

10 things to look for in a disaster recovery service provider

Executive Summary

Most organizations today understand that a disaster recovery (DR) plan is essential to their continued survival should a natural disaster occur. But implementing a DR plan entails substantial time, effort and cost — not to mention significant investment in developing new areas of technical expertise within the organization. As a result, many organizations are turning to disaster recovery service providers (DRSPs) to offload their disaster recovery operations.

This checklist describes what organizations should look for to ensure that the DRSP they select not only provides high quality service and expertise — but also meet their specific business requirements.



Why Organizations Need DRSPs

All organizations need a disaster recovery plan to protect their business in the event of unplanned downtime or natural disaster. Indeed, a 2012 study by the Business Continuity Institute found that (74%) organizations view unplanned IT and telecom outages as the top threat to their business, based on their own risk assessment¹. Organizations in regulated industries, such as financial, insurance or healthcare, moreover, must adhere to strict mandates to institute a DR plan or face fines.

Yet smaller organizations may lack the in-house manpower or technical expertise to set up the duplicate data centers necessary to implement the DR strategy. Many organizations also find that having in-house staff perform DR diverts valuable IT resources from supporting the organization's core business activities. Faced with the high costs and

substantial human resources necessary to design and implement a DR plan, many organizations are turning to disaster recovery service providers (DRSPs) to perform these tasks rather than do so in-house. With considerable expertise specifically devoted to disaster recovery, DRSPs also do a better job of preventing downtime than organizations can themselves. A recent report by the Aberdeen Group found that the average yearly cost of downtime for DRSP customers was \$207,000 compared to \$1,004,640 for organizations who managed their DR infrastructure in house².

It's not surprising then that Forrester Research found that 23% of organizations surveyed have moved or plan to move to a DR SP, while another 43 percent express interest in these services³.

1 "Horizon Scan 2012" Business Continuity Institute, January 2012 <http://www.bcifiles.com/BCIHorizonScan2012.pdf>

2 ["Why Mid-Sized Enterprises Should Consider Using Disaster Recovery-as-a-Service,"](#) Aberdeen Group, April 2012

3 ["State of Enterprise Disaster Recovery Preparedness, Q2 2011,"](#) by Rachel A. Dines, Forrester Research, May 18, 2011



How to Ensure a DRSP Will Meet Your Needs

Yet organizations may be concerned about how to select the DRSP.

The solution?

Before beginning the search, first define internal requirements, and then use those requirements to define the type and level of service the DRSP should provide. By carefully defining the necessary services and service levels, an organization will be in a better position to determine whether the DR SP meets their requirements.

Organizations define their internal requirements using a Business Impact Analysis (BIA). They then use the results from the BIA as the basis for the Service Level Agreement they demand from the DRSP.

Business Impact Analysis

Because no organization can justify the expense of including every business process and application in the DR plan, they need to prioritize the level of protection necessary for each one. Start by working with the line-of-business managers to inventory each critical business process and determine its vulnerabilities. Then identify the amount and cost of downtime the organization can sustain for each application. For example, processes that must be resumed within 24 hours to prevent serious business impact, such as loss of revenue or major impact to customers, can be rated as Priority A. Processes that must be resumed within 72 hours can be rated as Priority B. Those that can take more than 72 hours to be restored can be rated Priority C, and so on. Use these prioritizations to build the DR plan and determine the resources and service levels necessary for various applications.

Service Level Agreement

Develop a service level agreement (SLA) to define the level of service expected from the DRSP. The SLA should specify what service will be provided, the expected performance with regard to the services being delivered; metrics against which performance will be judged; and the remedies in case the agreed-upon deliverables are not satisfactorily delivered.



10 Things to Look for in a DRSP

Once the necessary services and SLA s for each application have been mapped out, it's time to perform due-diligence on the DRSP. The following 10 issues are of particular importance:

1

Support

Disaster recovery requires specialized knowledge and skills proven through successful and ongoing testing. A DRSP gives organizations access to a highly skilled technical staff that assists numerous customers through frequent test exercises and potentially several disasters over the course of a year. At the best DR SPs, employees bring many years of experience to their roles and receive ongoing training and certifications to stay current in the latest operating environments and different technology combinations. By meeting the varying needs of many different customers in multiple industries, they bring breadth and depth to each customer's DR plan.

Additionally, DR is the primary focus of DR SP staff. The service provider's entire business is built upon delivering disaster recovery services, facilities and support. Because it specializes in DR , a successful DRSP is likely to have greater DR experience and more proven know-how than even the best trained in-house team.

When evaluating DRSPs, look at whether they deliver support 24/7/365. The DRSP should also allow you to pick and choose from a full suite of support options, including:

- Designing the DR plan
- Testing the DR plan
- Notification of any problems
- Restoration



2

Testing

Recovering from a disaster hinges on preparing accurate and current disaster recovery procedures. Yet production environments are constantly changing. Many organizations fail to recover or take longer to recover than necessary because their procedures are not accurate or current. Periodic testing of the DR plan is critical to discover problems during the test and not during a disaster.

Make sure that the DRSP permits testing of everything in the contract — all servers, platforms, applications, and any other items to ensure the business continuity plan works. The DRSP should allow customers to schedule testing as necessary, typically one to three times each year.

3

Ability to Handle Recovery

Customers that work with DRSPs are typically responsible for managing their own recovery. However, during a disaster, staff may have difficulties traveling to the facility to begin the recovery. Organizations that have critical data that must be restored quickly should consider a DR SP that has the ability to furnish expert staff to start the recovery.



4

Ability to Support Multiple Customers

DRSPs typically serve multiple customers at the same time. But what happens if several DRSP customers declare emergencies simultaneously, a distinct possibility in the event of a natural disaster? The DRSP should have the expertise to prioritize the requirements for each customer to enable them to restore their most important applications first and get their other applications up and running within the appropriate timeframe.

5

Separate Production and Disaster Recovery Sites

Because hot DR sites entail significant and ongoing expense, many DRSPs look for ways to gain additional ROI from these sites by providing overflow or peak processing services. However, a DRSP that delivers production services will be unable to stop running production applications should a disaster occur, which limits resource availability for disaster recovery. Therefore, look for a provider that does not handle production and DR on the same equipment.



6

Remote Access for Recovery

Typically, organizations must send their staff to the DRSP site to recover from a disaster. However, some DRSPs provide another option that can increase convenience and lower costs: remote access. For organizations with hot backups, the DRSP can deliver remote access over the Internet. Customers with tape backups can send tapes to the DRSP, who will mount them and then deliver access via the Internet.

7

An Internal Disaster Recovery Plan

The DRSP's reliability, availability, and ability to serve users during a disaster are essential. This means DRSP needs its own disaster recovery plan. To research a DRSP's internal DR plan, start by reviewing the DRSP's SAS 70 audit. SAS 70 is the authoritative guidance that allows service providers to disclose their control activities and processes to customers and customers' auditors in a uniform manner. In addition, ask to see a copy of the DRSP's internal DR/BC plan. Ask how often the DRSP tests that plan — every four months is a good rule of thumb. The DRSP's continuity plans should be addressed as part of the SLA or contract.



8

Consistent Internal Processes for Serving Subscribers

The DRSP should have in place a set of internal processes to ensure that they provide a consistent level of service across all their customers. The DRSP should set up, document, and follow processes to provide a consistent level of technical support as well as comprehensive processes for on boarding customers, scheduling and performing testing, and for customers to use when declaring a disaster. These internal processes support ISO standards.

9

Data Center Considerations

The DRSP's data center itself is an important consideration. Look at:

- **Security:** Is the data center hardened with good physical security and control of access to the facility?
- **Location:** Are there any geographic hazards? For example, is the data center located on an earthquake fault line or in a tornado-prone area? Have adequate precautions been put into place to manage these risks?
- **Redundancy:** Does the data center employ redundant networks, communications links, and power supplies, such as a generator or a separate power grid?
- **Fire suppression:** What mechanisms does the DR SP use for fire suppression?



10

Expertise

Evaluate the expertise of the DRSPs. Go to their website to determine their level of ISO 9000 certification. What type of disasters have they handled? How many disasters have they handled? What type of recoveries have they performed? What is the average size of the company they've recovered? Ask for testimonials from existing customers. Additionally, many DRSPs provide customers with surveys after an event or test and then create a report that dissects what occurred during the event. Ask the vendor to see those reports — with confidential customer identification redacted.



Conclusion

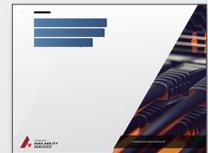
A good disaster recovery plan and implementation is critical to your business's very survival in the event of a disaster.

By following the 10 steps detailed here, organizations can ensure that they select a DRSP that adheres to best practices and has the expertise to deliver a successful disaster recovery. More importantly, they can ensure that this plan addresses the specific needs of their business.

Additional reading



[4 Reasons Why CIO's Lose Their Jobs](#)



[10 Things Your Team is Afraid to Tell You About Your DR Plan](#)

About Sungard Availability Services

Sungard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software.

To learn more, visit www.sungardas.com or call 1-888-270-3657

Trademark information

Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us

