A Step-by-Step Guide to

Create a Highly Effective Small Business Continuity Plan

PICS ITech
www.pics-itech.com

Table of Contents

Introduction

To help you understand the importance of creating an effective small business continuity plan, here are a few statistics that prove just how common emergencies are and how impactful they can be for the average small business.

- Ransomware attacks increased by 250% last year
- 1 in 131 emails contain malware
- 43% of cyberattacks are aimed at small businesses.
- The U.S. Bureau of Labor reported that 93% of companies that experience a data disaster go out of business within 5 years
- They also reported that 95% of all organizations experienced a data outage in the past year.

Disasters come in all shapes and sizes and being unprepared is no longer an option when it comes to ensuring the longevity of your business.

That's exactly why we created this guide.

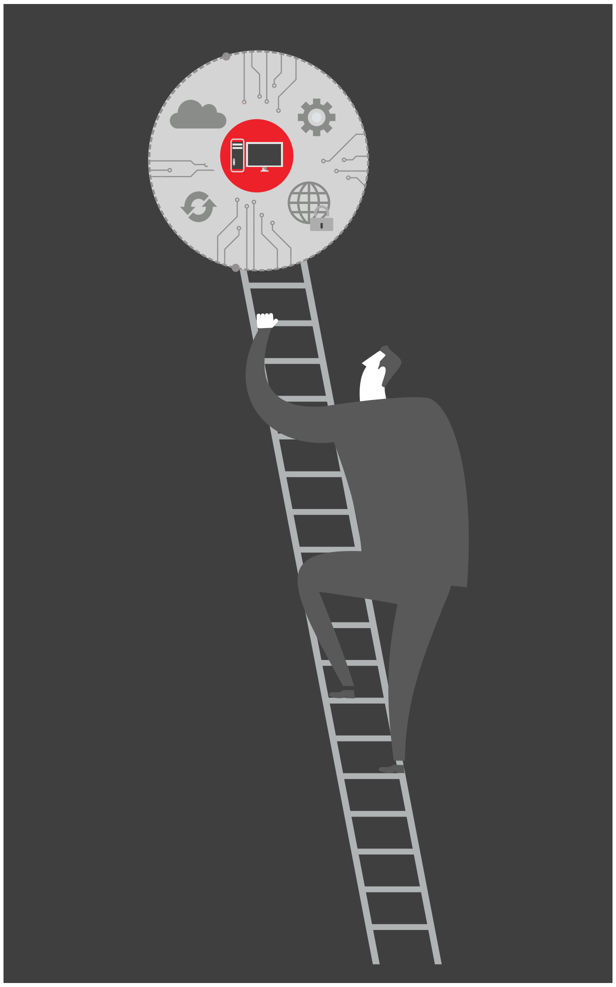
We're about to take you through the step-by-step process of creating a highly effective small business continuity plan, so **let's get started!**

What Is Business Continuity?

What Is Business Continuity?

Business continuity (BC) is a small business' ability to maintain and/or resume business functions quickly after an emergency incident. In the case of a storm that knocks out the phone lines for multiple days or your internet goes out for a week, how do you get up and running as quickly as possible so that you can continue serving your customers and making money?

Your BC plan is where you outline the specific steps you'll take to restore order. It includes the procedures—with instructions for the people carrying them out—ultimately ensuring that everyone knows exactly what has to happen and what they need to do in the event of an emergency.



More than Disaster Recovery

Business continuity is often found lumped together with disaster recovery (DR), but DR is just one part of an effective BC plan and is typically focused specifically on your data. BC looks at the bigger picture and includes business processes, HR, business partners, assets, and the continuity of your entire company.

To give you an example of the scope of the plan you'll be creating, imagine your call center that handles all of your customer service calls is lost in a fire. What measures do you need to have in place in order to ensure those reps can continue fielding calls? Do you need to establish a backup location or a systems that allows them to work remotely, even temporarily?

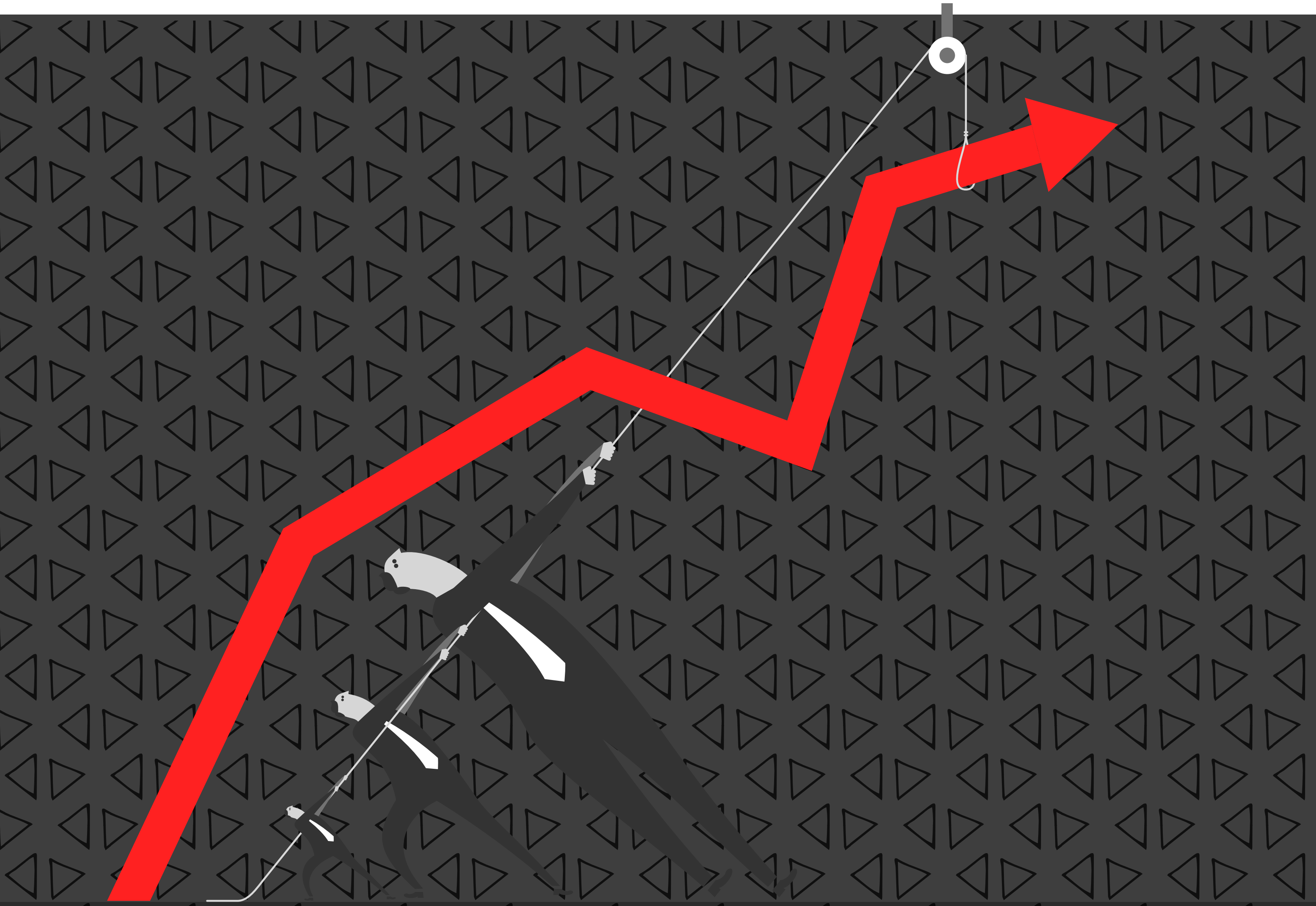
A more likely scenario, say your electricity, internet or phone goes out for 3 days after a major storm (think Hurricane Sandy). If you're phones go unanswered will your customers assume you've gone out of business. These are the types of things your business continuity plan will account for.

More than a Business Impact Analysis

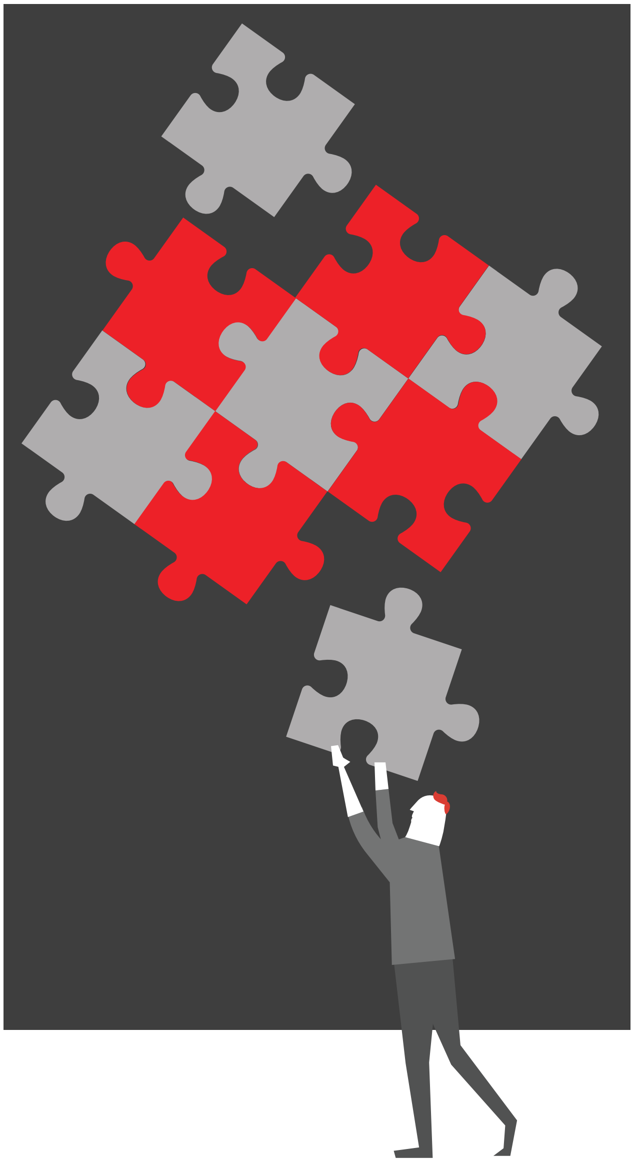
A BC plan is also sometimes confused for a business impact analysis (BIA), but again it's just one aspect of BC. Conducting a BIA helps you to understand what impact an emergency situation might have on your business, but doesn't necessarily include the steps necessary to remedy these issues.

A BIA is an important aspect of your BC plan because it can help you to determine whether or not it makes sense to outsource some or all or your BC activities. By identifying which of your business activities are most critical to your operations, you'll be able to determine which represent a priority that might be deserving of professional support.

Why You Need a Business Continuity Plan



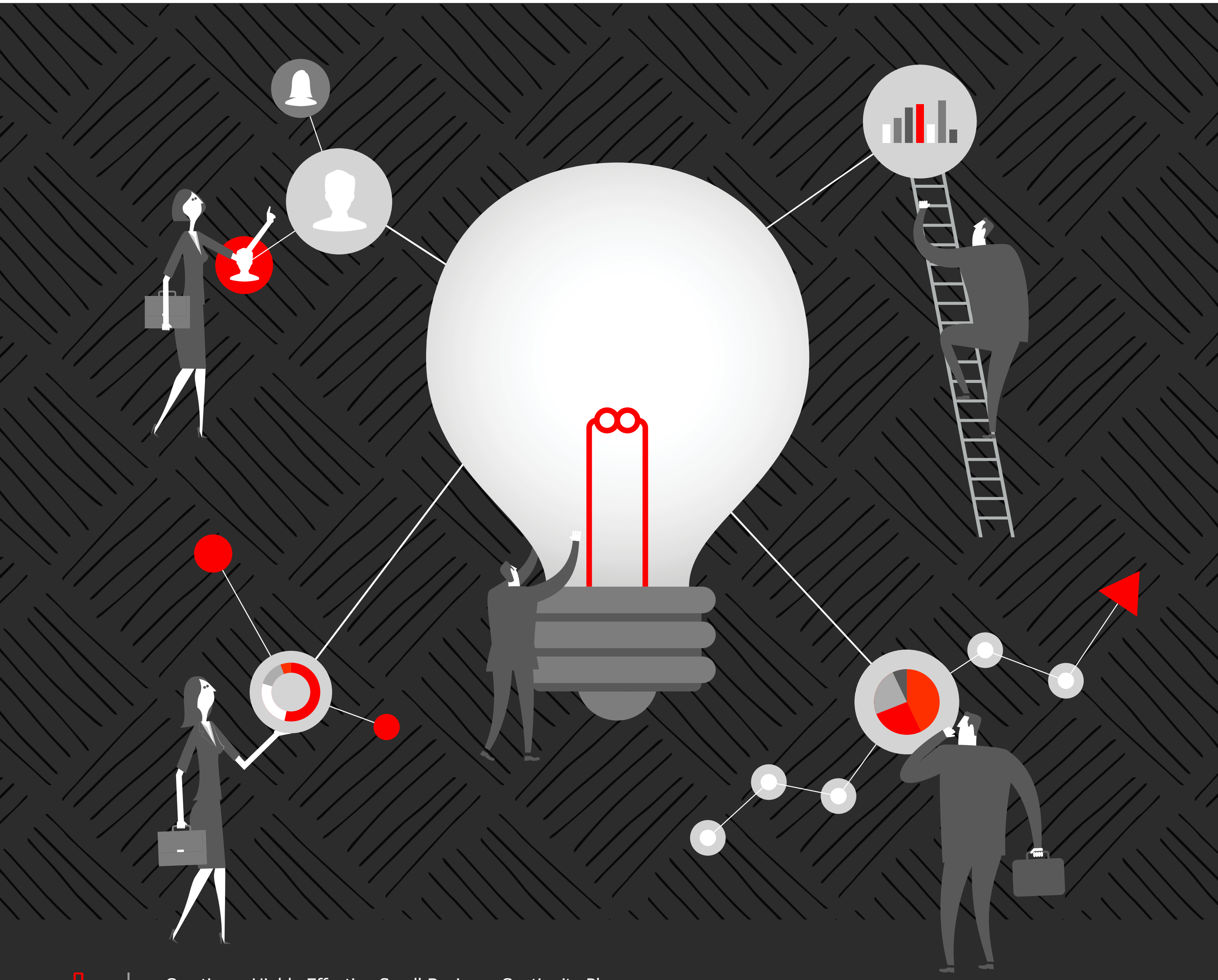
A BC plan does more than designate what happens in the event of a disaster or emergency; it allows your business to continue to operate at the highest possible capacity. That means you're able to continue generating revenue and serving your customers. It also means that you'll have a much better chance of minimizing losses during that time and, more importantly, surviving a true disaster.



Many businesses operate under the presumption that they'll never be impacted by such a disaster. However, when you consider the combined occurrences of natural disasters, infrastructure failures, internal errors, malicious attacks, and any number of other emergency situations, operating without a BC plan in place is a risk that no business should take.

In any case, a business continuity plan can support your external and internal communications, prepare your employees to work together in the event of a disaster, helps them understand the full scope of how your business works, and reduces the downtime you experience and the significant cost associated with it.

6 Steps to Your Highly Effective Business Continuity Plan



1 Step 1: Threat Assessment

Start your planning process by determining the actual emergency situations that your business might face. Obviously if you're not in a hurricane zone, planning for one would be a waste of time and resources.

However, work to include threats that may not be as apparent but still represent a very real risk. That includes:

- Any natural disasters you may be susceptible to
- Fires and flood caused by electrical or plumbing issues
- Internal errors
- Internal or external theft or loss of hardware or data
- Internal or external malicious attacks
- And anything else that may affect your business

You'll find that the list of potential threats is probably much larger than you originally assumed. In this step, be sure to assign a scoring system that helps you understand the likelihood of each threat actually unfolding.

2 Step 2: Internal Assessment

Do your best to evaluate what impact each emergency could have. Not the cost, but the actual things you'll lose.

For example, an earthquake that levels your building would have a different impact to a pipe bursting and flooding anything located on or near the floor. A malware attack that encrypts all of your data might affect you differently than the theft of a laptop.

Document the unique potential damages of each of the threats you outlined in Step 1. Then move onto Step 3.

3 Step 3: Business Impact Assessment

Once you understand and have documented the potential threats facing your business and how they may affect you, it's time to go into further detail about what that loss would actually cost you.

Evaluate the downtime that each threat would produce and the extent of that downtime. Certain disasters are going to affect your entire company while others may only impact certain departments or physical locations.

It's important to estimate your projected time to get up and running again in order to accurately assess the total cost of each threat. Furthermore, consider the total costs of customers losing faith, moving to other suppliers, loss of goodwill, bad publicity and so on.

Once you understand the extent of the associated downtime, work to evaluate exactly what that downtime costs based on your current data. The more accurate you're able to be during this step, the better you'll be able to prioritize the development of your procedures.

4

Step 4: Fundamental Information

Internal data

Include the necessary contact information for all supporting employees and external resources, as well as any relevant information that would support contacting them more successfully. Also, It's important to include IT and alarm companies, HVAC, insurance companies and agents and any other outside providers that you'll need to reach to get your systems up and running again.

Role Assignments

Each threat may require different people to be involved in different processes, but those responsible for certain aspects of your business will likely be in charge of those things for each potential emergency. Be sure to include any additional information that would be vital to understanding their roles.

Also, be sure to include information on who exactly can declare an internal state of emergency to implement your BC plan.

Descriptions and Terms

Depending on the type of disaster, the people executing your BC plan may need to change. Be sure to include short descriptions of each role as well as a glossary of terms and any information that might otherwise keep someone from taking action.

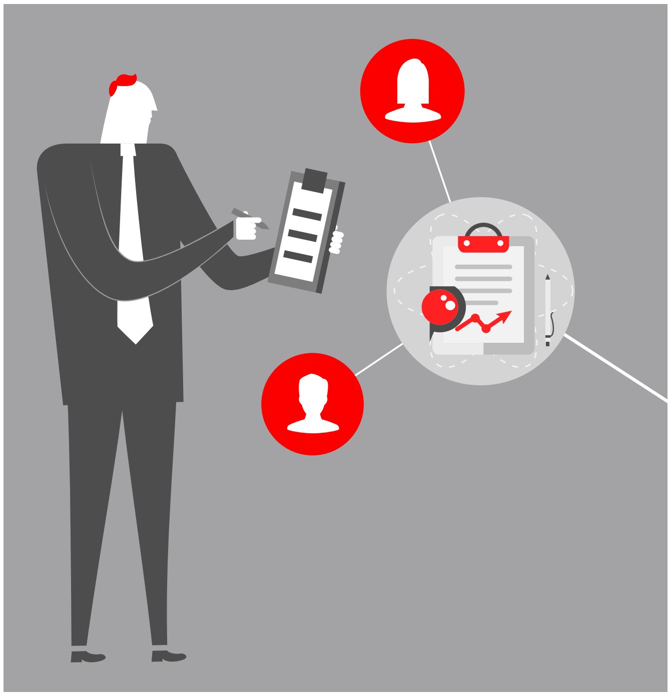
This is also the section where you would include the specific situations that designate an emergency and that your procedures be initiated.

Purpose and Scope

In order to help anyone reading the document understand why they're doing what they're doing, include a brief written description about the purpose of each procedure. In situations where a procedure can be carried out exactly according to plan, this will help the people involved sidestep any roadblocks that may have occurred.

Maintenance Outline

We'll cover testing your plan in much greater detail in an upcoming section, but be sure to include a section in your document that indicates how often your BC plan needs to be tested and who is responsible for testing and maintenance.



5 Step 5: Procedure Development

Once you have all of your assessments complete and fundamental information in place, you'll be ready to move onto the development of your procedures. A good BC plan is not complete until you've developed procedures to respond to each of the threats you identified in Step 1. However, approach your procedure development based on priority. The more substantial the cost of a threat and the more likely it is to happen, the higher a priority it is to plan for.

Document the following for each of the threats in Step 1:

Onsite Actions
There will be a series of on-premise actions that need to be taken in order to respond to each disaster. Be sure to outline every item and organize them by priority to ensure your mission-critical systems are up and running as soon as possible. This could be conducting inventory of your assets or installing backup hardware.

Offsite Actions
There will also likely be a series of actions that need to be taken off-site in order to ensure business continuity. This could be securing your predetermined backup location, or involving any vendors required to establish your internal network or systems

Roles and Designated Responsibilities
The roles you outlined in the fundamentals section likely won't change, but their exact responsibilities will. For each of the roles involved in responding to a threat, be sure to outline the exact items that they'll need to complete in order to accurately follow your procedure.

Checklists and Flow Diagrams
In order to ensure each of the necessary actions are being taken according to your procedures, create a series of checklists. Organize them by role in order to ensure nothing gets missed. You may also want to create flow diagrams that helps everyone understand the overarching process and exactly how it should be carried out.

Damage Assessment
To fully understand the scope of your emergency, a damage assessment should be carried out as soon as possible. This will also allow help to uncover any and all issues that need to be addressed in order to return to full capacity. Make sure the roles responsible for this assessment are not already responsible for restoring other mission critical systems.

Additional Information
There will likely be a variety of details not included in your fundamentals section that your people will require to complete the procedure. Be sure to include vendor contacts, emergency team information, alternate locations, and any other necessary information as it specifically pertains to restoring your company's operations.

Customer-Facing Details
Most of the information included in your plan will be focused on restoring your internal operations as quickly as possible in order to ensure you can continue serving your customers. Be sure to include any additional information or action items that you'll need to undertake in order to keep customer interactions flowing as smoothly as possible.

Depending on the situation being addressed, that could include how you'll remain in contact with your main phone lines out of order or how you'll process their orders. After all, the whole point of creating a BC plan is to ensure as little downtime and loss as possible.

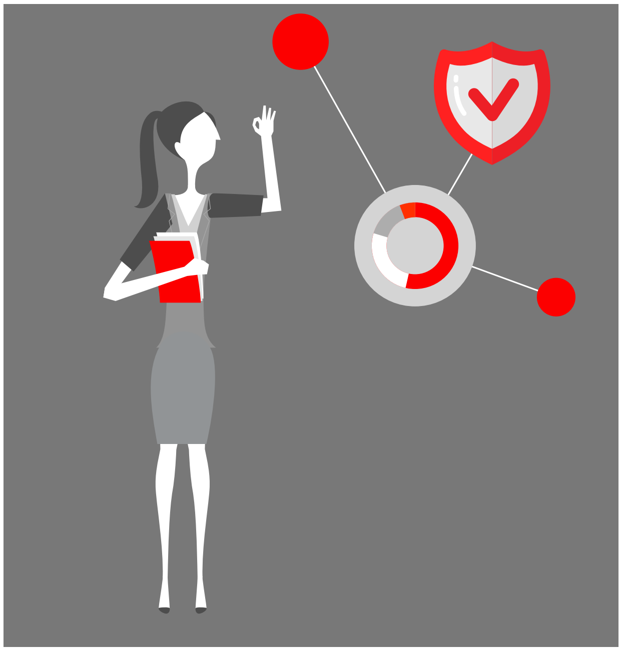
6 Step 6: Testing and Maintenance

What would constitute a highly effective business continuity plan today may not be so effective next year, or even in a few month's time for that matter. Testing and maintenance is one of the most important aspects of business continuity and should be approached with the same level of care as your original plan.

Unfortunately, many businesses create their BC plan once and assume it will be there for them whenever disaster strikes. We'll be the first ones to tell you that your BC plan needs to be tested and updated based on your results on a regular basis.

Make Someone Accountable
Assign someone to manage the testing and updating process, or a team of people responsible for different areas of the plan. (ie: Customer Service, Manufacturing, IT etc.) They won't be responsible for the entire testing process, as your whole company will need to be a part of that. Instead, they'll make sure testing is done regularly enough, as well as get all relevant employees to participate when testing is due. Finally, they'll be the one to update the document according to the feedback from the rest of your team.

Test in Stages
You don't need to test every aspect of your BC plan at once. Instead, break it into more approachable chunks. Test for a single threat or a few during one testing session, then focus on another when the next testing session comes around. You'll need to prioritize higher risk threats and ensure they are tested more frequently.



Check for Updates
Be sure to inspect any components of your plan that evolve or change. That could be something as simple as updating roles when employees leave or when new employees join the team. However, you'll also need to determine if any of your technologies are becoming obsolete or if your vendors are still able to support the elements of the plan in which they are involved.

Furthermore, you'd be well served to regularly update the initial steps of this process. You may find that new threats have presented themselves or the impacts of those threats have changed. The better you understand current threats, the better you'll be able to properly prepare for them.

Business Continuity Best Practices

1 - Make things easy.

Your BC plan needs to be as streamlined as possible in order to get you up and running as quickly as possible. Avoid excessive steps or unnecessary additions where possible.

2 - Make it short.

When it comes to your actual BC plan document, be sure not to get carried away explaining things in too much detail. Work to keep your document clear and concise.

3 - Get feedback from your employees.

Look to their experience solving problems to optimize your BC plan.

4 - Allow more time.

Even in the best of situations, you may need more time to complete each step of your plan. Incorporate that into your execution.

5 - Prioritize testing.

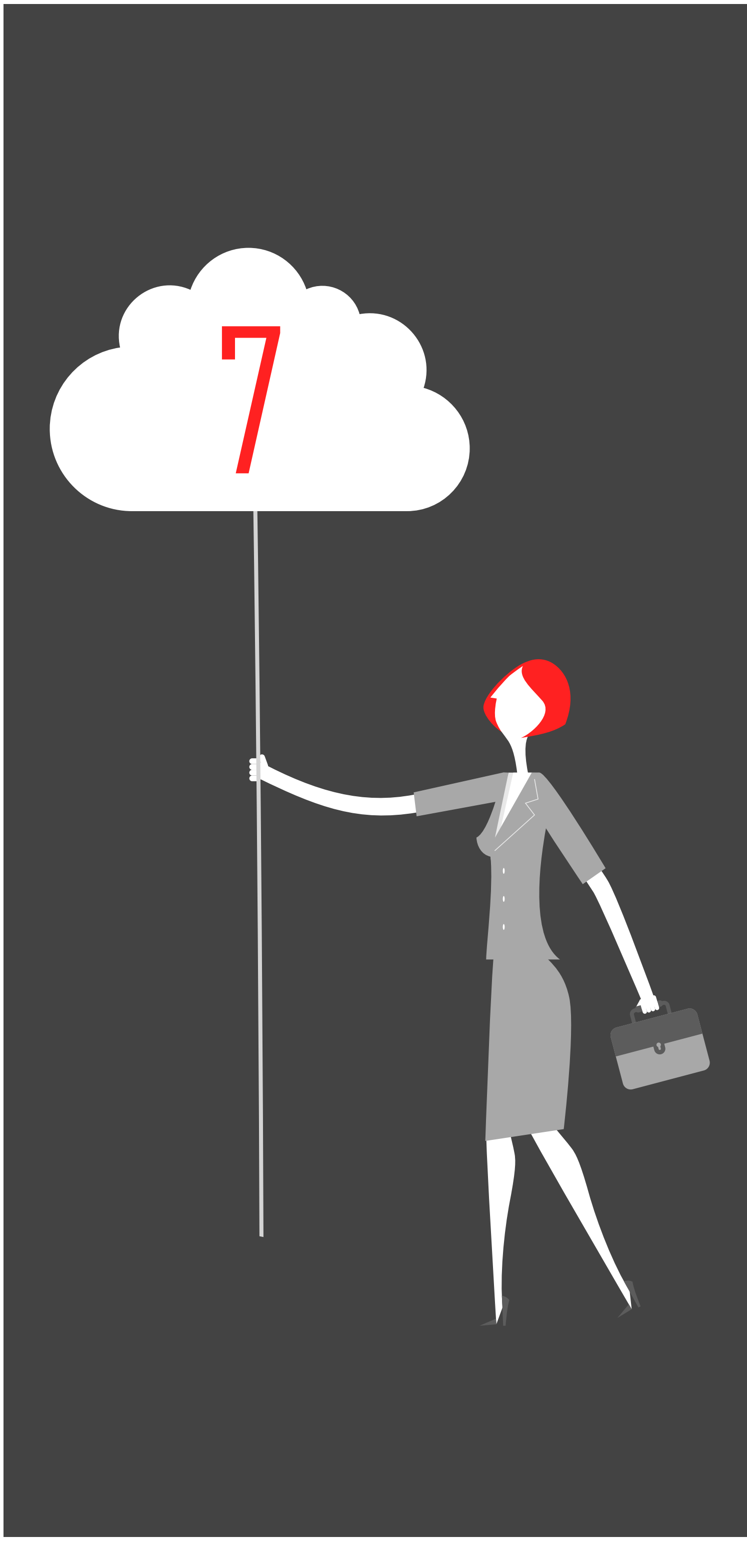
Regularly testing is vital to the successful execution of your BC plan. Be sure not to let other business priorities get in its way.

6 - Involve anyone responsible in the testing process.

Everyone who has a role in your BC plan should be responsible for testing the current plan and their ability to carry out their responsibilities accordingly.

7- Get help.

Business continuity is critical to your business's longevity, but not every company has the time or personnel available to create a highly effective BC plan. Fortunately, hiring an MSP allows you to delegate the some or all of the responsibility to expertly trained professionals.



Next Steps

Now that you have a deeper understanding of the threats facing your small business, it's time to take action. Establish a plan to protect your business in the face of both external and internal threats and dramatically improve your ability to recover from a disaster.

If you need help creating your plan or have determined that you may need to outsource some of your BC responsibilities **we'd love to help** you better understand your needs and how to go about meeting them most effectively.

ABOUT PICS ITECH

PICS ITech, co-founded by Terry Rossi and Richard Rosenthal, has been helping small businesses optimize their internal and customer-facing IT initiatives since 1995. They've worked with companies from around the world in nearly every industry to help them establish and implement highly effective IT strategies. PICS is continually working to improve their abilities in order to stay on the cutting edge in the ever-evolving world of information technology.

PICS ITech
www.pics-itech.com

46 High Street
Mount Holly, NJ 08060
United States

Phone: 609-614-3223
Emergency Support: 609-702-3920
Fax: 609-702-3915