Agility Recovery

www.agilityrecovery.com
info@agilityrecovery.com
866.364.9696

THE DEFINITIVE GUIDE TO DISASTER PLANNING

Why Does My Organization Need a Disaster Plan?

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, strong, 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.

STEP 1: 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

Determine Roles

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

Resources:
Building the Right Team check list

STEP 2: 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

Your organization's risk is as unique as your organization itself. Examine your internal and external risks to customize your disaster plan to your organization's current needs.

- 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

- No cost solutions (ex. moving power source away from the ground floor).
- Solutions that require an investment or cost your organization is able and willing to accommodate (ex. purchase of an on-site generator)
- 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)

Resources:
Risk assessment matrix
Risk assessment form

STEP 3: DETERMINE AND PRIORITIZE 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:

1. Affect the safety and security of employees, customers and guests
2. Are the most sensitive to downtime
3. Fulfill legal or financial obligations to maintain cash flow
4. Play a key role in maintaining your market share and/or reputation
5. 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

Conduct a simple Business Impact Analysis (BIA), which will document the impact on your organization resulting from interruptions to regular operations. In order to conduct a BIA, follow these steps with your disaster team:

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.

STEP 3: DETERMINE AND PRIORITIZE ESSENTIAL BUSINESS FUNCTIONS

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 function for 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 the above 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 most closely address 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.

Resources:
Critical Business Functions Template

STEP 4: 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. Therefore, extra time should be taken in this major stage of the process to clearly articulate the steps involved, including their anticipated timeframes and required resources.

Tasks:

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

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)

STEP 4: CREATE AN EMERGENCY MANAGEMENT PLAN

- 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

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 has the ability to declare the disaster or put the plan into action?

It should be noted that 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.

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.

Resources:
Executive Summary: Emergency Management Planning

STEP 5: 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

Resources:
Crisis Communications Checklist
Social Media Checklist

STEP 6: CREATE AN EVACUATION AND SHELTER-IN-PLACE 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)

STEP 6: CREATE AN EVACUATION AND SHELTER-IN-PLACE PLAN

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 afterwards to identify areas for improvement

Resources:
Evacuation Checklist

STEP 7: 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 w/ NOAA weather
- Battery backup, solar & crank chargers for mobile devices

Protecting Continuity of Critical Functions

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

Nice to Haves:

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

Resources:
Disaster Recovery Kit Checklist

STEP 8: 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 in the event that the local datacenter has been rendered unusable
- 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
- A customized schedule for each server should be developed and maintained

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 that have been trained and are up to speed on the recovery strategy.

STEP 9: 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
- 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:

American Red Cross
www.RedCross.org

Ready
www.Ready.gov

do1thing.com
SMALL STEPS TOWARD BEING PREPARED FOR AN EMERGENCY
www.Do1Thing.com

The most effective way to generate employee buy-in is to build a culture of preparedness in the work place and make preparedness fun. Lead by example by sharing your own personal preparedness plans, and consider hosting contests and offering incentives for participation.

A SOARING EXAMPLE: JetBlue

For National Preparedness Month in September, 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.

Resources:
Power to the People Whitepaper

STEP 10:
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 by far 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.)

Resources:
Power and Generator Checklist

STEP 11: 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 nonoperational. 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 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. Alternate 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

Resources:
Work From Home Infographic

STEP 12: 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 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 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.