CIO Guide:

Disaster recovery solutions that work

Making it happen with Azure in the public cloud

cbts

Consult Build Transform Support

When you're considering a shift to Disaster Recovery as a service (DRaaS), you have to figure out whose cloud services mesh best with your business.

Getting it right can be a riddle when the biggest names in technology—Amazon, Google, IBM, and Microsoft—offer robust cloud capabilities. A lot of companies simplify things by staying in the same software family. Thus, many Microsoft power users are adopting Azure cloud services.

Azure does a lot of things well, but it's especially well-suited to these kinds of DRaaS scenarios:

- **Region and compliance.** Microsoft data centers around the world can help comply with requirements for data storage within specific nations or geographic regions.
- **Legacy backup systems.** Many companies want to evolve beyond tape drives and optical disks and develop a robust disaster recovery program.
- **Specific Business Case needs.** Small to midsize organizations with tight budgets and comparatively simple disaster recovery requirements are a good fit for Azure.

Azure also taps the innate value of the cloud, switching from a capital-expenditure model to an operational-expense model. You pay only for the resources you use, expanding your computing power without having to invest in data centers.

Furthermore, data is replicated to Azure via an encrypted tunnel to keep snoopers at bay. Your managed disaster recovery vendor handles everything: planning, deploying, and restoring according to your recovery-time and recovery-point objectives—freeing your IT people to focus on strategic business initiatives.

It's one thing to appreciate the value of combining Azure with DRaaS. It's quite another to make it happen.

This eBook will summarize the fundamentals of DRaaS, outline a checklist for implementing Azure, and explain the advantages of working with CBTS for DRaaS/Azure.

Part 1: Disaster Recovery overview

The evolution of cloud technologies and virtualization software lets companies of all sizes develop business-continuity programs rivaling those of their largest competitors.

Years ago, organizations had to build duplicate data centers that sat idle most of the time. They wasted immense volumes of money, electricity, and company resources, but it was the only option out there—if they could afford it.

Smaller companies with fewer resources often relied on tape backups, hoping for the best while fearing the worst. Savvy entrepreneurs noted that cloud technologies could solve this challenge, so they started offering managed disaster recovery solutions that are delivered "as a service", hence DRaaS.

With a managed disaster recovery program you hand over all your recovery duties to a third-party provider who helps you:

- Assess your current IT environment and prioritize your recovery needs.
- Develop a tiered recovery architecture that best suits your precise business challenges.
- Test and document your backup-and-recovery model thoroughly to make sure it works in a crisis.
- Manage and monitor the process around the clock and act quickly to identify outages to get your systems back online as soon as possible.

Let's explore these Disaster Recovery protection options in more depth:

Assessments. Disaster Recovery protection requires a strategic approach to solving your disaster recovery challenges. That starts with assessing your entire IT environment, including your people, technologies, and business challenges.

Two key metrics to develop at the assessment stage are recovery time objectives (RTOs) and recovery point objectives (RPOs).

- RTO establishes how much system downtime your business can withstand before suffering serious damage to revenue, reputation, and operational efficiency. A high-volume eCommerce operation, for instance, would have a much shorter RTO than a B2B manufacturer that counts orders in hundreds vs. millions.
- RPO determines how far back in time your recovery should go: minutes, hours, days, weeks, etc. The further back you go, the longer it takes to recover—and the bigger the recovery will be. Thus, you can meet a two-day RPO much sooner and with less disk space than a two-month RPO.

Disaster Recovery assessments also identify all of your hardware, applications, and dependencies, and estimate how long it should take to recover them in an emergency.

Design. Knowledge gained during the DR assessment forms the foundation of the disaster recovery system architecture.

Disaster recovery design has to get two things right: Replicating your environment at a remote site and responding quickly to an incident. A holistic approach is required to account for all of your hardware, software, resources, and business demands—and to align them with your RTOs and RPOs.

There's no substitute for sound recovery-system design. Poor design infects everything that follows, forcing delays and tacking on costs at every stage.

Testing and documentation. Design cannot anticipate every problem that might crop up in the disaster recovery process. The only way to find the flaws is to take systems down, spin them back up and document the entire process and tweak along the way.

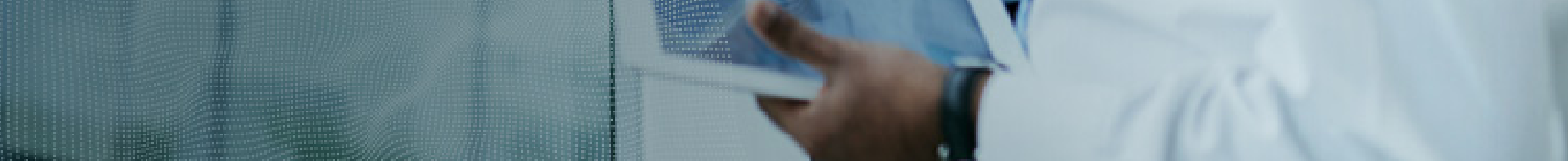
Testing can be a tricky process because you can't afford to let tests interfere with your business operations. Furthermore, you need to make sure your IT people know when tests are happening, so they don't try to "fix" testing-driven problems. Strong testing has three components:

- **Culture.** Everybody understands that testing is mandatory.
- **Buy-in.** Stakeholders support your testing initiatives.
- **Compliance.** Tests always follow the rules for privacy protection and data governance.

Management and recovery. The heart of DR is managing data replication full-time and recovering systems in accordance with your RTOs, design, testing, and documentation.

The best DR providers nail the strategy and the implementation. They ensure their clients have a mix of highly trained specialists to solve tricky challenges and real-time support personnel to monitor systems and do the right thing when downtime erupts.

Next up, we'll cover the nuts and bolts of implementing DR on Azure.



Part 2: Azure implementation checklist

Implementing Azure requires all the processes outlined in Part 1. The disaster recovery infrastructure consists of the technologies for virtualization, management, and replication on the original site. The recovery site should have a cross-platform design that enables automatic failover and bi-directional migration to and from the Azure environment.

Here's a handy checklist for implementing DR on Azure:

- Assess
  - Compile a list of all virtual machines in your IT environment.
  - List relevant applications and their VM relations.
  - Perform walk-throughs of the most common disaster recovery plan scenarios.
  - Collect and analyze performance data.
- Design and implement
  - Build a logical and physical design.
  - Establish disaster recovery procedures and review with stakeholders.
  - Set up DR components including replication software on each site.
- Validate and document
  - Perform an initial sync of the primary and secondary environments.
  - Conduct initial tests to flag exceptions and validate procedures.
  - Define recovery and test/live procedures.
  - Create run-book documentation.

- Manage and monitor
  - Supervise and oversee all disaster recovery infrastructure.
  - Adapt operational changes as they arrive.
  - Alert proper personnel to issues that arise during monitoring.
  - Resolve problems in accord with overall DR strategy.
- Improve
  - Disaster recovery software provides alerts to issues. Use these notifications to tweak services and boost performance.
  - Conduct a full test and validate documentation at least once a year.

Remember: Your Azure implementation cannot be static—it must adapt to your ever-changing IT environment. Conversely, upgrading and expanding your IT environment should conform to your DR program.

Part 3: The CBTS advantage for DRaaS and Azure

Designing, testing, and implementing a DR solution is a tricky business. Each organization has unique marketplace demands that produce wildly diverging IT infrastructures. Thus, the system built for a regional restaurant chain might not look like the one crafted for a Silicon Valley startup.

At CBTS, we have decades of experience building, configuring, and managing change data centers to data protection solutions for enterprises in every industry. That knowledge helps us master the complexities of developing and implementing robust disaster recovery systems that align with companies' marketplace demands. Our broad experience with Microsoft technology in the enterprise extends to mastery of the Azure cloud platform.

About CBTS

CBTS is a wholly owned subsidiary of Cincinnati Bell (NYSE:CBB) that serves enterprise and midmarket clients in all industries across the United States and Canada. From Unified Communications to Cloud Services and beyond, CBTS combines deep technical expertise with a full suite of flexible technology solutions that drive business outcomes, improve operational efficiency, mitigate risk, and reduce costs for its clients.

Contact us today at 1.866.587.2287 | cbts.com