



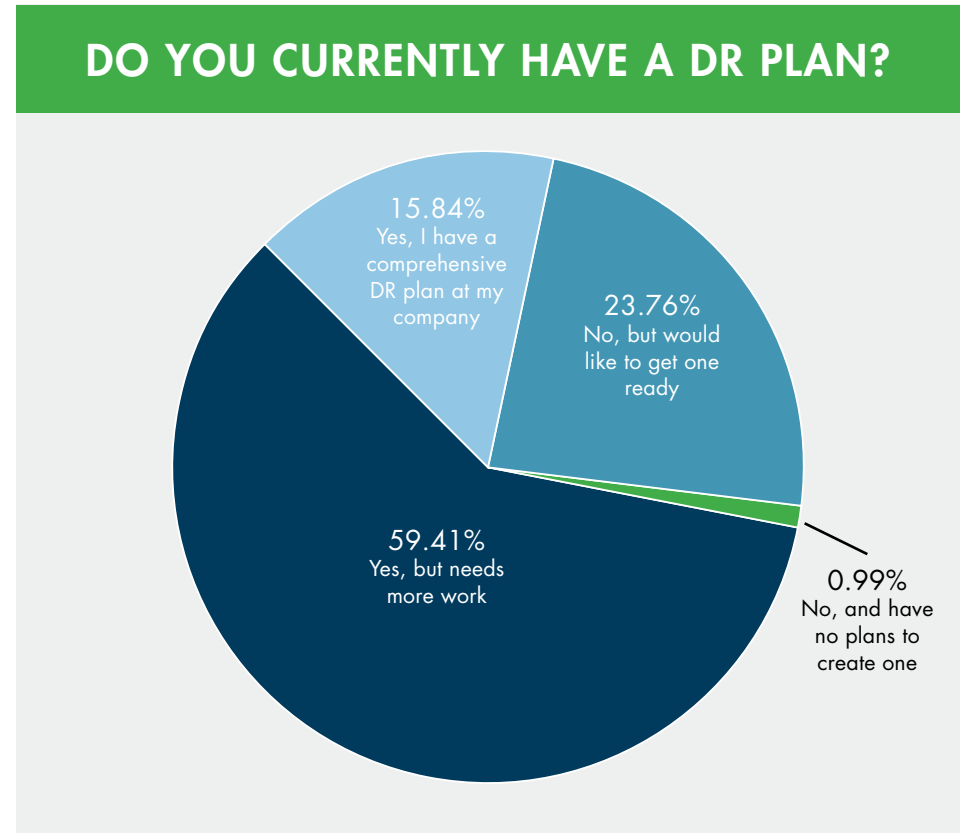
Best Practices in Disaster Recovery Planning and Testing

Best Practices in Disaster Recovery Planning and Testing

Disaster Recovery plans are widely accepted as a way to ensure all critical data, IT systems and networks can be recovered in any event classed as an emergency. These plans also ensure that corporate business objectives can be achieved during the disruption. In short, it is a plan that keeps a business operational.

In a recent Disaster Recovery survey, we asked business owners if they currently had a Disaster Recovery Plan in place. While only 1% felt secure without one, the overwhelming majority didn't. More than 57% of those surveyed said they currently have a plan that needed a little work; 27% said they don't have a plan, but would like to develop one; and the remaining 15% have a plan that they felt was good to go.

You may think of these plans as a documented strategy to save your business in the event of a major disaster like a flood or fire, and you wouldn't be alone. But the reality is that a Disaster Recovery plan is created to protect your infrastructure against any event that could cause disruption, including technical glitches, system failures, power outages and even cyber attacks or data theft. These disruptions cost companies thousands (and in some cases hundreds of thousands) in damage and an even bigger loss at the end: damage to the company's brand.









White Paper: Best Practices in Disaster Recovery Planning and Testing



DEVISING YOUR PLAN

There are a few key elements necessary for your plan to run efficiently:

- 
Management Support:
 Without the support of management, creating the plan is futile.
- 
Approved Funding:
 Keeping your company running takes additional resources and these resources cost.
- 
Structured Plan Framework:
 This ensures that everyone is on the same page with the plan.
- 
Access to Qualified Staff:
 Don't assume that everyone in your IT team is qualified to put together or execute this plan. This may require additional training or bringing in expert consultants.
- 
Access to Relevant Information:
 You'll need to conduct a little research or a few interviews to gather the information you need.
- 
Documentation and Testing:
 Your plan has to be documented and tested regularly to ensure smooth execution in the event of an emergency.

All of these elements combine to form the goal of the DR plan, which is to build a plan and associated documentation based on a structured framework that is consistent with good practices and standards. The good practices and standards ensure that you're not only following the guidelines of what's best for your business and industry, but that you are also compliant with any regulations that surround recovery and planning in your industry and country. Common standards used in the DR industry include:

- Standards:**
 NFPA 1600:2010; ISO 27031:2011; ISO 22301:2012; NIST 800-34
- Regulations:**
 FINRA 4370
- Good Practice:**
 BCI Good Practice Guidelines, FFIEC Handbook
- Corporate DR Policies:**
 Existing corporate policies that should apply to your DR plan

Gathering the above information will take a little time, but it's worth it to keep your business going through any situation. When gathering this information, it's important to also identify anything that could cause a glitch in your plan, the objectives you have for your system, network and IT asset recovery and anything your company can do to mitigate your risks. In the next section we will explore the components that make up your plan.

White Paper: Best Practices in Disaster Recovery Planning and Testing

Sample Policies and Standards

For a comprehensive list of existing legislation and regulations worldwide related to Disaster Recovery and Business Continuity, refer to the [Business Continuity Institute publication BCM Legislations, Regulations & Standards](#).



The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), recognized NFPA 1600 as the National Preparedness Standard. Created by the National Fire Protection Association, the NFPA 1600 “[Standard on Disaster/Emergency Management and Business Continuity Programs](#)” contains provisions related to the development, implementation, assessment and maintenance o programs for prevention, mitigation, preparedness, response, continuity, and recovery.



The [ISO/IEC 27031:2011](#) describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization’s ICT readiness to ensure business continuity. The [ISO 22301:2012](#) specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.



NIST [Special Publication 800-34, Contingency Planning Guide for Information Technology \(IT\) Systems](#) provides instructions, recommendations, and considerations for government IT contingency planning.



[Rule 4370 of the Financial Industry Regulatory Authority](#) requires firms to create and maintain business continuity plans (BCPs) appropriate to the scale and scope of their businesses, and to provide FINRA with emergency contact information.



The [Business Continuity Institute Good Practice Guidelines \(GPG\)](#) are the independent body of knowledge for good Business Continuity practice worldwide.

Gathering the above information will take a little time, but it’s worth it to keep your business going through any situation. When gathering this information, it’s important to also identify anything that could cause a glitch in your plan, the objectives you have for your system, network and IT asset recovery and anything your company can do to mitigate your risks. In the next section we will explore the components that make up your plan.

White Paper: Best Practices in Disaster Recovery Planning and Testing



PLAN COMPONENTS

The previous information is there to help you structure your plan, but these components are what you need to run it. For a Disaster Recovery plan to actually work, there are certain elements that have to be included. These are all important to the plan's ease of execution and effectiveness and they begin with your company's own DR policy. Since both management and non-management staff are involved in Disaster Recovery, everyone should be aware of these policies. A meeting or the distribution of the policy will be necessary as soon as the key members of the plan are identified.

Your DR plan should include the IT DR plan, the results of previous efforts for testing the plan, and supporting documents.

The supporting documents for your DR plan are what stand between a successful recovery and a failed one. These documents include processes for data backup, information about off-site storage and processes, vendor and maintenance contracts, diagrams, and training plans.

DEFINE

- Plan scope, purpose and authority
- Policy statement
- Management approval and funding
- Staff roles and responsibilities
- Authorized person to declare disaster
- Step-by-step procedures for recovery of all physical, mechanical and virtual items (this includes premise security, records and wireless technology)
- Step-by-step procedures for alerting key people (includes members of staff, family members, media, vendors and alternate vendors, clients, stakeholders and first responders)
- Process for training

IDENTIFY

- IT resources
- Risks and impact on IT assets
- Process for equipment replacement
- Process for obtaining spare parts
- Designated spokesperson

DETERMINE

- Recovery Time Objectives (RTO)
- Recovery Point Objectives (RPO)
- Preventative controls
- Response and recovery strategies
- Event notification procedures (could be an automated feature or an outsourced call center)
- Recovery failover procedures
- System restart/failback procedures
- Resumption of business procedures

USE

(if necessary)

- Hot/Cold Sites (Hot sites have most of what you need to keep your business running, including hardware, software, servers and computers. Cold sites provide the power, environment and workspace, but no equipment.)
- Help desk support
- Call trees
- Automated Notification Systems
- Conference bridges

White Paper: Best Practices in Disaster Recovery Planning and Testing

Next, everything should be compiled into a document. All aspects of your plan (including the above gathered information) should be made available to all DR personnel. Your plan should have a TOC (Table of Contents) and outline that lists each step of the plan in order of importance. (Emergency Response Actions should always come before anything else).

Lastly, include a Business Impact Analysis Report and Risk Assessment Report – this is vital. The RA (Risk Assessment) will outline events that could disrupt your business and the BIA (Business Impact Analysis) will illustrate how these disruptions will impact it.



THINGS TO AVOID WHEN CREATING THE DISASTER RECOVERY PLAN

Although gathering the above information is a lengthy process, avoid skipping any of the steps or required sections. Some businesses make the mistake of utilizing generic DR plans or the plans of other businesses in their industry. This may seem like a time-saver at first, but you'll see during testing that it could prove disastrous. The other business (or the business that the generic plan

is modeled off of) could have more assets or finance than you or have fewer risks than you. So, if that plan only covered natural disasters and your business is the victim of data theft – it's pretty much useless. This makes research – and more importantly a BIA and RA– a must.

Other pitfalls you'll want to avoid are:

- ✘ **Not defining a clear budget from the start**
- ✘ **Skipping testing and reviews**
- ✘ **Creating the plan without management's backing**
- ✘ **Keeping all copies of the DR plan on-site**
- ✘ **Summarizing procedures in the plan**
- ✘ **Not training DR personnel**
- ✘ **Assuming that all systems will be backed-up and running immediately**
- ✘ **Assuming all listed personnel will be available (including IT staff)**

The last item is possibly the most important in this section. As your business grows or expands into other areas, your needs, risks, vendors and key personnel may change. This requires you to manually update the plan and recalculate any figures contained within it. Once you do, the new plan should be discussed and another exercise should take place.

White Paper: Best Practices in Disaster Recovery Planning and Testing

TECHNOLOGY OPTIONS FOR DISASTER RECOVERY

A good Disaster Recovery plan will also discuss the technology behind your DR efforts. What kind of technology you use depends on your risks, how much data you have to store, the number of people needed to access that data, and the sensitivity of the data.

When we asked business owners what kind of technology they used for Disaster Recovery, the numbers were surprising. More than 69% said they still use local backup to a disk or tape. While local backup might seem like an attractive option at first, it leaves businesses susceptible to interruption in a variety of scenarios such as power outage, virus attack, or server crash. All three could have serious business implications.

Due to budgetary constraints, some companies build their own DR architecture, assembling different products or building some infrastructure in-house. We have seen, for example, companies using local backup products in combination with automated scripts developed by their

engineers to off-site data to a public cloud storage like Amazon. Other companies mix different flavors of server replication to accommodate for their heterogeneous environment.

While interesting at first, the “do-it-yourself” approach to Disaster Recovery leads to a number of issues. As explored by Forrester Research in its report on the risks related to DIY DR, companies report a number of challenges when it comes to their in-house DR infrastructures, namely:

- Lack of focus on DR relative to other IT projects
- Not enough DR testing
- Lack of funding to keep DR infrastructure up to date
- Lack of skills in-house
- Not confident in ability to respond to a real disaster

These results clearly show that bringing Disaster Recovery in-house is not the best choice for most companies. When looking at the different options available, businesses that have taken into consideration the Total Cost of Ownership (TCO) seem to have gotten a better bargain.

While an expanded discussion of TCO is outside the scope of this document, keep in mind that the effectiveness of a Disaster Recovery plan is also tied to the effectiveness of the underlying technology being used to recover from a disaster.

TOTAL COST OF OWNERSHIP

Total cost for owning a disaster recovery solution takes into consideration factors such as:



Capital Expenditures:

Cost of purchasing software, hardware, and implementing the solution



Operational Expenses:

Cost for maintaining the solution, including time spent reviewing backup logs, ensuring successful completion of backup jobs, troubleshooting error messages, testing restores and running full DR tests



Downtime:

The time that it takes to bring files, applications, full servers and a full site back into production after an outage and related costs associated for loss of productivity and revenue

White Paper: Best Practices in Disaster Recovery Planning and Testing

CONSIDERATIONS FOR DR TESTING

Businesses responded with surprising answers when asked, "How often do you test your DR plan and/or the ability to recover from a disaster?"

34%
Skip testing

24%
Once a year

12%
Two to four times
per month

5%
Every
month

26%
Not as often as I should

How often you should test is determined by your risks and assets. Those who are at a greater risk like to test more frequently (say, every week), those who are at a moderate risk may test quarterly, and those who are at a very low risk may only test once a year. However, no matter what category your business is in, you should always test your DR plan.

TIPS FOR DR TESTING

Here are a few tips to follow:

- » Make sure the test is set for a date that isn't critical for your business and a date where all participants or alternates are present. You'll also need to notify your IT staff at least two weeks prior to testing.
- » Document the step-by-step procedures of the test and hand them out to all selected personnel.
- » Before administering the test, think about the area you need to test. It may not be (and almost never is) possible to test all aspects of the plan at one time, so test section by section. You also need to keep in mind how much strain this test will have on your systems. Running a test might disrupt them and cause further disruptions to processes that need to keep running.
- » Find an environment to test in, preferably in a non-production area. Most businesses use conference rooms or empty offices for this.
- » Gather all personnel listed in the DR plan and have them play out their roles in the test.
- » Include a timekeeper.
- » Keep note of what did and didn't work in a report, and update the report based on the results.
- » Do a dry run first.

White Paper: Best Practices in Disaster Recovery Planning and Testing

All of the above tips are designed to keep you and your staff abreast of any changes that could affect the plan or the execution of it.

To make the most of your Disaster Recovery Plan, document it. You may not be present when an event occurs, so multiple copies should be available to selected staff members. Finally, run your DR plan by management each time a change is made to ensure financial backing and approval. By following this guide, you'll not only safeguard your business, but you'll also save yourself from hidden risks that would have otherwise gone unnoticed.

Additional Resources

For more information about best practices in disaster recovery planning and related topics, we encourage you to check out the following resources:

[Webinar Recording "Best Practices for DR Planning and Testing"](#)

[Webinar Recording "Key Criteria for Selecting a Business Continuity Solution"](#)

[Whitepaper "The IT Manager's Essential Guide to Preventing Downtime"](#)

[Whitepaper "The Five Myths of Reliable Tape Backup"](#)

[Whitepaper "Building a Business Case for Business Continuity"](#)



www.axcient.com



800-715-2339



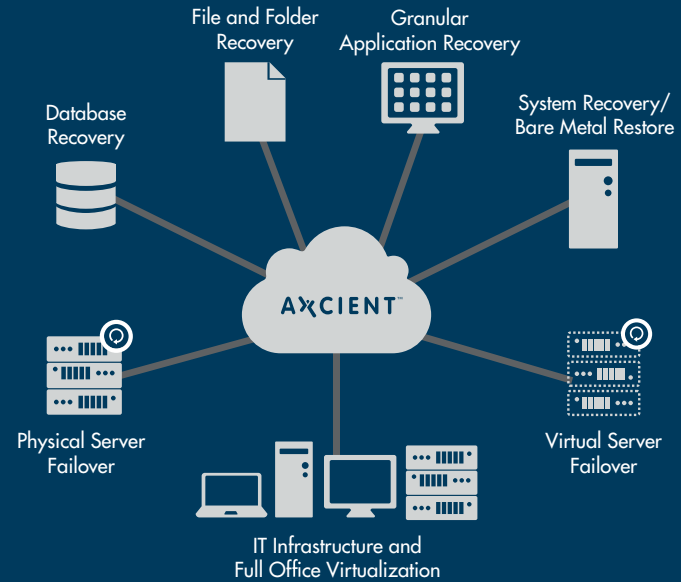
@Axcient



[linkedin.com/company/axcient](https://www.linkedin.com/company/axcient)



[axcient.com/facebook](https://www.facebook.com/axcient.com)



The Axcient Solution

Axcient's Recovery-as-a-Service cloud eliminates data loss, keeps applications up and running, and makes sure that IT infrastructures never go down. Axcient replaces legacy backup, business continuity, disaster recovery and archiving products, with a single integrated platform that mirrors an entire business in the cloud, making it simple to restore data, failover applications, and virtualize servers or an entire office with a click. Thousands of businesses trust Axcient to keep their applications running and employees productive.

Learn more at www.axcient.com.