Business Continuity Planning Checklist

When unexpected or even catastrophic events occur, businesses must protect their employees and continue critical operations that support their communities. To protect your business, planning is essential. As a business leader, you understand the strategic importance of a solid continuity plan. That's why Business Continuity Planning focuses multiple aspects of your business, making sure you can recover the technology and processes required to operate after an unforeseen failure in normal operations.

To help in your preparedness efforts, AT&T developed the following checklist. The checklist identifies important, specific activities that businesses can do now to prepare for an event.

1. Planning for the impact of an unexpected or catastrophic event on your business	Completed	In Progress	Not Started
– Identify a coordinator and/or team with defined roles for preparedness and response planning. Potential team members may include: Information Security, Operations, Systems, Police/Security, Physical Plant, Insurance, Legal Affairs, Public Affairs, Personnel Department, Comptroller, Audit Division, Safety Office and/or Emergency Response Team.	☐	☐	☐
– Conduct a business process and services inventory to understand which processes are mission-critical to the survivability of the business.	☐	☐	☐
– Determine acceptable levels of service during the recovery period, and what processes need to be maintained or restored first to keep the business running.	☐	☐	☐
– Identify essential employees and other critical inputs (sub-contractors, services, logistics, etc.) required to maintain business operations by location and function during the event.	☐	☐	☐
– Conduct a technology asset inventory to determine and document the mission-critical technology components, their location, how they're configured, and who is responsible for management.	☐	☐	☐
– Once key components are identified, determine what measures should be taken to protect and recover them.	☐	☐	☐
– Understand the rules or regulations governing your business operations. If you had a business failure, would you be able to maintain compliance? (Sarbanes Oxley, HIPPA, privacy, etc.).	☐	☐	☐
– Understand customer or business partner performance metrics/service level agreements to assess risk for breach of contract, or to put in place performance remedies for your customers.	☐	☐	☐
– Identify a budget: Quantify the potential costs of downtime or total business failure. Develop a business case to optimally invest in risk mitigation.	☐	☐	☐

2. Assessing your data and technology needs in the event of a failure in operations	Completed	In Progress	Not Started
– Determine the status of your existing disaster recovery plan. Do you have one and is it maintained? Have you tested the plan?	☐	☐	☐
– Determine vulnerability of your organization's technology infrastructure to natural disasters, including floods, fires, earthquakes, etc.	☐	☐	☐
– Set clear recovery time objectives for each of your business/technology areas.	☐	☐	☐
– Determine the need for off-site data storage and backup.	☐	☐	☐
– Develop a technology plan that includes hardware, software, facilities and service vendors.	☐	☐	☐

at&t

Assessing your data and technology needs in the event of a failure in operations (continued)

	Completed	In Progress	Not Started
– Secure clear understanding and commitment from vendors on your plan.	☐	☐	☐
– Secure a backup vendor, if necessary, to perform that critical function if your primary vendor is impacted by a business failure	☐	☐	☐
– Perform security risk assessments around specific threats where possible. Examples of data security include: virus protection, intrusion detection, hacker prevention, network events, component failures and systems crashes.	☐	☐	☐
– Assess, if possible and per prior events, how quickly and accurately your business and technology were restored by existing staff. What were the lessons learned so they can be addressed in future planning?	☐	☐	☐
– Determine the effectiveness of your data backup and recovery policies and procedures. Are the procedures fully documented and an appropriate staff member responsible for the maintenance of that documentation?	☐	☐	☐
– Perform a data recovery test. Was the test successful?	☐	☐	☐
– Prepare an incident plan for mitigating a security breach. Audit annually, as security threats can change.	☐	☐	☐

3. Communicating your plan to employees and vendor partners

	Completed	In Progress	Not Started
– Determine who needs to be contacted with critical information. Build distribution lists and maintain for accuracy.	☐	☐	☐
– Develop a contact plan to reach employees: wireless, home, etc.	☐	☐	☐
– Ensure employees know where to receive information and updates about whether they can return to work, or if they are to report to a different location (Internet, conference bridges, etc.).	☐	☐	☐
– Ensure mission-critical employees know their role in the plan and have access from remote locations (i.e., home broadband, phone, VPN for security).	☐	☐	☐
– Make sure the plan can be executed by alternate employees who are not necessarily the "expert" in cases where those employees cannot be reached.	☐	☐	☐
– Determine the need for a designated recovery site for your people to resume work. Plan for communications, data connectivity, desktops and workspace at that site.	☐	☐	☐
– If you require support from vendor partners, ensure they also have a documented plan that complements your needs. Review periodically to keep the plan current.	☐	☐	☐

4. Coordinating with external organizations and helping your community

	Completed	In Progress	Not Started
– Collaborate with your local government agency to share your plans and understanding of their capabilities in the event of a business-impacting catastrophe.	☐	☐	☐
– Share your plan with your building management so they have a clear understanding of their role in safely securing the building and your employees.	☐	☐	☐
– Share best practices with other business leaders in your community, chambers of commerce and business associations to improve community response efforts.	☐	☐	☐

Please visit us at www.business.att.com, under Products and Services, Security and Business Continuity, for articles, case studies and more or contact your account executive to discuss the how AT&T can address your business continuity plans.

at&t
Your world. Delivered.