were not available.

#4 Undefined BCP Priorities

Prioritizing the recovery sequence before the chaos of a disaster enables clear thinking during recovery and continuity, and minimizes disruption and severity. A Business Impact Analysis (BIA) involving all departments identifies critical business functions and prioritizes them based on impact to the organization.

At a minimum, the BIA should identify:

- Business functions each department performs
- Essential resources (IT, documents, dependencies, etc.)
- How quickly functionality should be restored
- Impact if recovery time is exceeded

Once priorities are established, senior management can assess risks and make informed decisions to guide the recovery process.

#5 Over-reliance on Outsourced Vendors

Companies that outsource back-office functions may erroneously believe that their vendor is solely responsible for their BCP. At the very least, review vendors' disaster recovery plans and test results to understand their recovery time commitment and your company's responsibilities during a vendor disaster.

Outsourced providers commonly commit to restoring service within 48-72 hours. If a vendor's commitment exceeds your expectation, then document interim operating and return-to-normal processing procedures and incorporate them into the plan.

If you use a vendor for "hotsite" services, make sure your contract either covers all critical systems and services that need to be recovered or have an alternate plan. And don't forget about increasingly important distributed (Intel) systems.

#6 Untested Backup and Restore

Data backup is a best practice for recovery from various disruptions. However, an estimated 20-plus percent of backups cannot be successfully restored, because they're on site or aren't tested.

Ensure data backup by:

- Saving critical files on a server instead of desktops
- Storing back-up tapes in a secure off-site location away from computer operations or at an off-site data protection provider
- Testing backups on a monthly basis



#7 Lack of Employee Awareness

Do your employees know company BC procedures and what their role is in a recovery situation? Do they know that the BCP exists?

An excellent way to increase employee awareness and preparedness is to practice response procedures in “tabletop” exercises in a conference room. Recovery team members walk through documented continuity procedures for responding to a real-life disaster scenario. This training also identifies areas for improvement and integrates BCP awareness into your corporate culture.

#8 Procrastination

Perhaps the most common pitfall is talking about BCP importance, but never acting. BCP is easy to push off to the next month, quarter or year. Begin now by making the process less daunting by establishing monthly or quarterly objectives to incrementally improve BCP preparedness. Remember, BCP is a program, not a project.

**By: Jeff Olejnik, President
Assurity River Group, Inc.
4500 Park Glen Road, Ste. 120
Minneapolis, MN 55416
952-230-6488
jolejnik@assurityriver.com
www.assurityriver.com**