Agility Recovery

The Definitive Guide for Banks

Maintaining Operations Before, During, and After an Incident

Table of Contents

1. How Safe is Your Bank?

Think back to August 17th, 2017. That's the day Hurricane Harvey first reached tropical storm status in the Atlantic and became the 8th named storm of the season. By the time it finally was downgraded to a tropical depression on August 30th, it had spread devastation across Texas & Louisiana, rivaling the most costly storm in US history by accumulating an estimated **$190+ billion in damage.**

Hundreds of financial institutions were out of operation for days, some of them weeks. If your bank came to a halt as a result of a hurricane or any other disaster, you realize the importance of business continuity. Being able to maintain operations through any disruption provides uninterrupted service to your clients. If your bank has never been stopped in its tracks by a major disaster, or even a minor incident, you're very fortunate. But what about the future?

Particularly in today's world of increased cybersecurity risk, it is critical to identify the gaps in your business continuity plan and determine how you can close those gaps before a disaster strikes. In addition, Sarbanes-Oxley requires business leaders to ensure that internal controls will protect the organization from fraud. If parts of your infrastructure are down, that can be a difficult promise to fulfill.

Regularly examining and testing your disaster readiness will help your bank be prepared for any kind of disruption. It will also ensure that you can bring systems back online quickly and efficiently.

Establish Disaster Recovery Protocols

To enable your bank to conduct critical business functions before, during and after a disaster, establish the following basic disaster recovery protocols:

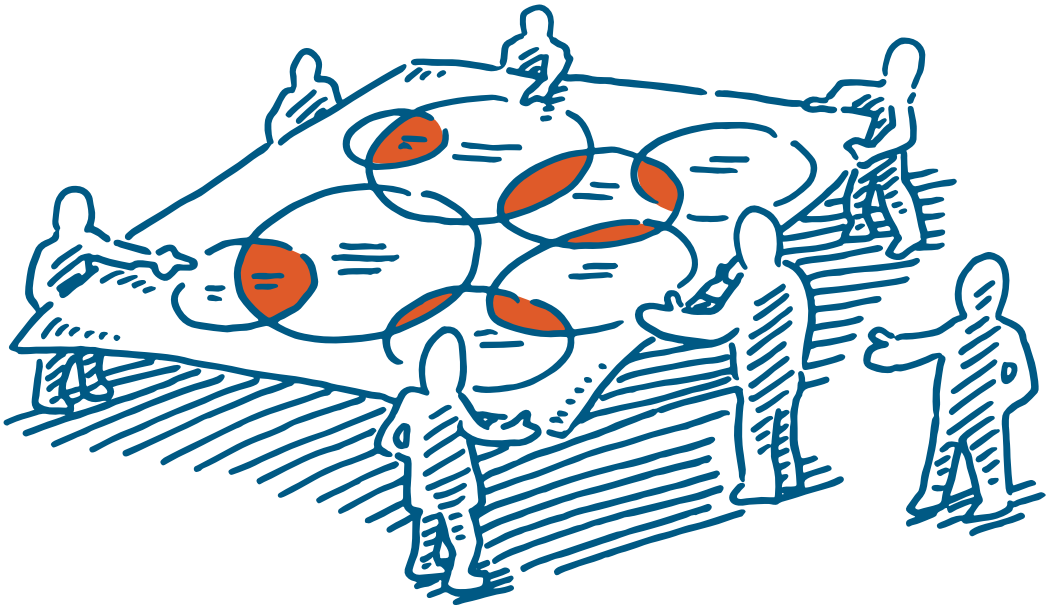
1. Assemble a disaster recovery team
2. Create a disaster recovery plan
3. Test, fine-tune and retest your disaster recovery plan

2. Assemble a Disaster Recovery Team

Get your employees involved in the disaster response planning process. Let them know you're ready for whatever crisis may occur and build buy-in to a culture of preparedness. Together, you can design a plan to accommodate challenges the team might face in 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.



The following list of disaster recovery responsibilities will get you started in identifying who should be involved:

ENSURING OFFICE & PERSONNEL SAFETY AND SECURITY
Responsibilities may include evaluating building integrity and safety, facilitating cleanup, or stocking and carrying the "go bags."

DATA ACCESS AND INTEGRITY
Responsibilities may include maintaining connectivity to your core processor and ensuring local server/cybersecurity protection or activating redundant data center.

CRISIS COMMUNICATIONS
Responsibilities may include initiating an employee call chain or alert notification protocol, or communicating with stakeholders (e.g., leadership, partners, suppliers, members, and the media).

FINANCIAL OVERSIGHT
Responsibilities may include calculating how much cash will be needed for increased transactions as well as incidentals like supplies, food/water, transportation, repairs, temporary lodging and replacement assets.

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 teams allows for equal consideration of priorities and critical tasks, as well as protects any significant inter-dependencies.

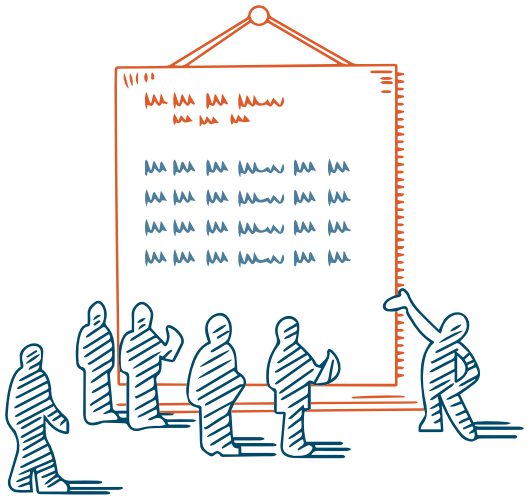
The first step is to invite every department head to an initial meeting. At this discovery session, make a list of all the responsibilities needed to maintain critical business functions (activities that are vital to your organization's survival) during a disaster. Do not attempt to incorporate all departmental functions, only those most significant to the tasks necessary following a major event.

Once you have established all the responsibilities required, assign each task to one or more employees to create redundancy. For some technical tasks, such as restoring access to data, responsibilities will closely match a person's current title and job description within the company. Other functions, such as being part of a call chain, can be assigned to a variety of staff members. Take the time to cross-train any personnel you may rely on for alternative responsibilities in a crisis.

3. Create Your Disaster Recovery Plan

Once every responsibility is outlined, write a step-by-step disaster recovery plan. Your plan should spell out who is in charge of different recovery processes, first actions to consider, and how to quickly evaluate and escalate needs.

Begin by considering the most important functions within your organization, and develop plans and strategies for protecting each from the top risks posed to your organization. Discuss how to prevent failure in each area, or if that is not possible, what it would take to bring each service or area back online quickly and efficiently.



A Good Disaster Recovery Plan Will:

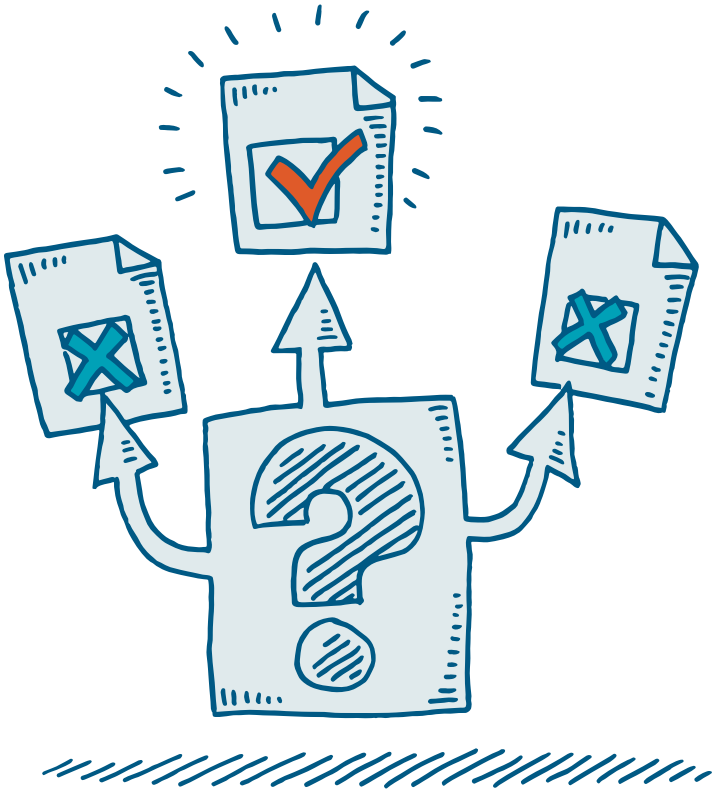
1. Establish who will be on the recovery team as well as detailed descriptions of their responsibilities. Include at least two ways of contacting each member of the team.
2. Demonstrate information on all exits and alternative ways of evacuating your building, procedures for sheltering-in-place, and the location of go-bags with description.
3. Determine how your organization's critical functions will continue to operate immediately after an incident. This may include functioning with reduced staff, replacing compromised systems, offering partial services, relocating staff and operations, communication protocols, and mitigation or recovery procedures.
4. Establish how actual recovery logistics will proceed in terms of precisely outlining and adhering to timelines, decision points and verified procedures.
5. Detail the required resources needed for mitigation and recovery. You'll want to consider what resources are required for restoration of basic services such as:
   - Office Space
   - Power
   - Applications
   - Data
   - Unique assets
   - IT network & hardware
   - Employees/staff/ partners/suppliers
   - Communications (telephone, internet, fax, etc.)
   - Other: Restroom facilities, HVAC, food/water, etc.
6. Outline the Emergency Plan procedure. Who has the ability to declare the disaster or put the plan into action?

4. Test, Fine-tune, and Retest Your Disaster Recovery 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. Testing or exercising your plan should be a gradual and continual process.

A Good Test Will

1. Use realistic scenarios based on identified risks to your organization
2. Meet compliance or regulatory requirements
3. Increase employee, management, and community confidence in the plan
   - This includes setting realistic expectations for response team members
4. Expose holes, gaps, misperceptions, or other potential failures of the plan
5. 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 (when performed safely!)
6. Improve your overall readiness and reduce recovery time



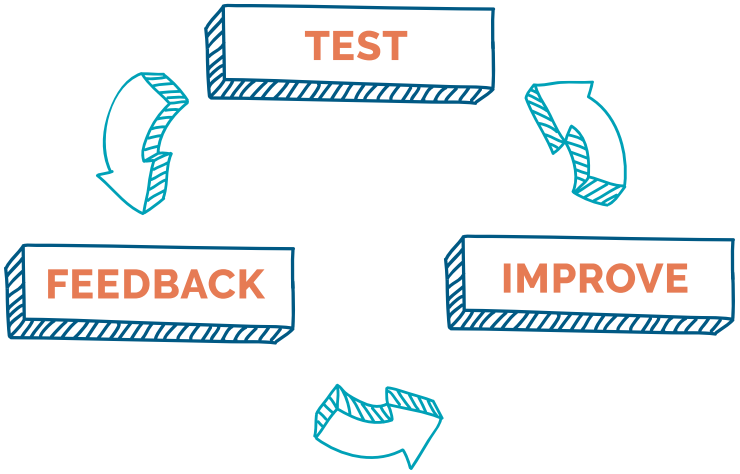
Hold regular walk-throughs of building emergency exits, and conduct drills for both shelter-in-place and workplace violence scenarios, as well as building evacuations. More elaborate and comprehensive testing can be facilitated in one of three places: at your facility, at your off-site backup center, or at a disaster recovery-partner testing site. You can choose to do a table-top meeting-style run through or a full-scale hands-on test, using canned or live data and a variety of scenarios.

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.

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 members after a disaster.

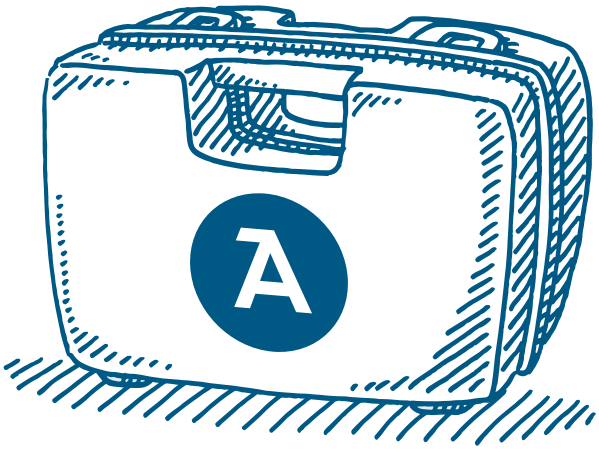
We recommend that you do a full-scale test annually for a wide range of critical functions, including access to electricity, water, gas, facilities, staffing, technology, telecommunications and more, not only to survive, but to thrive in any unexpected situation.

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:



5. 10 Ways a Disaster Recovery Solutions Provider Can Help You With Testing

1. Determine priorities and objectives and build outcomes
2. Simulate real-time business transactions
3. Test all aspects of your recovery operation
4. Evaluate how much generator power is needed
5. Determine realistic recovery timeframes
6. Resolve discrepancies
7. Conduct a server rebuild and restoration
8. Test network connections, & build redundancy in your systems
9. Practice reconnecting to your core
10. Test a mobile office setup



6. What is a Go-Bag?

A go-bag is an emergency kit that is ready to be used at all times. Your emergency kit should contain everything your organization needs in the event of evacuation. When disaster strikes, time is of the essence. An office emergency kit is unique and includes a few key items not in a personal emergency kit. Store the following items in one or more central locations in a waterproof container.

Employee Health and Safety Items

First Aid Supplies/Kit

Plan to regularly restock and ensure proper quantities of first aid supplies

AED

(Automated External Defibrillators)

Emergency Supplies

Food, water, flashlights, tools, battery powered radio, mobile and solar chargers, petty cash, building keys

Items for Protecting Continuity of Critical Functions

Important Documents and Records

- **Documents**: recovery plan, damage assessment forms, critical process flow documents, server recovery scripting, phone redirect scripting, data backup procedure
- **Records:** insurance policies, employee rosters and contact information, contracts, vendor/ partner contact information, fixed asset inventory

Login and Password Credentials

Office Supplies

7. Regulatory Compliance and Disaster Recovery

Banks are required by FFIEC to have disaster recovery plans in place before they can be approved. They require a risk assessment to identify and quantify threats to information assets and to ensure that the solutions institutions have in place to mitigate risks are viable.

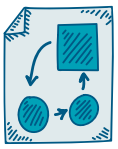
One of the questions asked during an audit could be the date of your most recent risk assessment. There is also an entire section focused on your disaster recovery program that asks the following questions:

Y	N	
		Do you have an organization-wide disaster recovery and business continuity program?
		Are disaster recovery and business continuity plans based upon a business impact analysis? If yes, do the plans identify recovery and processing priorities?
		Is disaster recovery and business continuity included in your risk assessment?
		Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations?
		Do business continuity plans address procedures and priorities for returning to permanent and normal operations?
		Do you maintain offsite backups of critical information? If yes, is the process formally documented and audited?
		Do you have procedures for testing backup media at an offsite location?
		Have disaster recovery/business continuity plans been tested? If yes, please identify the system(s) tested, the corresponding test date, and the date reported to the Board.

8. Lessons From Major Hurricanes: How to Protect Yourself from the Next Weather Disaster

Every Storm is Different

Don't just learn the lesson of what happened. Think ahead. Every weather pattern is unique; don't assume you will have the same experience every time.

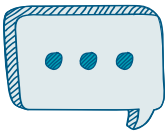


Proper Business Continuity Planning Saves Jobs and the Local Tax Base

The most successful way to prevent a lengthy business disruption is to plan for it. Thorough planning will ensure that your team always has a blueprint for recovery that will work in a real-life situation.

Think, Work, and Act Like a Team

Employers should encourage employees to have their own family emergency plans and to strengthen their homes to withstand disasters as well as possible. Since employees are the first line of defense in a disaster, employers should offer advice and try to help their employees in any way they can.



Make Communication Your Number One Priority

Disaster recovery requires everyone to work together, meaning that communication is integral to disaster recovery success. Communication keeps everyone in contact during business recovery, and allows companies to locate all employees in a crisis situation.

Test and Retest

What sounds good on paper might not always work in a real situation. Did it take longer to get down a certain hallway than you had planned? Did your redundant server automatically protect your data when your primary server went off? Did the security cameras stay on when the electricity went out? These are the types of things that can only be determined by doing.

9. Testing and Preparedness are the Keys to Survival

We work in a world today where automation and connectivity are crucial to smooth business operations. Many information technology systems are virtual and many applications and databases are in the cloud. These are competitive strengths when they're working, but when electricity and telecommunications are down, all these systems come to a halt.

Testing of information technology recovery and restoration is all the more vital in today's digital world. Having regular back-ups, redundant infrastructure, and a disaster recovery partner who can relocate your operations to a fully stocked mobile branch, or other temporary space, are all competitive advantages in a crisis situation.

As the most recent hurricanes showed us, lack of access to financial institutions makes it difficult for people to recover from crises in a timely fashion. Following these events, people were hurt, hungry, and had nowhere to go. As a bank, you should ensure that situations such as these don't happen again to the communities you serve.

No matter what the situation, disasters don't have to shut down your bank. Proper planning and testing mean your organization will have minimal, if any, downtime during a crisis. Take steps today and put your testing procedures in motion.

Agility Recovery

1601 Wewatta Street, Suite 300, Denver, CO 80202

866-364-9696
contactus@agilityrecovery.com

We are the leading provider of business continuity and disaster recovery solutions. After a business interruption, we deliver the resources that make recovery and resilience simple. Our customers have guaranteed access to temporary power, furnished mobile office space, communications equipment, and technology, as well as planning and testing resources. In the wake of the unexpected, we make resilience simple by providing the expertise and resources your organization needs to recover quickly. Whether you're a seasoned continuity professional or creating your company's emergency plan for the first time, we're ready to support you and your team.