datalink
An Insight company

White Paper

Cloud Disaster Recovery: Public, Private or Hybrid Cloud Solutions Supporting Disaster Recovery

Table of Contents

Introduction 2

Business continuity and disaster recovery development flow 3

Those unprepared for a disaster 3

Disaster recovery in the cloud is a two-part equation 4

Part one: the best practice approach to disaster recover 4

Part two: choosing a cloud solution 5

- Cloud options to consider 5
- Moving the technology stack to the cloud 6

Validation comes with testing 6

Disaster Recovery Preparedness Council, June 2016 6

Cloud disaster recovery assessment 7

Assessment time requirements 8

Additional disaster recovery services 8

Ready, set, go 9

Conclusion 9

Why Datalink 10

References 10

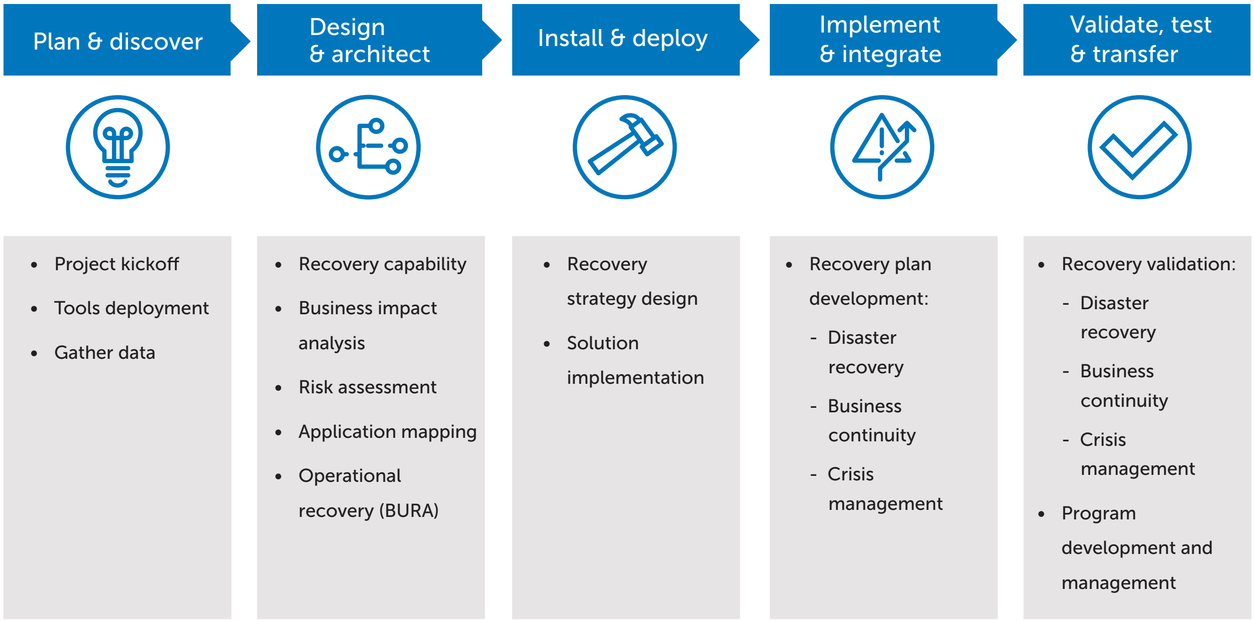
Introduction

In years past, mentioning disaster recovery to executives immediately created angst. Everyone envisioned enormous sums of money being spent on technological safeguards with no quantifiable return on investment. Often it was referred to as “expensive insurance that will never be needed” or a “money pit,” consuming budgets that would be better spent elsewhere. Today, however, we all see the news, along with vivid pictures of damage caused by hurricanes, tornados, tsunamis, earthquakes, floods, fires, terrorism and violence of all types occurring around the world. These kinds of disasters are the most easily understood. Unfortunately, disasters occur in other ways that are much less obvious, such as employee sabotage, data corruption, hacking and data theft. Whether natural or manmade, disasters happen, and unfortunately we don’t know when or where they will strike.

Executives know that having disaster recovery solutions in place makes good business sense. But traditional costs to own the necessary hardware and software, and to employ the staff to support the chosen solutions, continue to impede efforts. Today, cloud offers a myriad of options capable of addressing the needs of businesses regardless of their size, type, or complexity. Public cloud provides robust, scalable, convenient, and cost-effective solutions, enabling more businesses to move forward with their disaster recovery initiatives. Public cloud is most often managed by a third party, which yields the benefit of lower staffing needs. As with any solution a company considers, they must understand what is appropriate for the organization, both in terms of meeting business objectives and regulatory requirements.

Business continuity and disaster recovery development flow

Cloud disaster recovery is only one part of a greater equation. Below is a model depicting the evolution of work for cloud and traditional business continuity and disaster recovery.



Plan & discover

- Project kickoff
- Tools deployment
- Gather data

Design & architect

- Recovery capability
- Business impact analysis
- Risk assessment
- Application mapping
- Operational recovery (BURA)

Install & deploy

- Recovery strategy design
- Solution implementation

Implement & integrate

- Recovery plan development:
  - Disaster recovery
  - Business continuity
  - Crisis management

Validate, test & transfer

- Recovery validation:
  - Disaster recovery
  - Business continuity
  - Crisis management
- Program development and management

Those unprepared for a disaster

Businesses caught unprepared for a disaster suffer losses in many different ways, including damaged reputations, loss of customers, fines/penalties, and revenue impacts because they believe it wasn't necessary to be proactive. Disasters do not have to be large to be costly. Simple data breaches, losses, or corruption events can be very expensive.

Data breaches hit organizations squarely in the wallet. The average cost per record goes up depending on who or what caused the exposure.[1]

- **Human error:** Breach caused by human error or negligence costs an average of $137 per record or $3.85 million per event.
- **System glitch:** A system glitch exposing records costs an average of $142 per record or $3.99 million per event.
- **Hackers and insiders:** When hackers break in or insiders leak data out, the cost per record is $170 or $4.77 million per event.

> "The likelihood of an outage from weather is only 14%. The two major causes of data loss are technology failure and human error. The question isn't whether or not disaster will happen; it's when."[2]

Disaster recovery in the cloud is a two-part equation

When a company considers building a disaster recovery program utilizing the cloud, there are two parts to consider.

1. **Building the program:** At this point nothing changes. The process and methodology to build an effective disaster recovery program is the same.
2. **Choosing a cloud solution:** Ensure your solution best fits the technologies used by the organization and the requirements of the business to recover.

Part one: the best practice approach to disaster recovery

According to the Disaster Recovery Institute International (DRII), there are 10 Professional Practices that comprise the Body of Knowledge used to develop and implement a program. "Use of the Body of Knowledge and Professional Practices can increase the likelihood so that no significant gaps will be present in your program, as well as increase the likelihood that the various parts of the program will work cohesively in an actual event."[3]

It should be noted that these 10 Professional Practices (below) are exactly the same in every business continuity and disaster recovery program and do not change if a cloud solution is used. Cloud is simply another site with technology solutions implemented to support disaster recovery.

1. Program initiation and management
2. Risk evaluation and control
3. Business Impact Analysis (BIA)
4. Business continuity and disaster recovery strategies
5. Emergency response and operations
6. Plan implementation and documentation
7. Awareness and training programs
8. Business continuity and disaster recovery plan exercise, audit and maintenance
9. Crisis communications
10. Coordination with external agencies

After initially building out a program, it is vital to keep it maintained. Continuous improvement efforts must be included in a company's daily routine. This includes performing processes and activities to ensure plans and documentation are updated. Development of policies, standards, and guidelines is crucial for success. These must be written to address specific regulations that impact the business.

Finally, implementing an internal audit program to verify compliance to the newly established policies, standards and guidelines is required. This ensures the program is ready at all times in the case that an event occurs. Some of the areas that an internal audit will review include:

- ✓ Developed strategies are updated as technologies are implemented, changed or removed.
- ✓ Change management is routinely used to ensure consistent methodologies are applied; solutions are tested and documented before introduction into the production environment.
- ✓ Change management will include sign-off by the business continuity/disaster recovery program.
- ✓ Documentation is routinely reviewed and maintained to relevant regulatory guidelines.
- ✓ Business continuity and disaster recovery program consistently uses a quality improvement methodology, ensuring the program accurately reflects the current state, remaining relevant and ready for use.

Part two: choosing a cloud solution

When choosing a cloud solution, organizations must address the technologies being used and the requirements defined by the business to recover. This will require an assessment of the features and capabilities of each type and their related costs. At this point, it is necessary to identify the "best fit" solution for disaster recovery and a cloud solution that may include public, private or hybrid cloud components.

Cloud options to consider

Gartner Inc. defines "cloud" as follows:

Public Cloud:[4] Public cloud computing is a style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies—i.e., public cloud computing uses cloud computing technologies to support customers that are external to the provider's organization. Using public cloud services generates the types of economies of scale and sharing of resources that can reduce costs and increase choices of technologies. From a government organization's perspective, using public cloud services implies that any organization (in any industry sector and jurisdiction) can use the same services (e.g., infrastructure, platform or software), without guarantees about where data would be located and stored.

Private Cloud:[5] Private cloud computing is a form of cloud computing that is used by only one organization, or that ensures that an organization is completely isolated from others.

Hybrid Cloud:[6] Hybrid cloud computing refers to policy-based and coordinated service provisioning, use and management across a mixture of public and private cloud services.

From a more general disaster recovery and business continuity perspective, a hybrid solution may include public and private cloud offerings combined with physical infrastructure addressing strategies not cloud capable (architecting the "best fit" disaster recovery solution).

Cloud is simply scalable data storage, computing resources and application hosting available via the Internet. Depending on the vendor a company may have additional tools and services available to you. The choice is driven by its business needs, cost, and support requirements.

Moving the technology stack to the cloud

Will not change:

- The commitment and ongoing support required by executive management
- 10 Professional Practices used to develop, document, and maintain a company's program
- Tangible and verified data collected through the various assessments, evaluations, interviews, and data gathering efforts

Will change:

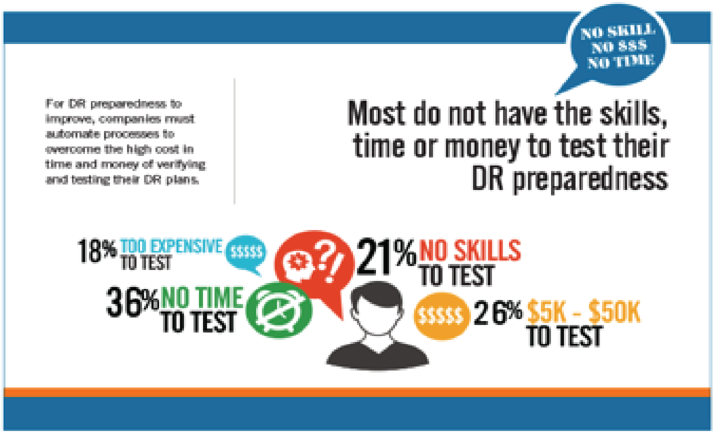
- Efforts required to manage the environment
- Resource types needed, as public cloud utilizes shared resources managed by a third party changing the level of control experienced
- How organizations think about and design security. Public cloud shares resources and often moves data from region to region (possibly country to country raising concerns about data sovereignty) without notifying stakeholders. It will be necessary to determine if this is acceptable in its environment of legal, contractual, and regulatory requirements.
- Types and strengths in negotiated Service Level Agreements (SLAs) and underpinning contracts
- The manner in which costs are expensed; capital expenses will now become operational expenses.

Validation comes with testing

Even companies that have invested in developing a disaster recovery program fall short when it comes to testing and validation of their strategy. Cloud disaster recovery can help address this problem. Cloud can provide a secure testing environment, is scalable, and may have automation tools or contracted third-party resources available to reduce the need for specialized skills. Cloud disaster recovery significantly reduces cost over traditional disaster recovery with physical hardware in a dedicated location.

In most organizations, testing can only be done on a limited level – perhaps quarterly and most often annually. Issues around cost, staffing, environment control and the impacts to business operations all impede testing efforts. This can be compounded by the use of multiple sites, time zones and other barriers. Many times, companies even forget that true testing requires end-user participation, and bandwidth on the network is under-sized or constrained by other activities.

The elasticity of cloud can address these concerns and greatly improve testing and validation efforts. It is now easier than ever to conduct frequent test cycles of any size or complexity without the negative impacts previously encountered. Organizations can size their cloud environment to meet the need, and when they are done, reset it in preparation for the next test. Public cloud makes this very cost-effective since companies pay for what they use and only when they use it.



Disaster Recovery Preparedness Council, June 2016

Cloud disaster recovery assessment

> "For 2016, cloud will become the first option when building new IT architecture. This means that companies will start by considering public cloud, then will move to private cloud, hosted systems, or on premise systems if needs dictate. Ultimately, the infrastructure will be a diverse mix, and monitoring/management will become a top challenge."[7]

> "The market for public cloud services is continuing to demonstrate high rates of growth across all markets and Gartner expects this to continue through 2017."[8]

To meet this growing challenge, identifying all of the business drivers and requirements is vital. It is absolutely critical that companies know and understand what they have in place today so it can be addressed by new cloud architecture. To reach this level of understanding, a cloud disaster recovery assessment will guide a company in its cloud analysis. A consistent methodology of requirements and data gathering, analysis, and strategy formulation take the mystery out of cloud. An informed organization can make the appropriate decisions needed to drive a successful cloud disaster recovery initiative. Regulatory requirements and strategic decisions aside, knowing what you need and must do, and how it must perform, is the starting point.

Some of the key elements in a cloud disaster recovery assessment include:

✓ Discovery

- Understand business disaster recovery goals and objectives
- Gather interview and workshop data to understand business disaster recovery issues and operational requirements

✓ Analysis

- Review documentation (infrastructure inventory, operations plans, diagrams, P&Ps, SLAs, cost information, existing disaster recovery plans)
- Review people (skill sets, job descriptions)
- Review processes (operations, infrastructure, governance and disaster recovery)
- Review tools (operations and disaster recovery – management, monitoring, charge-back, automation and orchestration)
- Review existing infrastructure architecture (storage, compute, network and security)
- Review existing application architecture
- Review cloud solution vendors to identify "best fit" options

✓ Strategy

- Develop a Disaster Recovery Infrastructure and Capabilities Assessment report
- Recommend cloud disaster recovery solutions with supporting detail
- Implement a cloud disaster recovery roadmap

Assessment time requirements

Using the cloud disaster recovery assessment methodology takes an investment of 4-6 weeks depending on the business size, type, drivers, availability of essential information and customer involvement. This assessment is typically conducted on-premises with access to key staff across all business units and infrastructure locations. A thorough review of documentation and other support materials is included. The assessment methodology is highly interactive in order to develop a realistic understanding of business needs. This will ensure IT decisions and investments are aligned to desired business outcomes.

Additional disaster recovery services

Disaster recovery solution providers offer a myriad of additional services aimed at helping companies move their program forward. They can address any need – from the initial assessment and building out the program to program documentation and validation of implemented solutions. Typically, their services address business continuity and cloud disaster recovery, as well as the more traditional models.

- ✓ Cloud automation and orchestration
- ✓ ITIL/ITSM
- ✓ Recovery capability assessment
- ✓ Application mapping
- ✓ Business Impact Analysis (BIA)
- ✓ Risk assessment (RA)
- ✓ Backup, recovery & archive assessment (BURA)
- ✓ IT Service Continuity strategy design
- ✓ IT Service Continuity Plan and Runbook development
- ✓ Capability validation using multiple methods such as Desk Check reviews, TableTop and failover exercises

The services of a solution provider are designed to augment your own business efforts. They build off of a company's work and results when any services are added to an engagement. This helps in managing scope and cost when budgets are tight.

Ready, set, go

Companies must ask themselves, “Are we ready to invest in disaster recovery? Have we considered cloud to optimize our strategies while reducing our financial spend?” Most companies admit that “we don’t know what we don’t know.” Getting started may seem like a daunting task to undertake, but help is available.

A cloud disaster recovery assessment helps a company define what is needed, how cloud can fit into your disaster recovery program, determine what cloud options will be the “best fit” for an organization and more. Companies can benefit from and take advantage of public, private or hybrid cloud. A cloud disaster recovery assessment is a detailed look at an organization’s existing infrastructure and program, helping them answer questions that will guide them toward a working, reliable and efficient cloud solution.

Conclusion

Disaster recovery utilizing the cloud has many benefits that will help today’s businesses reach a level of preparedness they may not have previously experienced. Cloud also has pitfalls that need to be considered when deciding which type to use. Companies that understand what cloud offers and what they need to do to prepare are well-positioned to realize the benefits.

Costs to implement and maintain a disaster recovery environment will certainly be lower using a public cloud solution. Cloud can improve a company’s ability to test individual solutions as they are implemented or validate an entire strategy before it is called upon. To decide what type of cloud is right based on operational needs and budget, a company should complete a full assessment. Ideally, a company should have a disaster recovery solution provider ready to analyze all relevant information and work with them to guide decision-making.

A customized disaster recovery solution is critical to a company’s ability to protect its data, assets, people, and customers. With advances in cloud-based disaster recovery technology, the cloud is proving to be an increasingly attractive option.

Datalink's Cloud Disaster Recovery Assessment is a detailed look at an organization's existing infrastructure and program, helping them answer questions that will guide them toward a working, reliable and efficient cloud solution.

Why Datalink?

Datalink's highly skilled and experienced professionals provide vendor-agnostic services to support IT transformation efforts. We ensure that your initiatives are relevant and successful in today's environment of growing customer expectations and decreased IT spending.

Our team has deep experience in:

- ✓ Helping customers make cloud disaster recovery decisions
- ✓ Implementing cloud disaster recovery automation tools
- ✓ Developing automated end-user self-service portals
- ✓ Transferring our skills to your team
- ✓ Comprehensive services from cloud, business continuity and cloud disaster recovery strategies to robust technology solution architecting, managed services and cloud disaster recovery program development

References

1: Ponemon Institute, 2015 Cost of Data Breach Study, December 14, 2015

2: Disaster Recovery Preparedness Council, 2014 Annual Report

3: Disaster Recovery Institute International, drii.org, Professional Practices, June 30, 2016

4, 5, 6: Gartner IT Glossary, Gartner.com, June 2016

7: Seth Robinson, Sr. Director, Technology Analysis, CompTIA, December 21, 2015

8: Gartner Inc. press release, January 25, 2016

datalink

An Insight company

datalink.com | insight.com

CDR-WP-2.0.03.17