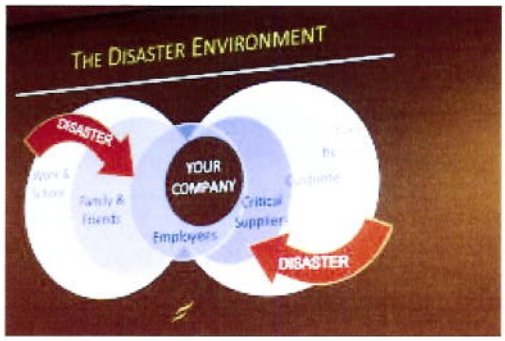
How to Create a Business Continuity Plan

A Business Continuity Plan (BCP) is the least expensive insurance any company can have (especially for small companies, as it costs virtually nothing to produce). Unfortunately, many companies have never taken the time to develop such a plan.



Here you will see suggested steps and considerations, in an abbreviated way, for *small* companies to create a BCP that will improve their chances of continuing operations during or after significant disasters. Development of a BCP for larger companies is not within the scope of this document.

Business Continuity Plans are sometimes referred to as Disaster Recovery Plans (DRP) and the two have much in common. However a DRP should be oriented towards recovering after a disaster whereas a BCP shows how to continue doing business until recovery is accomplished. Both are very important and are often combined into a single document for convenience.

Steps [edit]

1. **Document internal key personnel and backups.** These are people who fill positions without which your business absolutely cannot function – make the list as large as necessary but as small as possible. Consider which job functions are critically necessary, every day. Think about who fills those positions when the primary job-holder is on vacation. Make a list of all those individuals with all contact information including business phone, home phone, cell phone, pager, business email, personal email, and any other possible way of contacting them in an emergency situation where normal communications might be unavailable.

2. **Identify who can telecommute.** Some people in your company might be perfectly capable of conducting business from a home office. Find out who can and who cannot. You might consider assuring that your critical staff (identified in Step 1) can all telecommute if necessary.

3. **Document external contacts.** If you have critical vendors or contractors, build a special contact list that includes a description of the company (or individual) and any other absolutely critical information about them including key personnel contact information. Include in your list people like attorneys, bankers, IT consultants...anyone that you might need to call to assist with various operational issues. Don't forget utility companies, municipal and community offices (police, fire, water, hospitals) and the post office!

4. **Document critical equipment.** Personal computers often contain critical information (you do have off-site backups, don't you?). Some businesses cannot function even for a few hours without a FAX machine. Do you rely heavily on your copy machine? Do you have special printers you absolutely must have? Don't forget software – that would often be considered critical equipment especially if it is specialized software or if it cannot be replaced.

5. **Identify critical documents.** Articles of incorporation and other legal papers, utility bills, banking information, critical HR documents, building lease papers, tax returns...you need to have everything available that would be necessary to start your business over again. Remember, you might be dealing with a total facility loss. Would you know when to pay the loan on your company vehicles? To whom do you send payment for your email services?

6. **Identify contingency equipment options.** If your company uses trucks, and it is possible the trucks might be damaged in a building fire, where would you rent trucks? Where would you rent computers? Can you use a business service outlet for copies, fax, printing, and other critical functions?

7. **Identify your contingency location.** This is the place you will conduct business while your primary offices are unavailable. It could be a hotel – many of them have very well equipped business facilities you can use. It might be one of your contractors' offices, or your attorney's office. Perhaps telecommuting for everyone is a viable option. Wherever it is, make sure you have all the appropriate contact information (including people's names). If you do have an identified temporary location, include a map in your BCP.

8. **Make a "How-to".** It should include step-by-step instructions on what to do, who should do it, and how. List each responsibility and write down the name of the person assigned to it. Also, do the reverse: For each person, list the responsibilities. That way, if you want to know "who is supposed to call the insurance company?" you can look up "Insurance". And if you want to know what Joe Doe is doing, you can look under Joe for that information.

9. **Put the information together!** A BCP is useless if all the information is scattered about in different places. A BCP is a reference document – it should all be kept together in something like a 3-ring binder. Make plenty of copies and give one to each of your key personnel. Keep several extra copies at an off-site location, at home and/or in a safety-deposit box.

10. **Communicate.** Make sure everyone in your company knows the BCP. Hold training classes – mandatory training classes – for each and every employee whether they are on the critical list or not. You do not want your non-critical staff driving through an ice storm to get to a building that has been damaged by fire then wondering what to do next.

11. **Test the plan!** You've put really good ideas down, accumulated all your information, identified contingency locations, put your personnel list in place, contacts, service companies, but can you pull it off? One thing you will definitely learn in the test is that you haven't gotten it all just exactly right. Don't wait until disaster strikes to figure out what you should do differently next time. Run the test. If you make any major changes, run it again a few months later. Even after you have a solid plan, you should test it annually. Pick a day – let everyone know what's going to happen (including your customers, contractors and vendors) then on that morning, act as though your office building has been destroyed. Make the calls – go to the contingency site.

12. **Plan to change the plan.** No matter how good your plan is, and no matter how smoothly your test runs, it is likely there will be events outside your plan. The hotel you plan to use for your contingency site is hosting a huge convention. You can't get into the bank because the disaster happened on a banking holiday. The power is out in your house. The copy machine at the business services company is broken. Your IT consultant is on vacation.

13. **Review and revise.** Every time something changes, update all copies of your BCP. Never let it get

out of date. An out-of-date plan can be worse than useless: it can make you feel safe when you are definitely not safe.

Tips [edit]

- All critical personnel should keep a copy. It's not a bad idea to keep one in your car.
- Prepaid cell phones are an inexpensive option for emergency communications.In some disasters cell phones don't work so considering a satellite communications system may protect your ability to communicate.
- The binder you use for your BCP should be very distinctive – bright, neon orange is a good color.
- Keep your BCP out and visible so everyone sees it frequently – that way the idea of business continuity will stay on everyone's mind.
- Have a weather plan for your employees with a number they can call to get an update on conditions. Look into some of the new Internet phone services with a voice mail message.

Warnings [edit]

- Do not rely on a fireproof safe to store your computer media. Fireproof safes are designed for paper; a CD, DVD, floppy disk or a magnetic tape will melt. Get a media safe for those items. Better yet, store data off site!
- Do not make pirated copies of important software. Even if you can do that (often you cannot) they might not work, and you could create serious legal problems for yourself. Contact your software vendor if you don't understand your options.
- Do not distribute your plan to people that don't need to have it. Your plan will contain sensitive and secure information that could be used by a disgruntled employee for inappropriate purposes.