Agility Recovery

Collection

Storm Season Preparation for Businesses

Resource Collection

Introduction

Each year disasters cost U.S. businesses billions in lost revenue and operational downtime. At Agility, our mission is to help businesses reach maximum resilience by providing end-to-end recovery services for organizations across North America.

With more than 34 years of experience helping organizations recover quickly, we know that preparation is the cornerstone of resilience. Use the resources in this collection to ensure that your business has everything needed to effectively prepare for and recover from any weather-related interruption. (New paragraph) To learn more about Agility and explore recovery solutions visit agilityrecovery.com. To reach a recovery expert, contact us via email at **contactus@agilityrecovery.com** or call **866-364-9696**.

Table of Contents

Guide

The Definitive Guide to Disaster Planning

12 Proven Best Practices to Protect Your Business from Workplace Threats

Table of Contents

Introduction

A lot is asked of today's business leaders. And the challenges faced on a daily basis already occupy the lion's share of a leader's time. However, in addition to other strategic initiatives inherent to the role, leaders must also be confident in their ability to maintain critical operations despite business interruptions.

Revenue generation, customer satisfaction, employee well-being and legal or contractual obligations can all be dramatically impacted by even the smallest incidents, not to mention the larger scale, regional events that are increasing in frequency and severity across the globe. Even if an organization is located in a low-risk area for natural disasters, man-made and isolated incidents pose an ever-present threat.

For this reason, robust, well-led organizations must have a disaster plan in place to overcome a variety of business interruptions and ensure your organization can:

- Recover from any disaster
- Protect your source of revenue
- Fulfill moral responsibilities to stakeholders
- Facilitate compliance
- Reduce exposure to civil or criminal liabilities
- Enhance your organization's image and credibility
- Potentially reduce insurance premiums
- Build organization-wide consensus and a culture of preparedness

The responsibility of ensuring the viability of an organization lies with senior management. Therefore, steps must be taken to establish a business continuity program and prepare to overcome interruptions. This will allow your organization to satisfy moral obligations to employees, clients, and the community, as well as fulfill compliance responsibilities to customers, stakeholders, and regulatory entities.

The remainder of this guide will outline the most basic, yet impactful steps any organization should take to build resilience in the face of all manner of threats. In many cases, these steps will not require complex, long-term projects for implementation, nor significant capital investment. Instead, much of the commitment simply depends on prioritizing the attention of your organization and building a company-wide culture of preparedness.

The hardest step is often the first when it comes to implementing such a strategy, but with the help of the following guide, the road toward preparedness does not have to be overwhelming.

Assemble a Disaster Team

There is perhaps no more important element to a successful disaster strategy than gaining support and buy-in across your organization. Additionally, an effective strategy cannot be created nor implemented without the help of others. Therefore, obtaining leadership approval is an important first step that is necessary for gaining support and funding for each element of your plan.

Leadership buy-in is critical for both the implementation and execution of your strategy. Of course, building a capable team will also set you up for success. Therefore, you should involve your employees in the disaster response planning process to let them know you're ready for whatever crisis may occur and build buy-in towards a culture of preparedness. By working together, you can design a plan that will accommodate the challenges faced throughout the organization during a disaster.

Responsibility of the Disaster Team

- Provide guidance, oversight and approval of resources for the continuity program.
- Facilitate the implementation and routine testing of the program.
- Ensure collaboration and buy-in across all departments.
- Execute the plan should the need arise.

When assembling your team, it's important to include members from all departments of the organization. Downtime after a disaster affects departments in various ways. Involving all departments allows for equal consideration of priorities and critical tasks, as well as protects any critical inter-dependencies.

Once you've chosen your team, it's key to establish clear communication and focus on the same goals. Here are some tips for building a high level of consensus among your team:

- Determine and agree upon high-level goals and prioritization (goals may include safety, physical security, or fiscal well-being).
- Solicit input from all involved.
- Ensure buy-in for resource allocation.

When Assembling Your Team, it's Important to Include Members From All Departments of the Organization

Team members must have defined responsibilities, tasks, schedules, and deadlines in order for your plan to succeed. The distribution of tasks will depend on the size of your organization, and roles may not necessarily relate to current job descriptions.

Possible Roles Include:

- Disaster team leadership
- Spokesperson/ communications
- Facilities management
- Financial oversight
- Vendor/supplier relations
- Data/technology
- Safety/security

Understand Your Risks

Identify. Prioritize. Mitigate.

It is necessary to consider all possible incidents and the impact each may have on your organization's ability to conduct essential operations. Properly identifying and prioritizing risks allows you to focus mitigation efforts in the most effective areas.

Identify

Areas of potential threat include:

- Weather-related disasters (consider the historical record of any catastrophic, naturally occurring events in your area).
- Facility location (consider your geographic location and your proximity to potential threats originating nearby, such as power grids or major transportation corridors).
- Facility design/construction.
- Technology failures.
- Isolated incidents.
- Supply chain disruption (risk to your organization extends to all of the external vendors and suppliers you rely on to deliver your everyday services and products to clients).

Prioritize

The best way to understand and prioritize risk is by using this basic formula:

Risk = probability x impact

You want to focus mitigation efforts on the risks with the highest importance, measured by multiplying the probability that an event will affect your organization by the impact that event would have on business operations.

Example:
On a scale of Probability (1 to 5) and Impact (1 to 5)

Nuclear disaster:
Probability 1 x Impact 5 = 5

Lost access to building due to plumbing issue:
Probability 3 x Impact 3 = 9

Though a nuclear disaster seems scarier than a plumbing issue, the latter is the risk your organization should be more focused on managing.

When quantifying your threat exposure, think about how the impact will relate specifically to your critical business functions (discussed in Step 3)

Mitigate

Develop a strategy to mitigate your risks, and manage risks that cannot be mitigated. (For more on this, see Step 4)

Three options to mitigation:

1. No cost solutions (ex. moving power source away from the ground floor).
2. Solutions that require an investment or cost your organization is able and willing to accommodate (ex. purchase of an on-site generator).
3. Solutions with a cost your organization cannot endure, and thus must be insured against (imagine a building fire that destroys the entire facility, including all equipment).

Determine and Prioritize Your Essential Business Functions

Critical business functions are activities that are vital to your organization's survival. Your needs will depend on your organization, and you should consider what it is that makes you who you are in the industry. For example, although protecting revenue is a key concern for most organizations, revenue generation is actually the outcome of a myriad of other functions within a company.

Even for industries that rely on a direct-to-consumer transaction of products or services, ensuring quality and delivery timeframes may be critical processes that lead to satisfying customer demands. Keep in mind, the process of identifying your critical business functions will require careful cross-referencing with findings from your risk assessment analysis.

Typically, critical business functions are functions that:

- Affect the safety and security of employees, customers and guests.
- Are the most sensitive to downtime.
- Fulfill legal or financial obligations to maintain cash flow.
- Play a key role in maintaining your market share and/or reputation.
- Safeguard an irreplaceable asset.

Properly determining and analyzing your essential business functions will allow you to prioritize those functions and best prepare to keep them in operation during a disaster.

Determine and Analyze Essential Business Functions

To document the impact on your organization from an interruption, conduct a simple Business Impact Analysis (BIA), using these steps:

1. Divide the organization into functional business units.
2. For each business unit, identify all routine and critical functions, their major attributes, and any inter- departmental dependencies.
3. Identify the staff that must be available and actively working for the function to remain operational.
4. Specify any equipment, applications, or tools that must be available to active staff.
5. Estimate the maximum amount of time your organization can remain viable without this function in place (consider that the more immediate you need something recovered, the more it will cost).
6. Determine the impact (both quantitative and qualitative) that the loss of this function has on your organization.

> ***Keep in Mind***
> *Be sure to consider and incorporate the loss of outside vendors, suppliers, service providers and other aspects of your supply chain on the function in question.*

Prioritize Functions

Once you have analyzed your essential operations you are equipped for prioritization, which is crucial due to realistic limits to time, money, and resources during a disaster. To determine priority, most organizations simply consider each function's criticality, which can be determined using the following guidelines:

- The organization objective/goal the business function supports
- How often the business function occurs
- How many departments perform the business function
- Whether or not the successful completion of the function depends on any other business functions
- Whether or not other business functions are dependent on the task of their successful completion
- If there is a potential for significant revenue loss if the business function is not performed
- If there is a potential for fines, litigation, or other punishment for noncompliance due to a regulatory requirement
- If noncompliance is tied to a specific downtime for the function
- Whether or not the function directly impacts your business image or market share of your organization

Following these guidelines will enable you to give each function a priority ranking within the entire organization's functions. Once you have completed this process for all your essential operations, you will know which business functions you need to address more closely as you create your crisis management plan.

This process may seem intimidating, but it can be accomplished efficiently through collaboration. Stay focused, start small, and keep it simple.

Create an Emergency Management Plan

Now that you've assessed the risks your organization faces and analyzed your critical business functions, you will use those conclusions to identify and consider available mitigation and recovery strategies. Begin by considering each of the Critical Business Functions discovered, and develop plans and strategies for protecting each from the top risks posed to your organization.

This is where all your discovery will begin to take the form of detailed strategies. That's why it's essential to invest enough time to specify all of the steps, including their anticipated timeframes and required resources.

Tasks:

1. Mitigate potential risks (when cost effective)
2. Develop options to establish continuity procedures that will protect critical functions and processes should threat actually occur and require recovery
3. Document and vet proposed recovery strategies, while determining the scope and required resources such that a cost-benefit analysis can be conducted for each proposed strategy

Establish how your organization's critical functions will continue to operate immediately after an incident. This may include details about functioning with reduced staff, replacing compromised systems, offering partial services, relocating staff and operations, communication protocols, and mitigation or recovery procedures.

Establish how actual logistics will proceed in terms of precisely outlining and adhering to timelines, decision points and verified procedures.

Establish in detail the required resources needed for mitigation and recovery. Required resources will vary by organization and function widely, therefore guidance should be sought from the findings of your Critical Business Functions to properly detail and comprehensively outline.

Establish the procedure by which the Emergency Plan will be enacted. Who can to declare the disaster or put the plan into action?

Not every strategy is either warranted or worth the investment. A simple cost-benefit analysis should be undertaken at this stage of the planning process to ensure that any recommended element of the strategy properly fits the organization's needs and resources available.

A Good Emergency Management Plan Will:

Establish who will participate on the Recovery Team and include detailed descriptions of their responsibilities. Roles and responsibilities can include:

- Life Safety Protection
  (protect employees, guests, and the general public)
  - First aid
  - Protective equipment
  - Evacuation planning
  - Shelter in place planning
  - Emergency response training
  - Alert notification

- Incident Stabilization
  (keep the incident from escalating, minimize its effects, and bring it under control)
  - Firefighting
  - Medical treatment
  - Containment
  - Relocation/redirection of traffic and personnel
  - Protection (isolate the scene)

- Damage Assessment
  - Inventory damaged property, locations and infrastructure (IT)
  - Document damage (take pictures, descriptions, and notes)
  - Assess value
  - Determine immediate replacement options
  - Notify crisis team of impacted facilities/assets
  - Contact insurance carrier
  - Coordinate activities and cooperate with proper authorities (consider your own internal investigation)

- Contingency Plan Execution
  - Act on the recovery strategy
  - Perform roles related to alternative procedures/methods/processes
  - Restoration of basic services
    - Office space
    - Power
    - Communications (telephone, internet, fax, etc.)
    - IT network and hardware
    - Applications
    - Data
    - Unique assets
    - Employee/staff/partners/suppliers
    - Other: Restroom facilities, HVAC, food/water, etc.
  - Communicate with larger teams/organization/customers
  - Plan for restoration of normal operations and transition to such

- Management of Recovery Vendors, Partners, and Existing Supply Chain
- Crisis Communications and Situational Awareness
- Liaison with Authorities, First Responders, and Government

Implementation and Execution Needs

After you have evaluated possible mitigation and recovery strategies, now is the time to consider whether to internally execute the strategy or work with an outside vendor. Though organizations' disaster teams are often incredibly capable and resourceful, there are many other variables to consider that could place internal recovery plans at risk of failure.

Successful organizations will establish a strategic mix of internal and external capabilities to enhance both execution and resilience. In doing so, a tiered response can be progressively executed based on conditions present at the time.

Create a Communications Plan

When a disaster occurs, the need to communicate happens immediately. Your employees, customers and stakeholders will look to you for real-time information, wanting to understand how they will be impacted. No matter how robust your overall plan may be, without the ability to communicate promptly and effectively during a crisis, these plans are destined to fail.

Communication may be the most important component of your disaster plan, and both internal and external strategies are crucial.

Here are some important steps to follow:

1. Assign a lead and backup communications coordinator, and outline roles for each.
2. Create an internal emergency contact list with each employee's home and cell phone numbers, business and personal email, and complete family information. Regularly update this list, and make sure employees know how to access it.
3. Setup an alert notification program that is tested and updated regularly.
4. Standard communications methods often fail during a disaster. Use multiple alternative communications methods such as text messaging, an emergency web page, or social media, and consider a plan to redirect your phone to cell phones or an answering service.
5. Create a list of key external contacts for before, during, and after a disaster. Possible contacts include:
    - Clients, vendors, and suppliers
    - Business or operational partners
    - Media and other community resources
    - Government disaster response entities
    - Insurance Agencies
6. Utilize social media
    - Post real-time status updates
    - Direct clients/employees to alternate locations
    - Provide emergency contact information and instructions
7. Test your communications plan at least once per year.

Create an Evacuation Plan

If a life-threatening event were to occur, orders to evacuate or shelter-in-place are issued to protect life safety. Threats to consider include building fires, severe weather events (tornado, earthquake, flood, hurricane), gas leaks or other utility accidents, workplace violence, and unique threats caused by the nearby environment. Be sure to follow all threats identified in your Risk Assessment.

Provisions for Notifying Building Occupants:

- Alarms must be distinctive and recognized by all those within your place of operation.
- If possible, alarms should automatically notify first responders.
- Alarm system should have auxiliary power supply as backup to power loss.
- Alarm should be unique to the threat to indicate the action to be taken (either evacuation or shelter-in-place).

An Evacuation Plan Should:

- Establish a clear, concise explanation of situations that would require an evacuation.
- Identify a clear chain of command to authorize and issue an evacuation command (can also identify "evacuation wardens" who are charged with assisting others).
- Specify evacuation procedures for each defined area within the office, floor, building and complex, including primary and secondary routes and exits.
- Include detailed, accurate maps and diagrams posted along routes (include at least two escape routes from each room, and indicate location of equipment like fire extinguishers and first-aid kits).
- Identify an exterior assembly area (at least 100 yards away).
- Include suitable arrangements for those with disabilities.
- Include a means of accounting for all employees and known visitors.
- Provide evacuation wardens with access to employee lists and any known absences.
- Designate which, if any, employees will remain after the evacuation alarm to shut down critical operations or utilities before evacuating (employees must be trained to recognize when to abandon the operation and evacuate themselves).

A Shelter-In-Place Plan should:

- Establish scenarios appropriate for taking shelter (such as severe weather events, gas leaks, workplace violence).
- Ensure shelter location is stocked with supplies (food, water, battery-powered radio, first aid kit, flashlights, batteries, emergency contact information).
- Ensure shelter location has the following characteristics.
- Interior room, with fewest windows and vents.
- Room for all personnel and guests to sit (10 sq. ft. per person is recommended).
- Access to some kind of communications device (landline preferred).
- Room for storage of emergency equipment and supplies.

Best Practices

- Assess the location and condition of existing signage and emergency equipment.
- Incorporate training into employee onboarding process and employee handbooks.
- Hold initial educational sessions to make employees aware of most likely threats.
- Conduct drills at least twice annually, ensuring scenarios are as realistic as possible.
- Drills should be conducted both with notice and without to simulate unusual conditions that can occur during an actual emergency.
- Conduct discussions or debriefs afterward to identify areas for improvement.

Create or Restock Your Emergency Kit

An Office Emergency Kit should include far more than simply First Aid Supplies. When disaster strikes, time is of the essence so beyond protecting health and safety, you must consider elements needed to ensure critical functions can continue. Below you'll find a list of items in several important categories needed to care for employees as well as those supplies required to keep your business operating.

First Aid Supplies/Kit:

- First Aid Reference Guide
- Gloves/Triage Kit
- Masks
- Bandages/Sterile Gauze
- Waterproof Tape
- Ice Packs
- Sanitary Supplies
- Tweezers/Scissors
- Antibiotic Ointment
- Anti-Inflammatory/Pain Meds
- Eye Wash/Irrigation
- Hand Sanitizer & Wipes
- Emergency Blanket
- Burn Gel/Dressing
- Sting/Bite Swabs
- Blood-Stop Pack

Emergency Supplies:

- Food–Nonperishable, Minimal Prep, Serving Supplies
- Water–1 Gallon Plus/Person/Day
- Flashlight, Lanterns & Extra Batteries
- Tools, Gloves, Protective Gear, Blankets
- Battery Powered Radio with NOAA Weather
- Battery Backup, Solar & Crank Chargers for Mobile Devices

Protecting Continuity of Critical Functions:

- Cash/Paper Checks
- Your Recovery Plan
- Login & Password Credentials
- Important Documents
- Letterhead, Envelopes, Cards
- Office Supplies
- Application Software
- Building Access Keys
- Emergency Contact List Copies
- Cleaning Supplies
- Basic Tools

Nice to Haves:

- 2-Way Radios
- Satellite Phone/Communication Tools
- Emergency Fuel Supply

Back Up Your Data

When a disaster occurs, you need critical systems and applications back up and running as quickly as possible. Your employees, customers and stakeholders all depend on these critical systems to be available for the organization to operate. It is important to note that disasters related to your IT systems can range from a single corrupted file that could take down your email system, all the way up to having all your servers destroyed in a natural disaster. Every disaster is different and it is important to have a flexible backup system in place that can react to your specific situation.

Everyone in your organization would agree that backing up your data is essential. Here are some guidelines to ensure effective restoration:

Employ a Hybrid-Cloud Backup System

- Allows for quick restores of data in the event of a localized failure.
- Allows for offsite cloud recovery scenarios if the local datacenter is inaccessible.
- Replicates data offsite for long-term retention to meet audit requirements.

Backup Your Data as Often as Possible

- Critical systems should be backed up at least once per hour.
- Less critical systems could be backed up less often.
- Each server needs to have a customized schedule.

Specific Resources Should be in Place for Managing the Backup Process

- If your organization isn't large enough to have dedicated resources, consider partnering with a company that focuses on Disaster Recovery/ Business Continuity.

Document the Backup and Recovery Processes for Each Server

- Understand which servers need to come up in a disaster to meet certain business requirements and understand what order they should be recovered.
- Record which servers are backed up and at what interval so there isn't any misunderstanding about protection levels, retention periods, etc.
- Documentation should be stored in a location where anyone on the recovery team has access to it.

Test Your Back-Ups Regularly in Different Scenarios

- Simulate loss of files, loss of local server(s) and loss of the entire datacenter (cloud recovery).

Make Sure More Than One Person Knows How to Access Your Data

- Have appropriate backup resources in place who have been trained and are up to speed on the recovery strategy.

Prepare Your Employees

Help your employees feel safe and prepared for a disaster. Develop an evacuation plan, and let employees know about that plan via email, workplace trainings, and postings throughout your building. Practice the plan, and hold an unscheduled drill so that employees understand how to implement your plan.

At Work Preparedness

- Develop an evacuation plan, and let employees know about that plan via email, workplace trainings, and postings throughout your building.
- Practice evacuation plans semi-annually, and hold an unscheduled drill so that employees understand how to implement the plan and know their primary role.

A Soaring Example: Jetblue

JetBlue's Emergency Response and Business Continuity team partnered with us to host a contest to improve preparedness. Here's how they did it:

For National Preparedness Month in September, JetBlue's Emergency Response and Business Continuity team partnered with Agility to host a contest to improve preparedness. Based on an Agility document about workplace preparedness, JetBlue created a poster that informed employees what to include in a personal 72- hour preparedness kit. JetBlue encouraged staff at each location to hang poster in the office, take pictures with the posters, and submit them to a raffle. Winners of the raffle received two free airline tickets and an emergency radio. More than 50 offices, with hundreds of crew members, participated.

- Cross train employees so essential operations can continue with reduced staff.
- Integrate emergency preparedness into all new employee training and communications.

At Home Personal Preparedness

If an employee is ill-prepared for a home-disaster and can't report to work, your organization will suffer. Notify your employees ahead of forecasted weather events, and make sure they are staying informed about other potential risks to their home. You should also encourage your employees to take the following steps in their homes and with their families:

- Create an evacuation/shelter plan and know where to go if their family gets separated.
- Maintain a home emergency kit at all times.
- Store critical documents somewhere safe and accessible and store duplicate copies in a separate location.
- Practice evacuation routes and know how to get out of their homes from a variety of exits.
- Develop a communication plan to remain in touch with family members during a crisis.
- Be familiar with local warning systems and emergency plans.
- Provide employees with the following resources to aid family preparedness:
  - The most effective way to generate employee buy- in is to build a culture of preparedness in the workplace and make preparedness fun. Lead by example by sharing your own personal preparedness plans, and consider hosting contests and offering incentives for participation.

Plan for a Power Outage

Power loss is the #1 interruption to which Agility responds. In fact, nearly 70% of all businesses in the United States will lose power sometime in the next 12 months. Since every organization has different power needs, it is important to know and understand your risk as well as your building's power requirements.

Mitigating the Risk

- Back up data regularly.
- Install at least one land-line telephone.
- Obtain and test Uninterruptible Power Supply (UPS) devices and surge protectors.
- Install, regularly test, and maintain an on-site generator.
- Develop a work-from-home procedure and test the plan.

Preparation for Mobile Generator Recovery

- Know Your Power Requirements Ahead of Time!
- Assess the impact of loss of power on your operations.
- Know how long you can last without power, and establish your strategy accordingly.
- Determine your organization's power needs in advance by contacting an electrician and asking them the following questions:
  1. What phase is my electrical service? (Single or Three Phase?).
  2. What voltage is my service? (208v, 240v or 480v?)
  3. Is my power requirement for a Wye or Delta generator? (Note: Wye is the most common generator requirement).
  4. How many amps do I need to power key systems? (Hint: Determine your peak Amperage draw over the past 12-24 months).
  5. What size generator will be required? (Note: It is not advisable to undersize OR oversize your generator as damage can be done to the components in either scenario).
  6. Does my building have a power transfer switch? (Note: If no transfer switch exists, you have several options for distributing generator power to where it is needed, i.e. hardwire into your building panel or a spider box, etc.).

Find an Alternative Place to Work

The best recovery comes from the best preparation. Now is the time to think about where you might temporarily set up or permanently relocate if your place of business becomes non-operational. Your relocation plan should be clear so that when the time comes, you can simply tell your team to activate it. Strategies may involve third-party contracts, partnerships or reciprocal agreements, or displacing other activities within the organization. In addition to obtaining management's approval, make sure your strategies include multiple means of recovery, with tiered or phased recovery implementation.

Suggested Recovery Site Options

1. **Primary Site**
   Use of unoccupied space or common areas for displaced employees in a minimally affected situation
2. **Alternative Internal**
   Site owned by your organization, unaffected by the event
3. **Reciprocal**
   Client, vendor or partner site, accessed through formal agreement
4. **Hot Site**
   Vendor-provided site with shared recovery capability but ready for immediate occupancy; shared or dedicated access based on contract terms
5. **Warm Site**
   Vendor-provided site with shared capability, requiring some preparation
6. **Cold Site**
   Readily accessible location, but requiring full provisioning for recovery
7. **Mobile**
   Fully functional office deployed anywhere, independent of terrestrial infrastructure

Important Considerations

- Facility type/location/accessibility
- Recovery timeframe
- Cost
- Availability and reliability of facility and/or vendor
- Impact to employees, customers, suppliers and stakeholders
- Access to transportation networks and basic services
- Duration of typical recovery
- Upfit or buildout requirements
- Ancillary costs (connectivity, lodging, travel, etc.)
- Whether or not you need guaranteed or dedicated space

Test Your Plan

Testing your disaster recovery plan is not only an essential part of planning, but a step that could mean the difference between giving in to a crisis and surviving one. This is the culmination of your planning process, and it allows a thorough assessment of both mitigation procedures and recovery strategies.

A Good Test Will:

- Feature realistic scenarios based on identified risks to your organization.
- Meet compliance or regulatory requirements.
- Increase employee, management, and community confidence in the plan.
  - This includes setting realistic expectations for response team members.
- Expose holes, gaps, misperceptions, or other potential failures of the plan.
- Be conducted both with and without notice.
  - Announced drills are learning exercises that allow employees to walk through actions they are trained on and expected to take during an emergency.
  - Unannounced drills provide the most accurate indication of what will occur during actual crisis conditions.
- Improve your overall readiness.

When you're running a test, make sure to take notes during the exercise. What was the task or issue? When was it started/identified? Was it resolved? How? What problems arose? Review the findings with participants and then update and distribute your written plan, making sure to write down notes for consideration on your next test.

Business continuity planning is an ongoing process, and testing is a critical step in continually assessing and improving the strategy as your organization grows and evolves. Your testing process should run in a continual loop: test feedback improve.

> ***Remember:***
> *A successful test is not necessarily one that runs flawlessly, but an exercise that allows you to identify failures and therefore improve your plan and increase your ability to serve customers after a disaster.*

Summary

Organizations face continuous threats that can put lives in danger and disrupt operations. However, implementing an incident management program that fits your organization is challenging.

To help mitigate these threats, Agility offers an integrated business continuity solution that helps your business plan, test, train, alert and recover—all in one. It enables organizations to eliminate business impacts and make sure their workforce is safe and informed.

Before an Incident

We help you manage and generate emergency action plans, provide online training with expert content, and offer unlimited document storage.

During an incident

Agility keeps your workforce safe and helps you recover 4 times faster with an integrated solution of data, planning, testing, office space, incident management, power, communications, and technology.

After an Incident

Agility will make sure your business is fully operational and prepared to withstand the unexpected.

Guide

What Business Insurance Covers

How to Protect Your People, Processes, and Operations

Table of Contents

Protecting Your Organization's Financial Well-being During a Recovery

While the number of different insurance products available in the market today is nearly limitless, there are a few common types of coverage that most businesses typically carry or at least consider. When it comes to large scale disasters and long-term business interruptions, these policies are also among the most misunderstood. By investing some time with your insurance professional and understanding each type of coverage explained in the guide below, you can take significant steps towards anticipating and perhaps even reducing your financial risk during business interruptions.

In this guide we'll explain a few key areas of insurance coverage to review with your carrier or broker to help your organization get prepared for a business interruption. This guide will also share some questions to ask when considering coverage.

Potentially Useful Coverage Following Interruptions

"Business Interruption Insurance" is a common coverage that helps offset lost income and expenses resulting from property damage or loss such as salaries, taxes, rents, and net profits that would have been earned during a closure. However, this coverage only applies to losses as a result of covered perils, which typically involve physical damage to your location(s). Therefore, you should consult with your provider regarding additional coverage that can protect against other common interruptions. They may include, but are not necessarily limited to, the following:

1. Extra Expense Coverage

This coverage, often combined with Business Interruption coverage, can not only help you offset costs related to restoring operations but may also significantly reduce your overall business interruption or business income claim. This coverage will often pay for additional costs in excess of normal operating expenses that an organization incurs to continue operations while its property is being repaired or replaced after having been damaged by an insured peril. These may include the costs to set up in a new or temporary office location or costs that allow the business to function where it currently is (e.g. generators), reducing the impact of a shutdown, overtime wages, expediting expenses, lost profits due to the business being shutdown, or, in some instances, repairing/replacing damaged property.

2. Utility (or Service) Interruption

Nearly all commercial property policies contain exclusions for losses due to a utility failure that originates away from the insured premises. Therefore, Utility Service Interruption Coverage is available to close that gap in coverage and can cover interruptions to water supply, sewer service, power supply and communications connectivity. Be sure to understand the covered locations, property that is covered, cause of losses covered and any limits in place. It is important to note if your coverage excludes interruptions to overhead transmission lines. If your utility service is delivered via overhead lines, be sure to request specific coverage for this. Also note that two different coverages exist for Utility Interruption: Direct Damage Endorsement which covers loss of or damage to covered property caused by an interruption in utility services, or Time Element Endorsement which covers a suspension of operations at your premises caused by an interruption in utility service to your premises.

3. Mechanical or Equipment Breakdown Coverage

This coverage can help protect your business from damages and costs related to computer or IT failure, as well as electrical or mechanical equipment breakdown.

This Kind of Coverage May Insure a Variety of Equipment Such As:

- Air conditioning and refrigeration
- Electrical equipment
- Computers and telecommunications
- Business equipment
- Production machinery
- Computer-controlled machines
- Security systems
- Retail “point of-sale” systems
- Ventilation systems
- Generators
- Elevators and escalators
- Boilers
- Water heaters
- Motors and pumps
- Engines

4. Debris Removal Insurance

This coverage provides reimbursement for clean-up costs associated with damage to a property resulting from an insured peril, such as charred wood from a building fire. Note that there are often limits to total coverage inclusive of property replacement which may limit the amount available for debris removal. Additionally there may be limits tied to a specific percentage of overall insurance available that is available for debris removal.

5. Cyber Liability Insurance

This includes data breach and technology errors and omissions coverage.

Because cyber insurance is often excluded from a general liability policy and nearly every organization is exposed to some level of risk to cyber incidents, this form of coverage is critical to protecting your organization in today's digital age. These policies are intended to cover a variety of both liability and property losses that may result when a business engages in various electronic activities, such as a data breach in which personal information is exposed or stolen. In addition, the policies can also cover liability arising from website media content, as well as property exposures from business interruptions, data loss or destruction, computer fraud, funds transfer loss and cyber extortion. Technology errors and omissions coverage is intended to protect providers of technology products and services, such as computer software and hardware manufacturers, website designers, and firms that store corporate data on an off-site basis.

6. Contingent Business Interruption

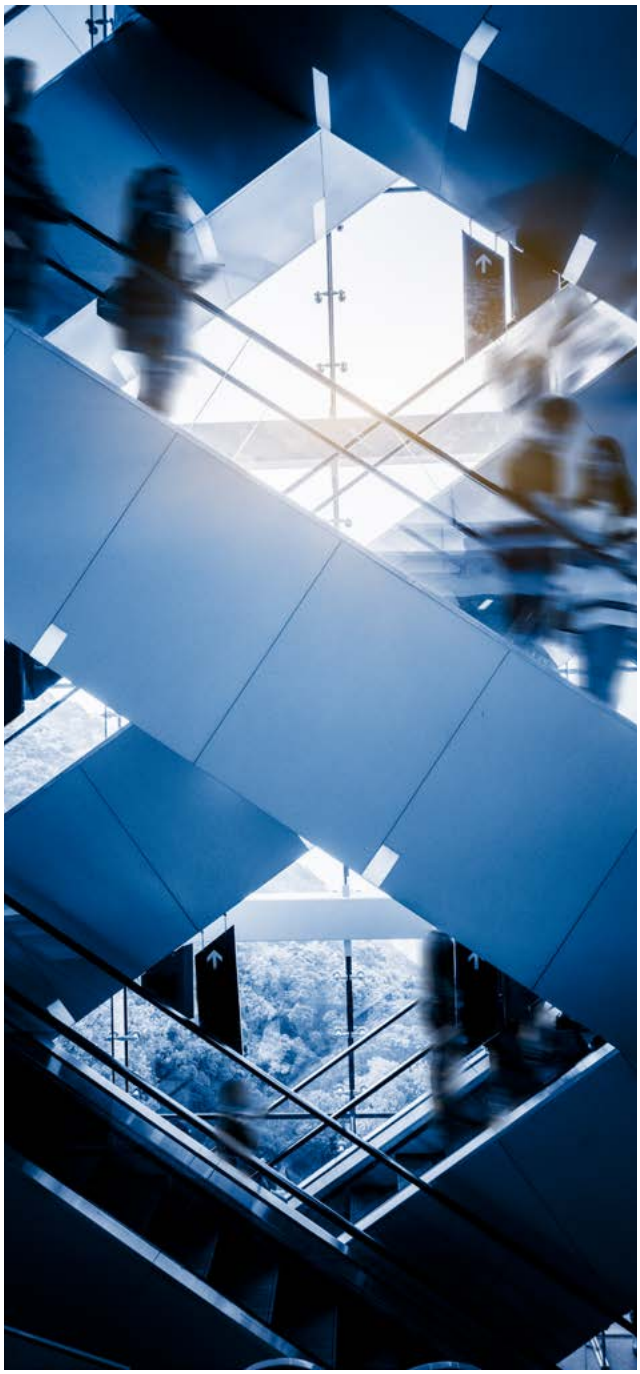
This is an extension to other insurance that reimburses your lost profits or extra expenses that are a result of interruptions of business operations at the premises of a customer or supplier. If the key components or core supplies that you rely on come from a limited vendor group, having CBI coverage is crucial because a break in the supply chain could have a dramatic impact on your ability to produce and market goods. The same coverage can apply to an interruption of operations for one of your key customers. It is important to note however, that coverage is only available for perils that YOUR business interruption policy covers.

Each organization's risk exposure and loss potential is different, but by investigating these options as potential supplements to your existing commercial property coverage, you could enhance your organization's preparedness and ability to recover quickly and effectively following a disaster.

Common Mistakes and Incorrect Assumptions

The most common mistake is relying on property coverage and ignoring the threat of lost income, the ongoing expenses you'll incur while shut down, the time it takes to recover and the additional expenses a recovery requires. Additionally, there are some steps you can take when you review your insurance coverage:

- Confirm all covered and excluded perils; never assume that all types are covered
- Review your policies at least annually to ensure that they are updated as your business evolves, revenue grows and exposures change
- Be aware of all limits to coverage and exclusions to specific property
- Understand the terms and timeframe under which your coverage takes effect, as in some cases, coverages will not kick in until your business is shut down for a number of days
- Determine the cost of rebuilding your facilities (including the costs of demolition, materials and professional fees) versus the market value or purchase price
- Become familiar with your deductibles or coinsurance due for the various coverages
- Conduct regular, accurate valuations of your business and property, and update policies accordingly (especially after any mergers, acquisitions or expansions)
- Determine an appropriate indemnity period that allows your business enough time to recover
- If you carry flood insurance, take note that the National Flood Insurance Program does not cover lost revenue



Questions to Ask About Insurance Coverage

Property Coverage

- Is the coverage based on “valuation replacement cost” or “actual cash value”?
- Is there a coinsurance provision?

Business Interruption Insurance

- Is there a separate deductible or waiting period for this type of coverage?

Extra Expense Coverage

- Can your insurer provide a worksheet of the expenses that are allowed under this coverage for recovery?
- Are there any “sublimits” applicable for expenses depending on the cause (e.g. fire, flood, etc)?
- Is there any deductible applied to extra expenses?

Final Word

Every organization must carry insurance, but is your organization getting your money’s worth for the investment and ensuring the proper coverage? Given the increase in the frequency and severity of large-scale natural disasters coupled with greater customer demand the criticality of maintaining your operations is more important than ever, regardless of the interruption. Speak with your insurance professional today armed with insightful questions and knowledge of your options. Take the time to dive into the question, “How much coverage is enough?” Your provider may provide you with tools to help calculate the proper coverage given your gross annual sales and existing or anticipated expenses. Tools such as this may help create a solid strategy to protect your employees, customers and your business as a whole.

Guide

The Ultimate Guide to Business Continuity Testing

A Complete Set of Practical Methods

Table of Contents

Introduction

Formulating a business continuity plan (BCP) is only half the battle. A solid BC strategy needs more than just a well-laid out theory. How well does your plan hold up in a real-world disaster?

Can your backup systems withstand a cyberattack? How efficient is your recovery time objective (RTO) for restoring data? Are your employees familiar with emergency procedures? Do you have an emergency communication strategy to let everyone know about an incident immediately?

Business continuity plan testing is the most reliable way to find out, and it is a critical component of continuity planning. By skipping regular testing, you won't know if your organization is prepared for a disaster—until it's too late.

61% of companies

are challenged with a lack of organizational engagement, which directly correlates with BCP's success.[1]

Testing in Numbers

Testing your business continuity program allows you to validate your BC plan and manage risks. In fact, 88% of companies test BCP's at their companies to identify gaps, and 63% of them do that to validate their plans.[2]

Business continuity testing isn't about pass or fail. It's about continuous improvement by learning from findings uncovered in a live exercise.

57% of companies

say that semi-annual or quarterly (consistent) testing helps to gain buy-in throughout the organization, making it more likely to be prepared for an interruption.[3]

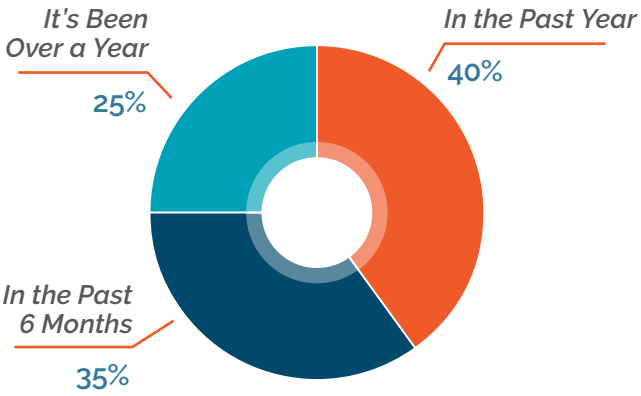
1. BC Benchmark Study, 2019
2. Make Your BCP Tangible with Testing, Online poll, 2019
3. BC Benchmark Study, 2019

Testing Your BCP: How Often is Enough?

If you already have a BCP, it may be filled with procedures for various events. But do you need to test everything? And how often do you need to do that? The answer to that depends on your organization's unique risks that could be identified in a business impact analysis (BIA).

A company that has more at stake in the event of disruption—loss of revenue, operational downtime, damaged reputation—will typically require a greater variety of BCP testing scenarios, as well as running those tests more often. Every organization is a unique entity, and its BCP will differ in scope and priority.

When Was the Last Time You Tested your BCP?[4]



Expert's Advice

Some scenarios, such as an active shooter, are more critical and need to be tested frequently. Tim Mathews, a business continuity practitioner, D. Sc., MBA, MBCI, suggests an approach of "working from the headlines." When various emergency events take place across the country, it's a potentially good exercise to include those scenarios in your test plan.

4. Make Your BCP Tangible with Testing, Online poll, 2019

Reasons to Test Your BCP

A well-orchestrated test strategy helps protect the brand, its promise, and its value proposition. If your competitors had a poor test performance or made a critical mistake in a real-life situation with a client, your company can shine by demonstrating its reliability and advance its business forward.

Here are the most common reasons to test your BCP:

- To help identify interdependencies, gaps, and areas for improvement.
- To demonstrates to your clients a higher degree of commitment.
- For suppliers to other firms, you rise among competitors, taking on more projects, and potentially winning new business due to your resiliency.
- To continually test and validate plans, while improving outcomes.
- To satisfy compliance requirements and regulations.
- To reduce recovery time and cost.

Barriers for BC Testing

Conducting a business continuity test isn't about failing or passing it, and it certainly shouldn't be taken as a personal failure if anything goes wrong during the test. That's why having the courage to initiate the process of testing may be the biggest obstacle. Overcoming this internal struggle will bring immense value to the entire organization.

Scenario Example

A call-center experienced a network outage, and all the phone lines were down. A 24-hour RTO isn't acceptable in this instance, as losing communication with their clients for so long will have a lasting negative effect. As a business resiliency solution, management can split their center representation geographically to have backup lines in their secondary facility. Often, finding such solutions is only possible through testing.

Expert's Advice

Tim Mathews believes that the biggest obstacle there is to testing business continuity lies within us. A business continuity manager or person responsible for this process may be too timid about exposing the imperfections of plans in place. However, no strategy or plan is ever perfect or complete. Finding gaps is what will drive your work to perfection; stagnancy won't.

Supply Chain Resilience

Every company can find itself somewhere in the supply chain eco-system. And it's typically a supplier that becomes a weak link in the chain. Even though it may seem reasonable to ask your supplier for a detailed BCP plan, along with an explanation of their RTO and RPO, they may not be willing to share it. Your supplier's management may allow for a week-long RTO. However, such a timeframe may not be acceptable for your business. Will this be a deal-breaker for your organization if you have an established and long-lasting relationship with that supplier?

How to Identify Critical Vendor Resilience

- Get started by shortlisting your top critical vendors.
- Engage with them via a supplier-resiliency survey, a letter, or by asking them to fill out a spreadsheet.
- Score your suppliers based on 4 essential elements: planning (BCDR), physical recovery, approach to testing and exercising, compliance with ISO 22302 Standards.
- For SMBs, when inquiring about your supplier's resiliency plan, make sure it's specific to their industry. A generic BC plan won't cut it.

Expert's Advice

One way Tim Mathews recommends approaching this situation is by offering this supplier some latitude and working on improving their RTO. Alternatively, this supplier could provide you with updated pricing for their products and services to mitigate the difference in your expectations from them.

Types of Tests and Scenarios

3 Types of Tests

A. Plan Review

A plan review is much like an audit of the BCP. The BCP team, along with the c-level management or department heads, get together to review the plan and to decide if any components are missing or need revision. This type of test is beneficial for training new members of the BCP team, or in regular onboarding.

B. Tabletop Test

During a tabletop—a scenario-based, role-playing exercise—employees participate in an actual exercise. Everyone involved practices their roles and responsibilities during an emergency, such as an earthquake, hurricane, or an active shooter.

C. Walk-through/Simulation Test

A BCP simulation test is a more hands-on type of tabletop exercise. Scenarios for this test can range from data loss and restoring backups, to live testing of redundant systems, network outage, physical recovery, emergency notification, and other relevant processes. In addition to critical personnel, all employees would be involved in this BCP event testing process.

Expert's Advice

Tim Mathews strongly recommends testing a BCP around a particular scenario, rather than assuming something may go wrong. Doing so will help your organization become more nimble and resilient and less dependent on huge commitments.

6 Common Test Scenarios

As your team is prepping for those tests, you need to agree on how realistic and detailed you want a test to be. Testing can present challenges for companies: it requires investing time and resources. With that in mind, it may make more sense to conduct a tabletop test at a conference room, rather than involving the entire organization in a full-blown drill.

1. Data Loss/Breach

One of the most prevalent workplace disasters today. The cause of data loss or breach could vary:

- Ransomware and cyberattacks
- Unintentionally erased files or folders
- Server/drive crash
- Datacenter outage

The goal is to regain access to that data as soon as possible. Restoring backup is the solution. However, who's responsible for that? What's the communication plan in this case? What are the priorities? Who needs to be contacted right away? Are there any vendors involved?

These and many other questions will be answered during a test.

2. Data Recovery

In this scenario, you need to make sure your BCDR systems work like clockwork. To do that, run a test that involves losing a bulk of data, and then try to recover it.

Some of the elements you'll need to evaluate will include your RTO, and whether your team met its objectives. Besides, was there any damage to the files during recovery? If your backup was stored in the cloud, did you come across any issues?

3. Power Outage

In this scenario, your incident response team needs to coordinate among themselves and communicate with the rest of the company. How will you notify your workforce about the incident? Who's expected to come in the office, and who's able to work remotely? Which departments get affected the most and thus need immediate relief (e.g., accounting, logistics)? Do you have a backup power generator? Do you or anyone on the team know how to use it? Do you have an arranged office or mobile recovery location?

Answers to these questions must be covered in your BCP.

4. Network Outage

Power outage inevitably leads to a network outage. However, network outages can happen with electricity still being on, and they could last indefinitely. In such scenarios, many businesses rely on a work from home strategy that isn't effective long-term. So, during your test, verify the following points:

- Does everyone have access to their work systems?
- Is everyone aware of the security measures to take while working remotely (VPN, safe network connection, etc.)?
- What is the plan for network restoration?

5. Physical Disruption

This is one of the most critical company-wide drills that must be completed annually. There may already be a local fire code compliance in your area, but if not, it's vital to conduct a fire drill. Consider including an earthquake or a tornado as potential disruptors.

6. Emergency Communication

Being able to communicate during a disaster or an emergency can provide a lifeline. Yet, the most disruptive events—hurricanes, floods, tornadoes—are very likely to leave you with no traditional means of staying in contact.

Regularly update the contact information of everyone in your contacts database, so that all employees receive timely notification. Additionally, create templates for every disaster scenario to streamline to process.

Getting Leadership Involved

Direct involvement of senior executives is what makes your BCP mature. When determining your business's RTO, take this question to your leadership for input.

Role-Based Benefits of BCP

When talking about the benefits of business continuity planning, industry vendors and business continuity planners typically tout one overarching benefit. When affected by business interruption, having a plan drastically increases your odds of preserving revenue and keeping your doors open.

To make a compelling case for the diverse benefits of business continuity, emphasize how it helps each executive meet their specific goals, and alleviates their pain points.

Chief Executive Officer (CEO)

CEO Perspective

The CEO is under enormous pressure to promote the company's vision and outrank the competition in a marketplace fueled by rapid technology changes and compliance issues. On top of that, today's CEO is struggling to overcome a disconnect with employees, who want the CEO to communicate more often, criticize less, and celebrate successes consistently.

How Business Continuity Helps

- Encourages communication between the CEO and staff by requiring interdepartmental coordination.
- Helps unite various departments and locations for a common purpose.
- Gives the CEO a chance to evaluate whether the business's operations reflect the company's overall vision.
- Creates a competitive advantage for the organization.
- Identifies opportunities for improving process efficiencies and revenue streams.

Expert's Advice

Include your management in different forms of test you plan to run. Whether it's inviting them to a Mobile Recovery Center you set up on your company's parking lot or sending them a test emergency notification message as part of the training. And always follow up with recognition. It will help them to feel part of the process and will be rewarding.

Chief Operations Officer (COO)

COO Perspective

"Work smarter, not harder" is the COO's motto. As the person responsible for doing things more efficiently and profitably, the COO is challenged with staying abreast of rapidly evolving technologies, processes, security concerns, and compliance requirements.

How Business Continuity Helps

- Allows the COO to become more familiar with critical business processes, products and services, supply chains, employee roles, and technology.
- Improves business resiliency by allowing the COO to identify interdependencies and single points of failure.
- Allows for innovation in everyday business activities and quick decision-making during an interruption, which gives the COO a chance to prove their value to the organization.
- Satisfies federal and industry regulatory requirements.

Chief Financial Officer (CFO)

CFO Perspective

The CFO role is changing, thanks to the influence of the global financial crisis, big data explosion, and widespread social media adoption. In addition to the traditional tasks, the CFO is becoming more active in working with the CEO on the company's strategic planning initiatives. In these different capacities, the CFO has to balance innovation with making sound decisions that protect the bottom line.

How Business Continuity Helps

- Protects the bottom line by reducing downtime and showing stakeholders the business will do what it takes to protect their interests.
- Helps mitigate property and profit losses.
- Provides an overall picture of business data and processes, which helps the CFO make business recommendations for improving day-to-day operations and avoiding lost revenue in the event of an interruption.

Chief Information Officer (CIO)

CIO Perspective

Rapidly changing mobile, social, and cloud technology are transforming modern businesses. As a result, the CIO has to think on their feet and collaborate with other executives to see how they can use technology to increase business performance while managing cybersecurity risks and mitigating downtime.

How Business Continuity Helps

- Gains other departments' cooperation in identifying key applications and interdependencies.
- Helps resolve both small- and large-scale IT threats.
- Improves the efficiency and security of day-to-day operations.
- Decreases frequency of outages and length of downtime.
- Improves response to cyber threats.

Chief Marketing Officer (CMO)

CMO Perspective

As the driving force behind the organization's brand image and customer experience, the CMO has to learn to align the company with the end customer and bring in the number of qualified leads and conversions required to meet projected revenue goals.

How Business Continuity Helps

- Assists the CMO in identifying new marketing angles by allowing them to collaborate with other teams.
- Reassures customers of the organization's ability to provide uninterrupted service, giving the business a competitive advantage and even gaining more conversions.
- Protects against reputation damage resulting from an interruption that would otherwise require remedial marketing efforts.

The benefits of business continuity extend beyond surviving an event (though that's part of it). By showing individual members of the C-suite that business continuity can help them meet their unique objectives, your organization as a whole can reap the benefits.

Post-Test Results and Actions

Finally, it's necessary to document the results of any testing conducted, along with any actionable findings from those tests. Doing so will help your workforce to learn what can and should be improved, and to visualize how much progress has been made. Following up on these items and consolidating recommendations from tests is the most crucial process in the BCP testing lifecycle. Testing, registering the results of your testing, and executing methods to improve your BCP is the most reliable way to strengthen your organization's response processes.

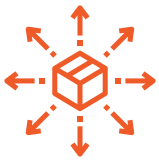
Tips to apply your findings:

Review
Review test findings with all participants.

Conduct
Conduct a Business Impact Analysis.

Assign
Assign responsibilities for open action items.

Capture
Capture items for consideration on the next test.



Update
Update and distribute the written plan.

Modern Business Continuity Model

In a continuously developing environment, traditional "check the box" and reactive approaches focused solely on recovery make organizations much slower to adapt, respond, and improve its processes.

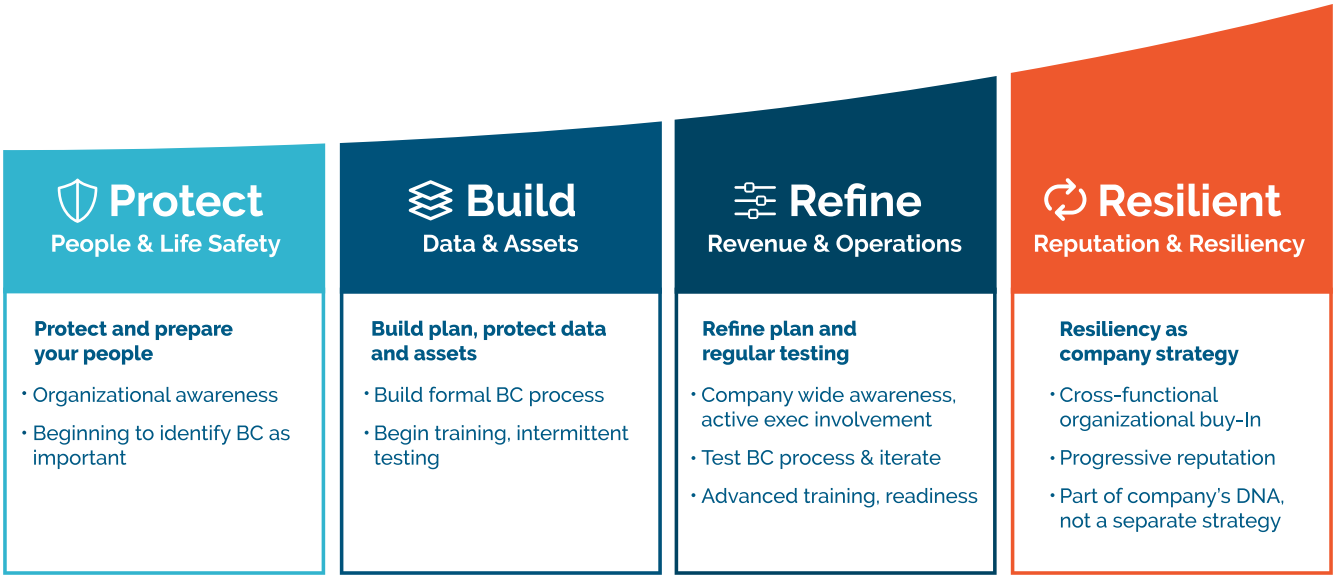
At Agility, we refer to a "resilient approach" as the one that focuses on anticipation rather than recovery. Resilient organizations establish alternative ways of servicing their clients in the event of disruption, beyond setting up the technological element (e.g., using recovery locations to provide critical business services when digital channels are down).

A maturity model demonstrates if an organization can achieve continuous improvement. It provides understanding if a business is being stagnant and what are the processes that need to be revisited. Organizational growth is fueled by creating review or auditing processes that need to be applied regularly to business processes to evaluate their effectiveness, identify improvements, and implement them.

Building our industry credibility is what led to create this model. We involved multiple stakeholders, customers and prospects, analyzed our acquisition strategy and conducted market research. The result is an impactful tool that presents a thought leadership stance, a clear and unified message with a customer-centric market approach.

Our team of experts, technicians, and industry professionals with thousands of recoveries under their belts continue to provide our clients and community with unmatched expertise and the knowledge that can't be acquired in any other way.

We blend practical, innovational, and historical methods, nurtured over the past 30 years, to address tomorrow's resilience challenges. This is how this model was born.



Lessons Learned

- Communicate disaster preparedness response efforts before, during, and after an incident.
- Conducting a business continuity test isn't about failing or passing it. It's about improvement.
- Understand the extent of BC testing done by your vendors.
- Get your C-level management involved.
- Don't spend time designing a plan for every unique scenario. Prioritize the risks and what gets impacted.
- Ensure back-ups are available for data, personnel, worksites, equipment, vendors, and other resources.
- Treat your BCP as "living documents" to be updated as circumstances change.

Summary

Organizations face continuous threats that can put lives in danger and disrupt operations. However, implementing a business continuity strategy that fits your organization is challenging. To help mitigate these threats, Agility offers an integrated business continuity solution that helps businesses plan, test, train, alert, and recover—all in one. It enables organizations to eliminate business impacts, make sure their workforce is safe and informed, and that the business is resilient in the face of any threats.

Before an Incident

We help you manage and generate emergency action plans, provide online training with expert content, and offer unlimited document storage.

During an incident

Agility keeps your workforce safe and helps you recover 4 times faster with an integrated solution of data, planning, testing, office space, incident management, power, communications, and technology.

After an Incident

Agility will make sure your business is fully operational and prepared to withstand the unexpected.

Checklist

Workplace Recovery Checklist

It's a deceiving assumption to think that people can work remotely or from home when their current office is inaccessible. How long will the work-from-home strategy be effective? Is it secure?

In fact, 40% of employees use a device that's not monitored by their employers. As for your recovery site, is it located in the affected area, and will the personnel be able to commute to it? How quickly can you get access to the recovery site?

This checklist will help you assess how much support you need.

Choosing Location

1. Proximity to your office

- Is the area included in the public transit system?
- Is there adequate parking for staff and visitors?
- Is the new location far enough away from your existing office?

2. Size, capacity and availability

- Are there enough workstations and space or will you need additional space elsewhere?
- How readily available will the office be for your staff and visitors?

3. Budget

- Have you confirmed your budget for additional space?
- Confirm the cost per capita, workspace and equipment use over time.

4. Dedicated vs. syndicated seating

- Do you need dedicated seating with year round access (more expensive) or syndicated seating for first come first served access – competitors or local organizations may also have a contract (less expensive)?

5. Physical and Non-physical security

- Does the building have safety and security measures in place to protect staff and information?

6. Mailing facilities

- Will you be able to effectively redirect post to the new location?

7. Reliability during an incident

- Is the building management willing to run exercises with you to validate recovery assumptions such as recovery time, equipment, access etc.

Employee Requirements

1. Team motivations

- Will staff be happy and motivated to work from the new location?
- Do your staff need to be together or can they work remotely elsewhere?
- Is the commute convenient for all critical staff members?

2. Staff reimbursements

- Will the team be compensated for additional travel, food, parking, or other expenses?

3. Staff working from home

- Will your organization create a work-from-home policy, covering security of remote connection?
- Do they have the minimum IT (software, hardware, capacity and connectivity) requirements to complete their roles?

Confirm Your Numbers

1. Space and seat number requirements

- Have you confirmed your critical departments and activities to recover?
- Which of the departments get prioritized over time?
- How many could work from an alternate location (e.g. home)?

2. Dependent activities and departments

- In larger organizations, many departments and activities may be interdependent – consider how this affects the numbers of people needed along the process flow.

3. Senior leadership and/or crisis management teams

- Is there an additional requirement for rooms dedicated to senior leadership or crisis management teams throughout the incident?

Technology Requirements

1. IT systems

- Which systems are needed to support the processes and people?
- How quickly do the systems need to be recovered to support the activities and people?
- Can you get access to the recovery site quickly enough to meet this need?
- Who will be responsible for the set up and installations?

2. Hardware

- Which hardware is required for the processes and staff?
- How quickly can the hardware be provided or sourced to meet your recovery needs?
- Are there 24/7 power generators to support equipment and staff?

3. Telecommunications

- Who are the providers, can that be negotiated and what are the associated costs?
- Confirm the internet connectivity, speed and capacity for your activities.
- How will you redirect phone lines and numbers?

Regulatory Requirements

1. IT systems (How will the location meet your regulatory obligations?)

- Information security
- Physical security
- Speed of recovery for customer focused activities
- Privacy
- Storage, archiving and data sensitivity
- Workforce health and safety

Checklist

Flood Preparedness Checklist

Flooding is a temporary overflow of water onto land that is typically dry. Failing to evacuate flooded areas, entering flood waters, or remaining after a flood has passed can be deadly. Floods may:

- Be a result of rain, snow, coastal storms, storm surges, and overflows of dams.
- Develop slowly or quickly, with flash floods occurring with no warning.
- Cause outages, obstruct transportation, damage buildings, and create landslides.

The following checklist will help keep your business afloat even if the worst happens. Most companies can save between 20% and 90% on the cost of stock and portable equipment by taking action to prepare in advance of flooding. These steps will help mitigate your organization's risk and protect your assets, revenue, and most importantly, your people.

Before the Flood

- Review emergency plan and evaluate your area's flood risk with your team and key employees.
- Take all necessary steps to prevent the release of dangerous chemicals that might be stored on your property, locate gas main and electrical shut-offs, and anchor all fuel tanks.
- Postpone any deliveries of nonessential goods.
- Contact your insurance agent to discuss policy and coverage through the National Flood Insurance Program (NFIP).
- Establish emergency communication method (e.g.,alert notification and incident management system); identify meeting place and time for all key employees in crisis management team; create voicemail for evacuation or office closure.
- Ensure you have an accurate and accessible inventory list.
- Use plugs to prevent floodwater from backing up into sewer drains, or install flood vents or flood proof barriers.
- Stay tuned to local television and social media accounts. Check if your city or county has an emergency alert system and note how they'll be updating the public.
- Contact Agility Recovery to go on alert; this will enable you to exchange contact information and set up regular communication times to discuss your status.
- Ensure you have an emergency communication plan

During the Flood

- Check if everyone is safe.
- Contact organizational stakeholders including employees, board members, customers, and media members with audience appropriate updates.
- Send noncritical employees home or notify them not to report to work.
- Raise elevators to the 2nd floor and turn off.
- Stay tuned to local media; safely evacuate when required.
- Take cell phones, chargers, emergency kits, and critical hardware with you.
- Unplug electrical items.
- Consider redirecting your business phones to cell phones in the event of evacuation or office closure through an answering service, Google Voice, or Agility Recovery.

After the Flood

- Listen to news reports to learn whether the community's water supply is safe to drink.
- Avoid floodwaters; water may be contaminated by oil, gasoline, or raw sewage. Water may also be electrically charged from underground or downed power lines.
- Determine what equipment will be necessary to access the network (laptops, computers, printers, mice, monitors, etc.) and arrange for it to be delivered within your RTOs.
- Clean and disinfect everything that got wet. Mud left from floodwater can contain sewage and chemicals.
- Contact employees using alert ladder notifications system and discuss next steps.
- Review any damage to assets and contact your insurance agent.

Flood Preparation 101

Know the Terms

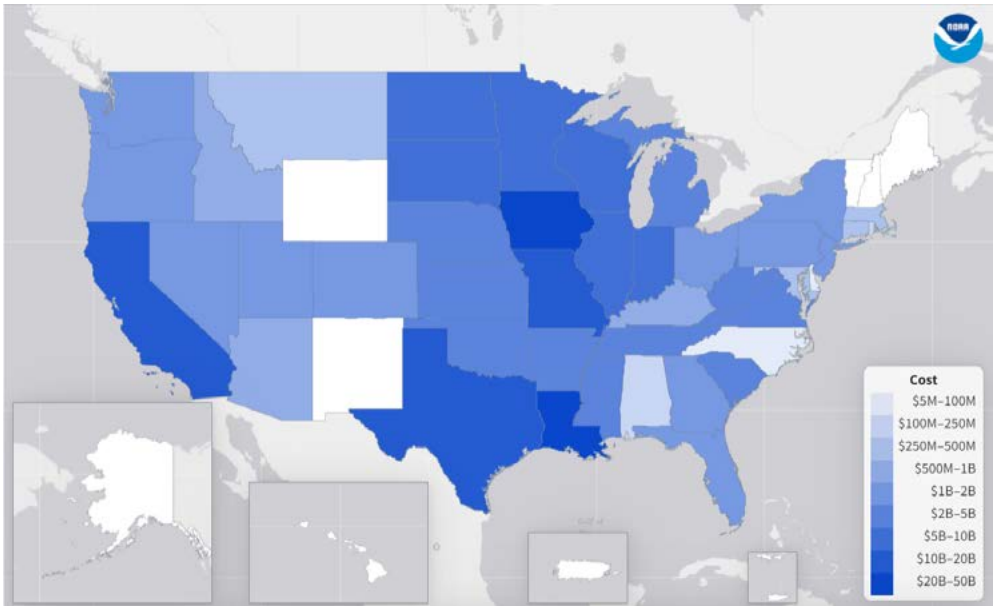
Flood Watch: Flooding is possible. Tune in to NOAA Weather Radio, commercial radio, or television for information.

Flash Flood Watch: Flash flooding is possible. Be prepared to move to higher ground; listen to NOAA Weather Radio, commercial radio, or television for information.

Flood Warning: Flooding is occurring or will occur soon; if advised to evacuate, do so immediately.

Flash Flood Warning: A flash flood is occurring; seek higher ground on foot immediately.

1980-2022 Billion-Dollar Flooding Disaster Cost (CPI-Adjusted)



References

https://www.ncdc.noaa.gov/billions/mapping

A Short Guide to Driving in Flood Conditions

If you can avoid driving, please do.

If you see a flooded road turn around. According to FEMA, most flood fatalities happen because people try to drive through dangerous waters.

Six inches of water will reach the bottom of most passenger cars, causing loss of control and possible stalling. Water at 12 inches can sweep most cars off the road entirely.

Be aware of areas where floodwaters have receded. Roads may have weakened and are at risk of collapsing.

Checklist

Power & Generator Checklist

Nearly 70% of businesses will lose power sometime in the next 12 months.

Know the steps to take before and during an outage so you can resume critical operations as quickly as possible. Contact Agility if you need assistance.

The following checklist highlights some of the steps that should be taken in order to effectively recover from any power outage.

Before a Power Outage

- Ensure your emergency preparedness kit includes the following items:
  - Flashlight with battery
  - Battery or handcrank powered Emergency Weather Radio
  - Avoid candles due to inherent fire hazard
- If possible, have a landline noncordless telephone in your office that does not operate on a VoIP network. Often, a fax line can serve this purpose.
- Create a personal policy that dictates which staff members should report and those that should remain home. Make sure all employees are aware of the policy.
- If security at your location is a concern, ensure that your alarm/security systems have proper battery backup systems, and that telephone connectivity to your monitoring service isn't reliant on power.
- Ensure all sensitive electronic equipment is protected by a power strip surge protector.
- Ensure all Uninterruptible Power Supply (UPS) devices are functional and tested regularly.
- Inspect all critical equipment such as sewer ejector pumps, HVAC condensate drain pumps, and any pumps that provide protection from flooding in lowlying areas. Ensure those pumps are part of the emergency power plan.
- Fuel up any critical equipment including company vehicles, backup generators, etc.

During a Power Outage

- Turn off and unplug all electrical equipment to avoid damage from power spikes when electrical service is resumed.
- Leave one light turned on so you'll know when power comes back on.
- Never run a generator inside or connect a generator to the electrical system unless prior steps have been taken to ensure it is safe to do so.
- Know your generator's fuel consumption rate and set up regular fuel deliveries ahead of time to ensure you never run out.
- Do not touch any downed electrical power lines and keep your employees away from them.
- Report downed lines to the appropriate officials in your area.
- Leave doors closed on office refrigerators and freezers as much as possible during outages. Food will keep much longer if the doors are left closed.
- Make sure the generator your receive includes the following:
  - Transportation to your building site
  - Appropriate amount of Cam Lock Cabling (standard is 50' unless more is requested)
  - Pigtails to connect the generator
  - Started fuel for the first few days of recovery
  - Set of operating instructions
  - Walk through of the basic operating instructions with your vendor
- Follow these steps to prevent generator theft:
  - Place the generator in a well-lit area
  - Install security cameras at the generator site
  - Consider running a metal ring into the ground and securing the generator with a chain
  - If you have to store the generator on its trailer, secure the trailer by chaining the wheels, defensive parking (surrounding with other cars, etc.), and removing the hitch
  - Chain or padlock the generator to other heavy equipment

Checklist

Tornado Preparedness Checklist

Unlike other natural disasters that typically occur in a specific geographic region, tornadoes have been documented in every state.

Here are some tips that will help your business prepare for a tornado:

An estimated
1,000 tornadoes
occur in the U.S. each year.

Before the Tornado

- Have medical supplies on hand.
- Purchase a portable AM/FM radio and spare batteries to ensure you'll have a way to follow weather updates if the power goes out.
- Look for the following danger signs: dark, often greenish sky, large hail, low-lying clouds (particularly if rotating), loud roar, similar to a freight train.
- Vault your data off-site and test your disaster recovery systems regularly.
- Plan how you'll reroute phone calls. Consider the possibility that you might not have cellular service in the event of a widespread blackout.
- Test your business continuity and disaster recovery (BCDR) plan and gather employee feedback.

During a Tornado

- Follow the instructions given by local emergency management officials.
- Know the difference between a tornado watch and a tornado warning.
- If you're inside, stay away from the windows and seek cover in a basement. If you don't have a basement in your office, go to the lowest floor of the building and seek shelter in a small center room (such as a bathroom or closet), under a stairwell or in an interior hallway with no windows.
- If you're caught in the middle of a tornado while in your car, stay put.
- Keep your employees informed by sending out an alert through an emergency notification and incident management system

After a Tornado

- Account for all employees.
- Address staff injuries. For those severely injured, call 911.
- When safe, inspect both the exterior and interior of the building for damage.
- Avoid downed power lines.
- Communicate with employees, customers and vendors to let them know the status of your business.
- Refer to your BCDR plan to determine next steps for continuing your business operations.
- Review your plan to determine what worked and what areas needed improvement.

Checklist

Wildfire Preparedness Checklist

A wildfire, or forest fire, is an uncontrolled fire that occurs where natural vegetation is the predominant ground cover. Though wildfires usually occur in less developed, rural areas, they can threaten urban environments if they are not brought under control, and they are geographically widespread.

There were 1,167 large or significant wildfires and complexes reported in 2018*. The impact of a wildfire can include direct property damage, cost of suppression, and damage to personal property and natural resources. The severity of effects is directly related to the intensity and extent of the wildfire.

Below is the Agility Recovery checklist of just some of the things to consider to prepare your business for such an event as well as to ensure the safety of the people within your organization.

Losses from wildfires added up to **$5.1 billion** over the past 10 years*.

The impact of a wildfire can include direct property damage, cost of suppression, and damage to personal property and natural resources. The severity of effects is directly related to the intensity and extent of the wildfire.

☐ Before the Wildfire

- Keep an adequate number of appropriate fire extinguishers in strategic locations (such as near loading docks and waste collection areas) and maintain them properly.
- Train key employees and their backups on how to use fire extinguishers correctly.
- Consider maintaining a water supply at your facility to control small fires until emergency personnel can arrive. You might install a water tank or hoses and pumps to an existing swimming pool, pond, river, or lake. Be sure the hoses are long enough and inspect them regularly.
- If your business is located in an area subject to freezing temperatures, be sure that water outlets and pumps are protected.
- Evaluate water levels in extreme hot and cold weather conditions.
- If your water pump uses electrical power, consider obtaining a gasoline- or diesel-powered pump or generator in case electricity is cut off during a fire. However, be aware of the risk of storing a large quantity of fuel. Use an appropriate storage facility that is protected against vehicle impacts and fire.
- Have appropriate tools, such as rakes, axes, saws, buckets, and shovels, available to help control small fires while waiting for emergency personnel to arrive.

During the Wildfire

- Go to a pre-designated shelter area such as a safe room, basement, storm cellar, or the lowest building level. If there is no basement, go to the center of an interior room on the lowest level (closet, interior hallway) away from corners, windows, doors, and outside walls. Put as many walls as possible between you and the outside. Get under a sturdy table and use your arms to protect your head and neck. Do not open windows.
- Evacuation orders will often be swift and accurate for affected areas. However, if unable to evacuate, stay inside and away from outside walls. Close doors, but leave them unlocked in case firefighters need a quick access into your area.
- Turn on battery operated radio to get latest emergency information.
- If your office roof is accessible by ladder, prop it against the building so you and firefighters have roof access.
- Mark your position clearly with anything that may signal rescue workers to your presence inside the building. This could be articles of clothing or bright colored material attached to the outside of your location.
- Close windows, vents, doors, blinds, etc. Shut off gas meters, pilot lights, and propane tanks. Turn on all lights in the building to increase visibility in heavy smoke.

After the Wildfire

- Immediately check the roof (if accessible) and put out any fires, sparks, or embers.
- Contact your Agility Member Services Representative for direction on 'standing down' from an alert or declare status.
- If there is no power, check to make sure the main breaker is on. Fires may cause breakers to trip. If the breakers are on and power is still not available, contact the utility company.
- ALWAYS contact 911 if you believe it's potentially dangerous to re-enter the building and contact local experts before finally moving back in.

Your People

- Train your employees in general fire safety, especially for tasks with a high fire risk such as welding and cutting, fueling vehicles, working with flammable liquids, etc.
- Teach employees about the importance of good housekeeping and grounds maintenance in preventing and controlling fires.
- Have an adequate number of fire extinguishers and maintain them properly.
- Train key employees in when and how to use fire extinguishers.
- Consider when and how to evacuate employees if a wildfire threatens.
- Establish an evacuation plan and keep it up-to-date.
- Hold evacuation drills regularly so all employees will know who is in charge and so that they become familiar with evacuation routes and routines.
- Make sure all employees can get out of the building, find shelter, and communicate with responsible personnel.
- Plan primary and secondary exits from your buildings. Consider how employees will escape if doors or windows are blocked by an exterior fire.
- Plan two evacuation routes out of your neighborhood. Consider how employees will evacuate on foot if roads are closed or impossible to use, such as if they are blocked by emergency personnel.
- Remember that ponds, lakes, rivers, and landscaping or swimming pools can serve as safety zones.
- Keep appropriate emergency supplies on hand, including flashlights, battery-powered portable radio, extra batteries, first-aid kit, manual can opener, non-perishable foods, and bottled water. If designated employees will be working to protect the property, have appropriate clothing available, such as work boots and gloves, personal protective equipment, and sturdy work clothes.
- If you are located in a wildfire area, consider advising employees to keep personal disaster supplies and copies of important documents at work in case they need to evacuate immediately.

Recovery Solutions

- Backup Power & Fuel
- Workspace Recovery
- Data Backup & Recovery
- Technology Equipment
- Connectivity & Communication

Agility Recovery

Agility is the leading provider of the Business Continuity Management suite of solutions. Through Agility Central, we offer a business continuity training center, document storage, tabletop testing templates, emergency messaging, business continuity planning platform, advisory services, and workspace recovery. Visit our website for more information.