Business Continuity Plans (BCP) provide procedures for how employers and employees will stay in touch and keep doing their jobs in the event of a disaster or emergency, such as a fire at the office. Unfortunately, many companies never take the time to develop such a plan, typically because they do not feel it is necessary. However, creating a comprehensive BCP will allow you to enhance your company's ability to continue business as usual during or after significant disruptions to business operations.

Method 1 of 4: Understanding What Makes a Good Business Continuity Plan

Accept the potential threats and risks facing your company.

The possibility of a disruption shutting down your business operations is scary to think about, but you should always be prepared and willing to accept that risks and threats can cause turmoil for your business. Once you can accept that unplanned for risks and threats can have devastating results on business operations, you can then make a plan that ensures that both your business's assets and personnel are sufficiently protected.

- *Make a list of possible risks and their impact upon your company. For example, the death of a key person will not typically result in closing the doors for a while, but can severely impact results, supplier relations and customer service.*
- *After identifying risks, sort them by impact and livelihood to prioritize your planning.*

Don't confuse business continuity plans with disaster recovery plans.

Business Continuity Plans are sometimes referred to as Disaster Recovery Plans and the two have much in common. Disaster Recovery Plans should be oriented towards business recovery following a disaster, and mitigating the negative consequences of a disaster. In contrast, Business Continuity Plans focus on creating a plan of action that focuses on preventing the negative consequences of a disaster from occurring at all.

Consider the potential threats/risks facing the company. Business impact analysis (BIA) plans consider the potential consequences to your business when the ability to function and process has been disrupted by a threat or risk. As a result, creating a BIA allows you to determine which issues, risks and threats that your business

continuity plan needs to address. You should consider the possible effects a disruption to business operations could cause, such as:

- *Lost income and sales*
- *Increased expenses*
- *Customer defection/dissatisfaction*
- *Tardiness in service delivery*
- *Regulatory fines*
- *Delay/inability to commence future business plans.*

Method 2 of 4: Determining Key Recovery Resources

Make a list of key internal personnel. Following the occurrence of an event that disrupts normal business operations, you will need to quickly mobilize key personnel in order to successfully execute a BCP. Create a list of internal key personnel and backups --- these are the employee's people who fill positions without which your business absolutely cannot function. Make the list as large as necessary, but as small as possible.

Make a list of all key internal personnel with all contact information including business phone, home phone, mobile phone, business email, personal email, and any other possible way of contacting them in an emergency situation where normal communications might be unavailable.

Consider which job functions are critically necessary to continue every day operations. You should think about who fills those positions when the primary job-holder is on holiday.

Remember that key personnel do not just include high-ranking Directors. For example, a mid-level accounts clerk might be responsible for processing reports that show affecting loans or collections, which greatly affect the amount of available operating income. The accounts clerk should be considered key personnel, because that person's job function facilitates the company's access to capital provided by the processing of monies and the collection of funds.

Document critical business equipment

On-site business computers often contain the most critical information that you and your employees must be able to access even when working off-site. You should make a list of critical equipment/data, and create a strategy for secure access in the event

of a disruption. Don't forget software that would often be considered critical equipment, especially if it is specialized software or if it cannot be replaced.

This list should include passwords, identification data and the location of key files.

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?

Identify critical documents. You should compile all documentation necessary to start your business over again in the event of a fire or other disaster that destroys critical documents located on-site. Make sure that you have alternative copies in physical storage offsite and ways to access critical documents such as articles of incorporation and other legal papers, utility bills, banking information, critical HR documents, building lease papers, tax returns and other critical documents.

You should consider what the plan of action would be if there was 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?

Identify who can remote into the systems In the event that business operations cannot continue at the regular location, remote working from home is a great way for employees to continue doing work as usual. Your employees' ability to work, even when away from the office, will mean that at least some of the delays in performing work as usual can be avoided. Some people in your company might be perfectly capable of conducting business from a home office.

Find out who can and who cannot work from home because of internet connectivity limitations or other issues, and make sure to provide your employees with the necessary resources for remote working.

Method 3 of 4: Creating Your Business Continuity Plan

Identify contingency equipment options. Contingency equipment options are accessible equipment alternatives that can be used if and when normal business operations are disrupted.

Where would you rent trucks if a disaster damaged or destroyed vehicles used in the ordinary course of business? Where would you rent computers? Can you use a business service outlet for copies, fax, printing, and other critical functions?

Alternative equipment suppliers typically do not have to be identified specifically, unless they are unique and an arrangement has already been negotiated (very rare).

It is more important to identify the services, equipments and/or resources a substitute must be able to supply. The key personnel entrusted with the responsibility of managing the relationship with the substitute must have the necessary authority to make relevant decisions.

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 satellite offices or a contractor's office.

A storage rental facility near your regular site might be a great place to relocate and store products in a pinch.

Perhaps home working for everyone is a viable option.

If you do have an identified temporary location, include a map to the location in your BCP. Wherever it is, make sure you have all the appropriate contact information (including people's names).

Make a "How-to" section in your BCP. It should include step-by-step instructions on how to execute the BCP and address 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.

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 solicitors, bankers, IT consultants...anyone that you might need to call to assist with various operational issues.

Don't forget utility companies, community offices (police, fire, water, hospitals) and the post office!

Put the information together! A BCP is useless if all the information is scattered about in different places. A BCP is a reference document and 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.

Method 4 of 4: Implementing Your Business Continuity Plan

Communicate the BCP to relevant employees. Make sure all employees who could be potentially affected by a disruption have read and understand the BCP. Take the time to ensure that employees are aware of their relevant roles in the implementation and execution of the policy.

Provide essential BCP plan information to non-key personnel. Don't leave things to chance! Even if key personnel are informed about their role under the BCP, you should still make sure that all employees are aware of building evacuation procedures, as well as contingency locations. This way the unforeseeable absence of key personnel will not prevent non-key personnel from knowing how to respond to business operation disruptions.

Plan on modifying and updating your BCP, No matter how well your BCP, it is likely that there will be disruptive events that are not provided for in your plan. Be open to updating and/or modifying your BCP in light of additional information and/or changed circumstances. Every time something changes, update all copies of your BCP, and never let it get out of date.

Do not rely on a fireproof safe to store your computer media. Most 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 on a cloud platform!

Source: http://www.wikihow.com/Create-a-Business-Continuity-Plan