bluelock®

Ultimate Guide to DRaaS

How to empower your business with Disaster Recovery-as-a-Service

Bluelock LLC • 5303 Lakeview Parkway South Dr., Indianapolis, IN 46468 • 888-402-2583 • bluelock.com

BUILDING A BETTER DR PLAN

Disaster recovery (DR) is not easy. It's critical to protecting your organization's most precious assets, though typically under-funded and under-appreciated. Now that always-on business is the new normal, any form of downtime can be detrimental to the livelihood of your organization. Having a strategic plan in place is paramount.

Disaster Recovery-as-a-Service (DRaaS) is changing the way many businesses are tackling the complexities of DR. This action-oriented guide will help you assess your organization's needs and priorities and develop an effective DRaaS strategy. We'll help you recover data quickly and effectively, with confidence.

YOUR DRaaS CHECKLIST

- ☐ **Assess your budget** - Learn what you are able to spend across all applications and determine what cost approach would best meet the needs of each.
- ☐ **List your applications** - Rank each application and group them into tiers, based upon their importance to your daily operations.
- ☐ **Perform a risk assessment and business impact analysis for each application** - Know how long the business can function without each application and how much data and time can be lost in a worst case scenario.
- ☐ **Determine each application's ideal RTO and RPO** - Your budget may not allow for each application to be protected with minimal RTO and RPOs. Establish a timing and budget framework for your solutions.
- ☐ **Establish your recovery destination** - Once you've grouped your applications into recovery tiers, determine what destination would be best for failover and recovery during a disaster.
- ☐ **Review security needs to protect sensitive data** - If you have sensitive data, thoroughly assess providers and technology capabilities for the best protection.
- ☐ **Create a DR playbook** - Lay out the recovery process step-by-step to document the order of recovery for your applications. Consolidate those steps into a Disaster Recovery Playbook and keep a hard copy where you can get to it when needed.
- ☐ **Establish a regular testing schedule** - Test, test and then test again. This will alert you if any changes need to be made, building confidence in your recovery plan.

#1 Assess your budget

Determine what budget you have to spread over your applications for recovery and backups. Then discuss what applications are the most critical and which need the most attention during a crisis. This will help you focus your budget accordingly.

To assess what applications warrant the majority of your budget, it's helpful to estimate a **recovery time objective (RTO)** and **recovery point objective (RPO)** for each application.

A RTO may be seconds, minutes, hours or days depending on its time sensitivity and impact. To accurately determine a RTO, consider what the ideal recovery time frame would be for a disruption. Then determine what time it would take to validate that application before returning it to regular functions. It's important to keep in mind that the faster the desired recovery time, the more expensive it will be.

RPO denotes the point in time from which you choose to recover data. For example, everything prior to an application's RPO will be recovered, but anything after that point in time will be lost. The desired RPO may vary depending on the importance of each application and data set, and the nature of the disruption. For example, you may want to be able to choose a different RPO range for an intrusion event than a power outage. Use technology that allows you to choose a specific recovery point.

There may only be a few applications that will warrant the budget to recover with your minimum RTO and RPOs. Some applications may be fine with a downtime of 3-5 days on backups and some applications may be considered test/dev and not warrant protection at all.

Sometimes, your budget can be strained to accomplish minimum RPO and RTOs in-house. Compare the costs of outsourcing your DR plan to a DRaaS provider who can take on the most time-intensive management aspects of DR. Without needing to purchase hardware, hire new team members and devote your in-house talent to DR implementation or testing and recovery, you can free up your team to focus on other business initiatives – which saves money. Your DRaaS provider should also be able to share insight into how other companies have managed multiple tiers of recovery effectively within budget constraints.

#2 List your applications

Compile a comprehensive list of every business application, understanding the role of each, then organize them based upon their importance to business continuity. Open a dialogue with all business units so that you can fully inventory everything and learn which applications they value most.

Establish a point of contact within each business unit who will keep a dialogue with you. This will encourage future discussions regarding significant changes, new applications or older ones being phased out. Also, this will ensure you aren't protecting legacy applications or leaving new applications unprotected.

Through cross-functional conversations, you will be able to prioritize your applications based upon their importance. Arranging them will determine which applications need the most attention during an event. After you create your list, you are able to set the RTO and RPO for each.

#3 Perform a risk assessment and business impact analysis for each application

Once you've noted all applications, work in conjunction with other business units to perform a risk assessment and business impact analysis for each application. This process is vitally important to making sure your DR plan protects what is most important to your business.

During this process, remember to look at the totality and connectivity of the applications. The business unit may not be aware of how one application affects another. Don't just consider outage scenarios, but smaller interruptions too – anything that could impact the business should be assessed. It might not be a hurricane that hits your datacenter, but rather a faulty wire or human error that causes an event or outage.

When evaluating the critical nature of an application, look beyond the revenue-generating applications and remember to include customer service, financial and other core functioning applications. Determine which will be necessary in the event of a disruption and in what order they should return to full operation.

#4 Determine each application's ideal RTO and RPO

After you've assessed all business applications, determine the ideal **recovery time objective (RTO)** and **recovery point objective (RPO)** for each. In order to determine your RTO and RPOs, you will need to consider what technology is available to meet your needs. Here are some common DRaaS solutions:

Always-On: This allows continuous protection and disaster recovery for always-on availability. If one environment should fail, the other is already running and is fully accessible. By having things kept in a production-like state, this results in instant RTO and RPOs. This solution may be in the form of Active/Active or Active/Passive.

Real-Time Replication: Also known as *Continuous Data Protection*, this provides recovery in a matter of seconds or minutes. Real-time replication tracks and writes changes as they occur in an environment, so you can roll back to an earlier version if something goes wrong. These restore points can be for updates down to the smallest level of granularity.

Backup-based Replication: For applications that don't have a high rate of change, you can replicate them in timed increments at an application or block-level. Backup-based replication records a full environment, then reports changes on a regular basis (typically once a day) based on the nature of the application. It doesn't archive iterations like a traditional backup. Instead, you can set times for replication and consolidate changes over a longer period of time.

Traditional backups are not specific to DRaaS, but are still important to consider. While backups don't facilitate flexibility or efficiency as a recovery method, they offer a good offsite, long-term solution for data retention, especially for environments with a low rate of change or data with specific archival retention requirements.

The goal of DRaaS is to achieve data recovery for as close to "now" as possible. To match each application to the right form of recovery, understanding their rate of change and bandwidth requirements will allow you to select the best solutions.

Your application needs, ideally, will differ in their RTO and RPOs. In order to achieve a successful DR solution, you will need to organize them into tiers. Your environment will not be a one-size-fits-all, so define your needs to map each application to their specific risk tolerance and to choose what technology would best

fit them. You can prioritize your applications and VMs within each specific tier to note which receives attention first. Here's an example of one way to sort your applications into a tiered structure:

Tier 1 applications require instantaneous RTO and RPO. This tier is for your most critical applications that require the fastest uptime. The best recovery solution for this tier will be Active/Active or Active/Passive.

Tier 2 applications are business-critical, but can withstand downtime of a couple minutes or hours.

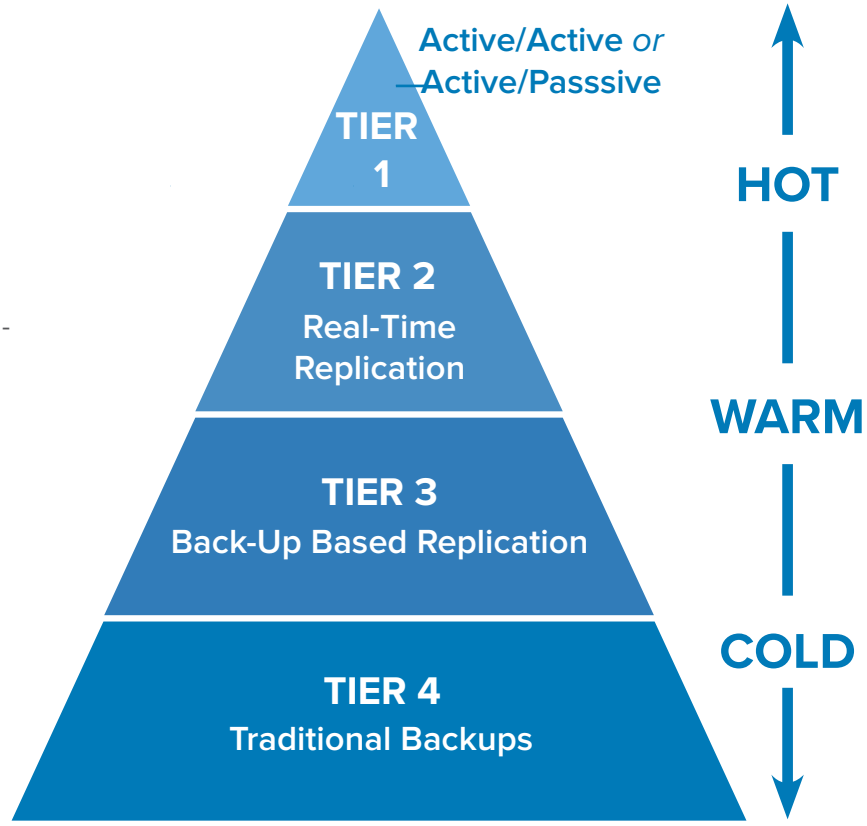
Tier 3 applications may require 24-hour RPOs and 24-48 hour RTOs.

Tier 4 applications would be the minimum required for recovery, likely 24-hour or longer RPOs and 48-hour or longer RTOs, depending on the scenario.

How you tier your applications is solely up to you, but seek insight from your DRaaS provider.

Depending on the nature and importance of your applications, you may need various or paired options. Having conversations with your stakeholders and your DRaaS provider will determine which works best for your applications.

Ideally, a DRaaS provider should solve the needs of all tiers, streamlining your solutions to a single point of contact – saving both time and money.



#5 Determine your recovery destination

To pick a recovery destination that best suits your business, determine different types of disasters that could occur to each application. Discuss what effect each type of disaster would have on each application.

Guarding against multiple types of disasters emphasizes the importance of an offsite location for your DR solution. Consider how far your production environment should be from your recovery site. Your recovery site will also be dependent on the type of technology you decide to use. Perhaps your company is large enough to have private datacenters in multiple locations and enough headcount to manage the replication, monitoring and testing in-house. If that's the case, consider using DRaaS replication to your secondary site(s).

If multi-site recovery isn't an option, choose a DRaaS provider with datacenters in varied regional locations. This will allow you to failover to another location in a time of crisis, ensuring your vital business data will be secure. DRaaS providers work cooperatively with your workforce in the event of a disaster, and can even carry out your recovery plan if your IT team isn't available.

TYPES OF DISASTERS

Application Disasters – Exclusively impacts the application(s). Consider DRaaS solutions that can handle partial datacenter failovers.

Infrastructure Disasters – Impacts the infrastructure the application is hosted on and potentially the application.

Datacenter Disasters – Impacts the entire datacenter, infrastructure within the datacenter and likely the applications hosted within the datacenter.

Metro Disasters – Impacts an entire metro area. As a result, it impacts more than just your datacenter but your infrastructure and application too. This may affect your workforce, since it could include acts of nature like tornados.

Regional Disasters – Wide-spread disaster impacting an entire region and therefore multiple metropolitan areas. This could include hurricanes and floods and may also affect your workforce.

#6 Assess security needs to protect sensitive data

If your business handles sensitive data like social security numbers, patient records, credit card information or legal depositions, consider DRaaS providers with secure technical capabilities and processes. With the ability to maintain accessibility, integrity and confidentiality of data, DRaaS can help you meet the strict standards of compliance for many industries and protect against cybersecurity breaches. To be sure you receive proper security measures, choose a DRaaS provider that specializes in security. Look for someone that will first understand your specific needs in order to properly protect your environments.

Before you can choose the right level of security, it's important to assess the current state of your applications and determine if there are any improvements needed. Picking a robust solution can be daunting, so look for a DRaaS provider that offers a **recovery assurance program**. This should include solutions with mature delivery models, which ensure your environment is secure, tailored and supported. An ideal DRaaS provider should offer role-based access, identity management, data eradication, and support for your compliance standards, whether it's SOC 2, DoD 5220.22-M, NIST 800-88, ITAR, FISMA, HIPAA or PCI.

With role-based access, public, private and hybrid cloud capabilities allow you to add and adjust permissions within your organization, setting tiers of access based upon job functions. An ideal DRaaS provider will have an easy-to-use online portal to adjust these settings, with secure access points for identification. Your provider should offer encryption and security services for both recovery operations and failover.

#7 Create a DR Playbook

Most DRaaS providers offer a simple disaster recovery runbook that describes the order in which your systems should recover. A playbook goes beyond the standard DR runbook to create a comprehensive outline of the critical components of your DR and business continuity practices. It looks at the whole recovery process so your team can work together in the event of a disaster.

The playbook should outline all DR procedures, runbook elements, recovery objectives, key contacts with roles and authorizations, system and network configurations and detailed failover and failback instructions. During the onboarding and implementation process for your DRaaS provider, the initial draft of the playbook should be created. After the first successful recovery test and during all subsequent tests, the playbook should be updated so it is accurate.

Organize the playbook by each tier of recovery. This ensures that if all systems go down, the most important assets are the ones that receive the first attention. Prepare two versions: a partial and full datacenter declaration process. Be sure to identify a point of contact for each data recovery step. When everyone knows who owns each responsibility, your team and your DRaaS provider will be better equipped to recover quickly.

A documented DR Playbook and QA checklist can provide assurance that your DR solution will live up to the promises you've made to the business and to your leadership. Validate the effectiveness of your DR Playbook based on the results of your DR test. When investing in DR planning and technology, you are responsible for ensuring it works properly. Your DRaaS provider should be equally invested in your success and should provide added confidence that everything is in order by working through the plans and testing with you.

#8 Test, test and then test again

A common misconception is that you test once, then you're done. Your environment evolves over time in ways you can't always predict. You should comprehensively test at least twice a year, if not more. Testing is not just about making sure a proper failover will happen, but about identifying and compensating for changes since your last test.

It's important to test against your playbook and make iterations. If you have a disaster with an outdated playbook, you could risk a failed recovery. Be sure to note any changes you make after testing and adjust your playbook accordingly. Even a test with errors is a successful test, because you've learned what would've happened in a real event. The value of your solution is equal only to your confidence in recovery. Working with the right DRaaS provider means not having to worry about an absent IT staff, too.

However, it's easy to focus on the failover and forget one of the most important parts of the entire process: the failback. For this reason, failback should be tested too. You don't want to end up having recovered from one disruption only to realize you can't failback properly. In failover, you're often moving to a clean environment that was previously unused. In failback, you're returning to an environment that could have been impacted by your disruption. Many DR products simply don't have a failback option and the process may be more disruptive than the initial incident.

A DRaaS provider will help with all of these tests and help you test often. With a support staff that acts as an extension of your IT team, it often entails little work on your end. You can schedule testing with the click of a few buttons - another reason why DRaaS is more affordable and easier to execute than legacy technology.

CONCLUSION

Now that your checklist is in place, get started! **Confidence in continuity begins with a plan that works.**

An ideal mix of RPO and RTOs tailored to your needs costs a fraction of traditional solutions. With cloud, if a disaster strikes or if your company experiences rapid growth, you have the resources to expand instantly. The price point is compelling because it beats legacy prices with physical equipment.

DRaaS gives clients the peace of mind that previously wasn't available. Users can see their replications working in a portal and click to test their solutions at any time. If anything should go awry, the DRaaS provider should have a proactive support team to help with failover and failback.

If you would like help assessing your risk or establishing your DR plan from an expert DRaaS provider, Bluelock is ready to help. Our seasoned professionals can help you recover your applications regardless of what strikes.

WHY DRaaS FROM BLUELOCK?

- ☐ **Support for each recovery tier (1-4)**
- ☐ **Partial and full failover support and expert help with failback**
- ☐ **Physical and virtual machine support for hybrid environments**
- ☐ **Secure environments and solutions to support compliance standards**
- ☐ **Only provider with Recovery Assurance: proven process for onboarding, training, testing and DR Playbook**
- ☐ **Easy-to-use management portal with high-level and drill-down visibility into your recovery solutions**
- ☐ **Comprehensive testing and validation of DR Playbook twice a year, plus unlimited basic testing**
- ☐ **24/7/365 proactive support team**
- ☐ **World-class datacenters in varied regional locations**

For more information on Bluelock DRaaS, or to speak with an expert, visit www.bluelock.com or call 888.402.2583.