Leveraging disaster recovery in the cloud as a cloud migration path: A case study

Cary Jasgur

Received (in revised form): 10th May, 2019

Mazars USA LLP, 47 East South Street, Suite 201, Frederick, MD 21701, USA
Tel: +1 202 258 6666; E-mail: cary.jasgur@mazarsusa.com

Cary Jasgur

Cary Jasgur *is a consulting manager with the Mazars USA organisational resiliency practice. He has over 25 years of experience in organisational resilience, business continuity, disaster recovery, emergency management, crisis management, incident management, certification and accreditation, risk management and mitigation, continuity of operations and information systems security. Cary is well versed in the NIST Special Publications relating to various information systems, and has managed disaster events both within the USA and globally. He holds a bachelor of science degree in technical management and master of science degrees in project management and organisational leadership. He is also a Certified Business Continuity Professional, Member of the Business Continuity Institute, and Project Management Professional.*

Abstract

Over the years, the 'cloud' has gained increasing traction in assisting organisations to become more resilient. Building on such successes as migrating office applications using Office 365, organisations are now looking to move disaster recovery to the cloud as a viable solution to protect critical applications at the time of disaster. This paper explores one organisation's journey through the maze that is disaster recovery cloud deployment. Using a case study format, it will explore the organisation's previous experience with cloud applications, the challenges it faced, the solutions put in place to address those challenges, the results of the deployment, the risks, and finally the benefits of the solution going forward. Finally, the paper will walk the reader through the ten steps that an organisation should take to move its own disaster recovery environment to the cloud.

Keywords: disaster recovery in the cloud, cloud migration, disaster recovery, organisational resilience, business continuity

Journal of Business Continuity & Emergency Planning
Vol. 13, No. 2, pp. 150–159

1749–9216

INTRODUCTION

In today's ever-changing business world, organisational resilience has become increasingly important. It allows leaders to take measured risks with confidence, responding quickly and appropriately to both opportunity and threat. Gone are the days where mere backup and recovery are enough to protect an organisation from business disruptions. The potential impacts to an organisation are even greater, with social media always looking to expose the underbellies of organisations that are not prepared to address business disruption. To keep their collective heads above water, organisations must look beyond the status quo. To stand out and win, every organisation, regardless of its size, sector or location, must develop a resilient approach

that is right for it — underpinned by its values and defining its brand.

A major aspect of a successful organisational resilience programme is disaster recovery. Disaster recovery can mean something different from one organisation to the next — indeed, even the industry's two leading authorities cannot agree on exactly what it constitutes.

The Business Continuity Institute (BCI) defines disaster recovery as 'The strategies and plans for recovering and restoring the organisations technological infrastructure and capabilities after a serious interruption'.[1] Meanwhile, the *Disaster Recovery Journal* defines disaster recovery as 'The process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure, systems, and applications which are vital to an organisation after a disaster or outage'.[2] Where they can agree, however, is on what disaster recovery covers:

> 'Disaster recovery focuses on the information or technology systems that support business functions, as opposed to business continuity which involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery is a subset of business continuity. Disaster recovery is now normally only used in reference to an organisation's information technology and telecommunications recovery.'[3]

Making the decision to move an organisation's production environment, or a part of it, to the cloud is not an easy one to make. There are several factors that technology leaders must first consider when determining whether the cloud is the proper location for their disaster recovery solution. Only once all the due diligence has been conducted and technology leaders have decided the best applications and services to place in the cloud can migration begin. Even then, migration can take many forms. This case study will explore one organisation's path to leveraging the cloud for its disaster recovery solution.

THE ORGANISATION

The subject of this case study is a global biotechnology organisation focused on the development and commercialisation of innovative products to address the unmet medical needs of patients with chronic and life-threatening conditions. Its strategic objectives are to:

- Develop the best medicines possible from its intellectual property;
- Conduct the most insightful clinical trials of its medicines;
- Achieve superior communication and awareness of its products among physicians;
- Grow its business to be in the top quintile of its peers; and
- Achieve its goals by doing the right thing and using the highest ethical standards.

Early experience with cloud applications

Like many organisations today, the organisation had already migrated all its communications and collaboration applications and services to the cloud using Microsoft's Office 365 subscription service, which includes access to such software as Outlook, SharePoint Online, Skype for Business, Teams, and office automation software such as Excel, PowerPoint and Word.

The challenges

The organisation was supplying information technology services to multiple locations on a global scale. However, its rapid growth was making it hard to maintain

the deployment of emerging technologies. Around the world, its various data centres, server rooms and equipment closets all needed extra staffing. The organisation needed a strategic initiative to improve and transform information technology operations today as well as into the future — all while finding a cost-effective means to improve organisational resilience across the enterprise.

The solutions

To understand what the organisation had in place, a thorough assessment of its current state was conducted from both a governance and a technological standpoint. It was important to integrate with the business to identify and prioritise critical business applications and services. To understand the organisation's needs with respect to critical business applications and services, the business continuity coordinator and disaster recovery team conducted an enterprise-wide business impact analysis (BIA). This gave the resiliency team an idea of when the business needed applications and services to be back online, thus creating the baseline for a disaster recovery solution.

The base requirement of the disaster recovery technical solution is that it must integrate into the organisation's information technology environment and include technologies to continuously replicate application data within recovery point objectives and restore critical business applications and services to normal operations within established recovery time objectives.

During the strategy project, themes surfaced that would influence product selection and shape the conceptual design. The following themes helped determine the future disaster recovery solution:

- The recommended disaster recovery alternate site and technologies must align and integrate easily into the organisation's information technology environment;
- The organisation's long-term information technology strategy is to host business applications and services in the cloud;
- The goal is to reduce the data centre footprint and focus information technology resources on building capabilities through hosted solutions, customer service, service integration and the transition of information technology expenditures to a predictable model;
- The disaster recovery solution should not increase site management responsibilities with respect to security and compliance;
- The disaster recovery solution must leverage the agility of virtualisation to improve application resiliency;
- The disaster recovery solution must not over-burden information technology resources;
- Overall total cost of ownership must be cost-effective;
- The disaster recovery solution positions the organisation to further exploit cloud services and provides a simple path to transition production workloads to the cloud.

An assessment and evaluation of several disaster recovery technologies was conducted to determine the proper solution combination to address the organisation's recovery requirements. Figure 1 illustrates the considerations and products that went into determining the eventual solution.

Through rigorous due diligence of all the options, the organisation selected one that not only met the current needs for disaster recovery but also provided room for expansion. The development of a detailed strategic plan and implementation roadmap ensured the successful implementation of the chosen solution.

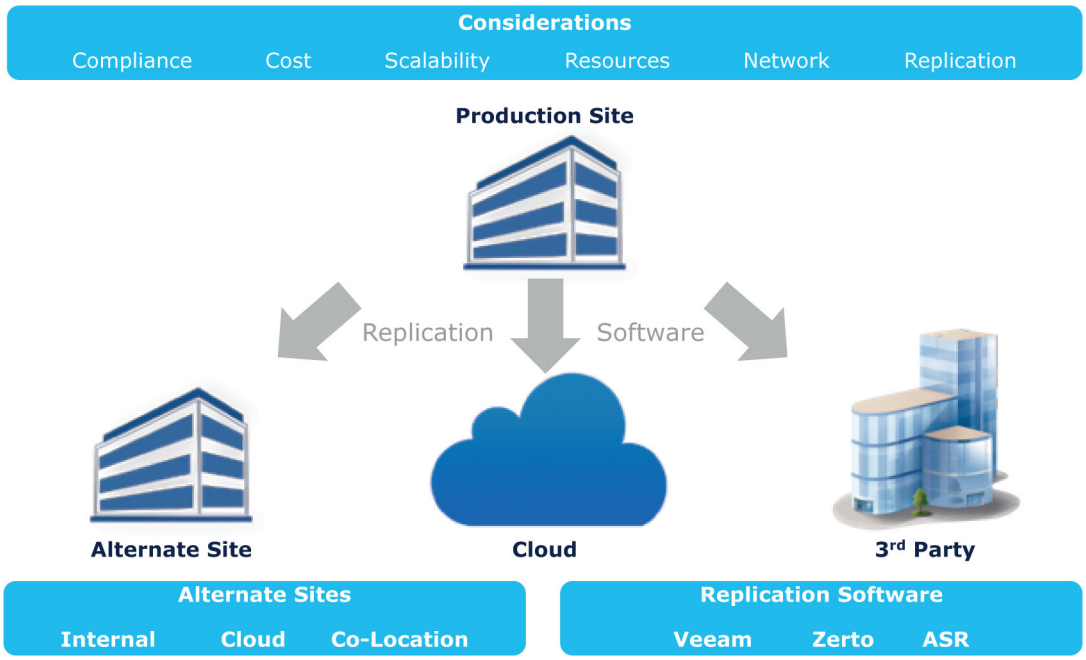

Figure 1 Cloud configuration considerations

By implementing disaster recovery in the cloud, the organisation now had an initial 'pilot' cloud infrastructure service in which to test the viability of running production applications and services in the cloud. Figure 2 provides a high-level visual representation of what the implementation looks like.

The results

The primary result of the engagement was the creation of a best practice enterprise-wide organisational resilience programme that would allow the organisation to protect its critical business applications and services in the event of a business disruption. The overarching results of the enterprise-wide BIA yielded some particularly useful information. Most importantly, the BIA identified the critical business processes, as well as the applications and services that supported those critical business processes. Also identified were the critical dependencies on which the critical business processes relied to recover or continue in the event of a business disruption. The outcome of the BIA allowed for the creation of simple, concise and actionable plans — not only for business continuity but for disaster recovery as well.

The deployment of the best-in-class cloud-based disaster recovery solution created a strategic initiative with a stable, sustainable and scalable operating model. In turn, this transformed the information technology operating model from legacy on-premises technologies into a new leading-edge information technology platform. The cloud-based disaster recovery solution allowed for an improvement in overall information technology efficiencies and a reduced cost, in addition to improved performance and scalability of the entire information technology environment. This allowed the information technology support teams to spend less time worrying about the status of legacy on-premises technologies, thus enabling

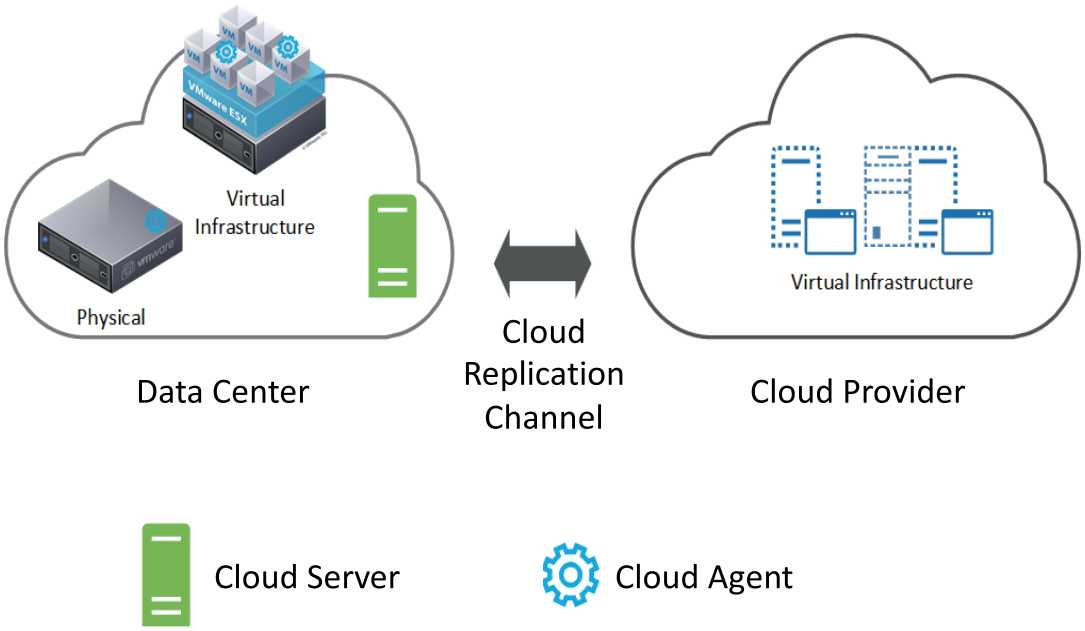

Figure 2 Cloud replication example

the business to enjoy improved information technology services and capabilities.

The risks

Risks are inherent in any information technology project. Migrating disaster recovery to the cloud is no different. The key to a successful disaster recovery cloud-based solution is to identify the risks as they present themselves and have a plan to mitigate those risks. In what follows, this article provides a roadmap for how to get to the cloud. Following these steps will help to manage the various risks that could have a major impact on a disaster recovery cloud migration project.

The benefits

The main benefit of a cloud-based disaster recovery solution is essentially the ability to push a button and transfer all production applications and services to the cloud ready for business users to continue their critical business processes. The configuration that this organisation chose allowed for a recovery time objective of just four hours with a recovery point objective of just 15 minutes. However, during the testing portion of the implementation phase, that time was just a matter of minutes — permitting almost seamless continuance of critical business processes, applications and services.

With the implementation of the cloud-based disaster recovery solution, the organisation has peace of mind that when a business disruption occurs, it will be prepared to execute its business continuity and disaster recovery plans to ensure that critical business processes can continue.

Once the cloud-based disaster recovery solution has been proven to be effective and operational through thorough testing, the chief information officer has an ace in the hole: the next time a business disruption occurs, the chief information officer and the supporting disaster recovery teams will execute the failover to the cloud … and never failback — effectively migrating the production environment to the cloud.

HOW TO GET TO THE CLOUD

The decision to migrate to the cloud may be an easy one to sell to senior leadership; however, the execution of cloud migration is not something to take lightly. Before migrating to the cloud, thorough research and a thoughtful approach are essential. If done right, moving to the cloud can benefit organisations in terms of speed, efficiency and cost. However, the process can be complicated.

The ten steps are described below.

Step 1: Determine why the organisation wants to move the current disaster recovery environment to the cloud

Asking why the organisation needs or wants to move disaster recovery to the cloud is by far the most crucial step in the entire migration process. Understanding whether the motivation is based on cost reduction, competition in the market, or simply improving on the security of the existing disaster recovery environment, will help to determine whether the organisation really needs to invest the time and resources in such a migration. Will moving to the cloud present any advantages or disadvantages to the organisation? This step will help everyone involved in the process, as well as senior leadership, to understand the risks and benefits of migrating the disaster recovery environment to the cloud.

Potential pitfalls

Of all the pitfalls associated with moving disaster recovery to the cloud, doing so for the wrong reason is the most common of all.

Step 2: Perform a detailed strengths, weaknesses, opportunities and threats analysis

Once the organisation has made the decision to move its disaster recovery environment to the cloud, performing a detailed analysis will help to determine whether migration is the correct decision. The analysis will show everyone involved in the project how migration will benefit the organisation; what risks or impacts there may be to information technology and business operations; where the organisation might reduce costs or improve functionality; and what potential harm could come from the migration. It is important to consider and outline costs in all the documented findings from the analysis. Within many organisations, cost is often the factor that decides whether a project gets the green light to start.

Potential pitfalls

It is important not to cut corners and sell yourself short; ensure that the analysis is thorough and covers the entire organisation from end to end.

Step 3: Perform an assessment of the current disaster recovery environment

Before the migration process begins, it is important to assess the existing information technology environment, the applications and services in use, the resources necessary to support those applications and services, the costs for recovering those applications and services, as well as any other pertinent details. This provides the basis for determining the next steps in the process.

When performing the evaluation, consider the following points:

- *Which applications can be or should be migrated to the cloud?* While there are many benefits to migrating disaster recovery to the cloud, it may not make sense for all organisations, business processes, applications or services. There may be operational or business reasons to keep certain applications or services in their current on-premises configuration — for example, a legacy application or service that cannot be protected by a

cloud-based disaster recovery solution, or a performance-intensive application or service where speed is more important than resiliency. In such circumstances, failure to identify all the requirements for each application and service being considered for migration would be doing the organisation a disservice.

- *Assess the current information technology environment (for costs and resources).* Having determined which applications and services are candidates for migration to the cloud, the next step is to analyse those applications and services for the following information points:
  - the infrastructure in use to support those applications and services — this would include the amount of compute, storage, data generated, networking and other dependencies;
  - the amount of capital spent on physical servers and the resources necessary to manage and support said servers;
  - any hidden costs, such as support agreements.

A thorough analysis of the infrastructure and costs will help to identify how to migrate the applications and services to the cloud and optimise them for better efficiency.

Potential pitfalls

Disaster recovery in the cloud does not have to be an all-or-nothing decision. Many organisations move only the most flexible components of their environment to the cloud, keeping the more sensitive or compute-hungry applications onsite.

Step 4: Select the correct cloud partner for the organisational model

For the absence of doubt, there is a clear difference between and cloud partner and a cloud provider. The former is an organisation, such as a consulting firm or professional services division that works alongside an organisation to ensure successful cloud migration. A cloud provider, meanwhile, is the organisation selected to host the disaster recovery solution. Several cloud providers offer professional services to aid in the migration process.

Any organisation that already has the technical knowledge to move disaster recovery to the cloud is ahead of the game. However, that does not mean it is ready to go it alone. Choosing the correct cloud partner for disaster recovery migration can make all the difference between a successful and fully-functional cloud migration and a résumé-generating event.

It is particularly important to choose the correct cloud partner to fit the organisation's needs. Consider reviewing the partner's past performance on projects like the one currently under consideration. There is often benefit in finding a partner with experience in projects of similar size and complexity, and within the same industry.

Potential pitfalls

Choosing the correct cloud provider is like asking for directions — you may well reach your destination without them, but they make the journey significantly smoother.

Step 5: Select the cloud environment that suits the organisation's needs

By this point, the disaster recovery cloud migration project is really starting to take shape. The next step in the process is to determine which cloud environment will aid the organisation in achieving its goals and subsequently meet its needs.

The first decision for the organisation is to determine which type of cloud is best suited to house the disaster recovery environment. Below, the article describes the three cloud environments available

today — the public cloud, private cloud and hybrid cloud — along with some of their pros and cons.

The *public cloud* is the most well-known and straightforward type of cloud environment. It offers convenience, access and scalability. Most notably, it is:

- Easy to use;
- Typically, a pay-per-use model, which makes it cost-effective;
- Operated by a third party; and
- Flexible.

However, the public cloud is not without its risks, as it can be unreliable and less secure.

The *private cloud*, meanwhile, is best suited to those organisations that are required (or simply desire) to know the exact location of their data, and need to exercise complete control over their data, including who has access to said data. The private cloud:

- Is organisation-specific;
- Customisable; and
- Offers more control and reliability.

On the down side, the private cloud is more costly and requires internal information technology expertise.

For those organisations that need a combination of both public and private cloud features, the *hybrid cloud* offers a mix-and-match approach to disaster recovery. The hybrid cloud is:

- Flexible and scalable; and
- Cost-effective.

Whichever environment the organisation chooses, it is essential to ensure that the due diligence has been completed and all the pros and cons have been assessed. The organisation's cloud partner can be instrumental in identifying the correct environment to meet organisational goals and needs.

Potential pitfalls

Do not progress without first weighing all of the possible options. Only in this way will the organisation find the right solution.

Step 6: Design what the disaster recovery technology should look like

With the knowledge gained in Step 3, determine the components the cloud-based disaster recovery solution will require to be functional today and into the future.

Some of the considerations during this step include how much storage will be needed, what kind computing power the applications and services require, and which tool(s) will be needed to move the data from production to the cloud-based disaster recovery solution.

Again, the cloud partner can lend knowledge and guidance to capture this information properly.

Potential pitfalls

Do not be short-sighted when designing a disaster recovery environment: plan for the future, not just what is needed today.

Step 7: Select the correct cloud provider for the organisational model

With so many cloud providers in the market today, determining which will best meet the organisation's needs and goals can be a daunting task. There is a mountain of information out there about cloud providers — some of it useful, some not so much. Sifting through this vast amount of information to ensure that the correct cloud provider is selected is a job for the organisation's cloud partner. For most organisations, cost is the driving factor in the selection process. In this regard, it is essential to compare what those costs provide. Ensure that the service-level agreement is

sufficient to meet organisational requirements. Consider customer service, as well as reputation within the marketplace.

Potential pitfalls

Review and consider what each cloud provider offers, paying special attention to where the data will reside.

Step 8: Plan the cloud migration

Having selected a cloud partner, determined which cloud environment is most suitable, finalised the technology design for the disaster recovery solution, and identified the cloud provider that best meets the organisation's goals and needs, it is now time to plan for the migration. As with any technology migration project, a great rule of thumb applies: plan twice, execute once.

The first applications and services to migrate will be the easiest, less critical ones. This will make it possible to get a feel for the migration process and to perform testing as other applications are moved over. If anything does not go as planned, this provides an opportunity to correct it before migrating the more critical applications and services.

Make sure that all information technology personnel are well versed in the operation of the new software and tools that make up your cloud-based disaster recovery solution. Migrating applications and services in waves is a useful way to train information technology personnel.

Potential pitfalls

Prioritise the execution: take time and get it right the first time.

Step 9: Execute the plan to migrate to the cloud

The big day is finally here. Assuming the earlier steps have all been completed successfully, the actual execution of the migration plan should be uneventful. However, there is always the possibility of something going a little sideways. Review the migration plan with all the involved parties one last time before beginning the migration process, so that everyone is aware of their roles and responsibilities during the migration, and more importantly, what to do if things do not go as planned.

Follow any procedures created to support the disaster recovery environment with the cloud provider. Ensure that proper testing has occurred to determine that the cloud-based disaster recovery solution is ready to receive applications and services from the production environment.

Follow the steps outlined in the application or service-level disaster recovery plans for how to properly migrate critical applications and services.

Finally, be sure to execute the test scripts and that the desired results with the applications and services running in the cloud have been obtained.

Potential pitfalls

Ensure the execution plan has an escape plan, in case something does not go right during deployment or testing. Be ready to take a step back and analyse what went wrong.

Step 10: Monitor the cloud environment

The last step in the process is the second most important. To ensure the cloud-based disaster recovery solution is ready and able to be utilised should a business disruption occur, be sure to conduct regular testing, monitor utilisation, keep track of storage used, and verify that performance meets organisational requirements.

Potential pitfalls

Disaster recovery in the cloud is a living breathing entity. If you take care of it, then it will take care of you when it is most needed.

CONCLUSION

There is no one way to implement a cloud-based disaster recovery solution. Similarly, not every organisation will be able to use their cloud-based disaster recovery solution as a pathway for migrating their production information technology environment to the cloud. However, with the information contained in this article, organisations can be better informed when making the decisions that will take their ability to deliver critical services to their clients and customers to the next level.

Finally, there is one, quite simple, instruction that is vital in any cloud migration project, whether it be for disaster recovery or the migration of the production information technology environment: be sure to assemble the right team to achieve the organisational goals and objectives. Only then will success be around the corner.

References

(1) Business Continuity Institute and *Disaster Recovery Journal* (2017) 'Glossary of Terms', available at: https://www.thebci.org/resource/bci---drj-glossary-of-terms.html (accessed 20th May, 2019).
(2) *Ibid*.
(3) *Ibid*.