



Johnson & Sheldon, PLLC
Certified Public Accountants



Contingency Planning for Business Owners



A contingency plan is simply a backup plan for any disaster or emergency situation that may affect your business. Hopefully, you will never need a contingency plan, but it's always a good idea to have one in place. You should also update your contingency plan regularly to ensure it meets the current needs of your business.

Most businesses need a contingency plan. After all, every business is open to some amount of risk when a disaster strikes. However, because each industry has its own potential risks, contingency plans may vary drastically from one organization to the next. A contingency plan helps ensure that your business functions as close to normal as possible should an emergency arise. It also helps everyone involved focus on taking action and solving the problem rather than panicking and making the situation worse.



Creating a Contingency Plan

A contingency plan may seem complicated at first, but it's a fairly straightforward process. It's most important that you make the plan as organized and easy-to-follow as possible. You never know how people will react during an actual disaster; a clear plan helps everyone stay calm and take action when it's most needed.

#1 Identify your companies greatest risk

The first step of contingency planning is identifying your company's greatest risks. There are usually several different scenarios that can cripple your company. However, some are more likely than others. Your goal is to brainstorm all the possible scenarios, then identify the ones that are the greatest risks to your company. This includes the most likely events as well as the ones that leave your company open for the greatest exposure. Here are some examples:

- **Employee Risks:** What would happen if you suddenly lost a key employee?
- **Financial Risks:** What if you lost a major customer? What if you were not able to collect on your receivables? What if interest rates increase? How would a sudden economic downturn affect your business?
- **Operational Risks:** Do you have any key vendors or suppliers? Do you have critical equipment or computer systems that could fail? Are you exposed to a cyber attack, data breach or accidental loss of data? Do you rely on transportation systems, communication systems, the internet or power?
- **Act of God:** Are you susceptible to natural disasters such as hurricanes or floods?
- **Management Risks:** Are there risks related to theft or neglect of critical responsibilities?

The above list is just scratching the surface, but it is important to think through every aspect of your business to identify potential points of failure, both internally and externally. Keep in mind that some of the above scenarios occur quickly, with little to no warning (cyber attacks, weather), while others may occur more slowly, with increasingly negative effects (recession, a supplier going out of business).



#2 Identify Exposure and Likelihood for Each Risk

Next, you need to determine the exposure associated with each risk. Also, estimate the likelihood of each event happening. This may include:

Financial Exposure:

How will this risk affect your sales? How much will it cost to resolve? Are there any other expenses that may be linked to this scenario? Remember costs may be direct financial costs or lost opportunities.

Customer Exposure or Loss of Business:

Besides monetary exposure, how will this affect your business overall? Are you likely to lose customers? Will you need to scale back your business?

Reputation Exposure:

Will this type of disaster affect your business' reputation? This is most common with criminal activity or security risks, but it could be an issue with other scenarios as well.

#3 Create a Contingency Plan for Risks with the Greatest Exposure

You don't necessarily need a contingency plan for each and every scenario. Instead, identify the riskiest scenarios and start at the top of the list. Create your plan with the following questions in mind:

a. How is the problem identified? What defenses do you have in place to help prevent the risk? What are the signs that this specific disaster has taken place? A fire may be obvious, but cyber threats are often more subtle.

b. Who needs to be alerted first and where is their contact information? Who is the key contact point for handling this type of disaster? Oftentimes, this may be the owner or president of the company, but that's not always the case. For example, if it's a cyber threat, the head of your IT



department should probably be notified immediately because he or she has the knowledge to help stop the threat. You can make the owner or executive a secondary contact person.

c. How do you stop the bleed? What specific actions must you take to address the issue? Your best line of defense is to immediately take all the necessary steps to mitigate your risk. When discussing your contingency plans with employees, you should always stress the importance of addressing the situation immediately. Many people first attempt to identify the cause, but that's not always helpful. It's more important to stop the bleed then investigate the cause later during a post mortem.

d. How do you communicate with all stakeholders – customers, vendors, and employees? At some point, you will likely need to address the situation with your employees, customers, and possibly even the general public. To help this process go smoothly, make sure all contact information is held outside of your main systems. You also need to have the ability to communicate via email.

The key here is to prepare your communications in advance so you can notify everyone as quickly as possible. If you're a software company, set up a status page. Prewrite emails and store them as drafts. Finally, make sure you know who must approve any communication ahead of time.



#4 Run Through the Plans with Employees

Once you have your contingency plan in place, you should go over the plan with your employees so they know how to handle an actual emergency. Make sure you include the details of each scenario. Your employees may see holes in your plans or have additional knowledge that can help streamline the processes. They may even think of scenarios you haven't included in your contingency plans at all.

#5 Organize and Safeguard your Contingency Plans

The final step is to organize your plans and store them so they're easily accessible during or after an emergency or disaster. It's best to keep at least one paper copy organized neatly in a three-ring binder. Of course, you should also store a digital copy in the cloud so you can access the file remotely if necessary. Safeguard the plans with locks and/or passwords to limit access to key personnel. Make sure each person knows they are responsible for retrieving the plan should the situation arise.

It's always a good idea to give a few people access to the contingency plans in case the primary person isn't available. In fact, many companies like to assemble a Contingency Plan team, which is simply a group of people who are in charge of regularly reviewing the plan, maintaining any tools or resources needed, and implementing the plan if necessary.



Final Thoughts

Contingency planning often falls onto the back burner within a business environment because it doesn't seem urgent. However, it should actually be a priority because disasters are more common than most people realize.

If you need assistance with your contingency planning or have additional questions, our experts are always happy to help. Contact our office for more information.



About Johnson & Sheldon, PLLC

Johnson & Sheldon, PLLC is professional corporation that has established itself as one of the leading, aggressive accounting and consulting firms in the Panhandle Region of Texas. Our clients have been relying on the experience and guidance of our partners, Terry Sheldon , Richard Blankenship and Jeff Joyce for over 30 years. Located in Amarillo, Johnson & Sheldon's client base consists of small to medium size mostly privately-owned business and organizations. J&S is a member of the RSM US Alliance, the nation's fastest growing association of independent accounting firms. Through our affiliation with this network, Johnson & Sheldon, PLLC can offer the pooled expertise and resources of the RSM US Alliance, as well as other network members.



Amarillo Location

500 S Taylor St., Suite 200
Amarillo, TX 79101
(806) 371-7661



Hereford Location

119 E 4th St.
Hereford, TX 79045
(806) 364-4686



Pampa Location

420 Florida St.
Pampa, TX 79065
(806) 665-8429



info@amacpas.com



www.amacpas.com

