aptum

EBOOK

# BUSINESS CONTINUITY PLANNING IN THE CLOUD

Plan for Continuity Regardless of the Disruption

www.aptum.com

# TABLE OF CONTENTS

# PLAN FOR CONTINUITY REGARDLESS OF THE DISRUPTION

**BUSINESS CONTINUITY IS ABOUT BEING PREPARED FOR THE UNEXPECTED, THE UNPREDICTABLE AND EVEN THE UNPRECEDENTED. MUCH MORE THAN DISASTER RECOVERY, IT MEANS ANTICIPATING ANY EVENTUALITY THAT COULD DISRUPT A BUSINESS OPERATION, AND LEVERAGING CLOUD TO HELP MITIGATE THE RISKS.**

From hurricanes and wildfires, to ransomware and phishing attacks, to global pandemics and other unforeseen events, organizations face myriad disruptions that, in the worst-case scenario, can put them out of business. A 2019 IDC survey, *State of IT Resilience*[1], reported that 91% of organizations experienced some type of business disruption. For the same percentage, there was an IT-related business disruption.

While the impacts vary, the disruptions are often severe: loss of revenue, major reputational damage or even permanent loss of customers. As the IDC report points out, these business disruptions are becoming more common, and organizations are facing increasing issues related to factors like new technologies and new business models. "The fact remains that data disruption happens," says IDC, "and the negative impacts can be significant."

This eBook provides insights to help you develop a Business Continuity Plan, leveraging the cloud to architect resilient solutions that ensure you'll withstand any disruption to your business.

[1] IDC 2019 State of IT Resilience Report

# BUSINESS CONTINUITY PLANNING: ESTABLISHING A RESILIENT ORGANIZATION

Companies rely on people and processes, so in the event of a business disruption — whether a planned IT migration, ransomware attack or global pandemic — it's critical that the organization is resilient to protect those people and processes.

That's where a Business Continuity Plan (BCP) comes in. A BCP details how an organization will respond to what is really critical during planned or unplanned disruptions. Many see it as a disaster recovery (DR) plan, which is a key aspect of business continuity, but a BCP is much broader in scope. A disaster recovery plan focuses on recovering from a specific disaster, such as a fire or data breach. It is a plan to identify critical IT assets and assess data backup and recovery practices to recover as quickly as possible after the crisis.

A Business Continuity Plan, on the other hand, is about how to keep the business up and running in the event of a major disruption, either planned or unplanned — and it addresses more than IT. It defines policies, procedures and critical functions that must be performed across all aspects of the organization.

In addition to the prospect of business disruption due to IT, a BCP covers critical business needs like the requirement for alternate suppliers (if supply chains are disrupted) and the need for alternate space (if the current space becomes unavailable). It takes into account everything from business assets and processes to human resources, partners and suppliers.

Since disruption could be related to an IT failure, power outage, malware attack, weather event or natural disaster, a BCP is about *being prepared, to the best of one's ability, for the unexpected, the unpredictable and the unprecedented* — such as a global pandemic.

[2] Gartner Business Continuity Survey, March 2020

**12%**

**ONLY 12% OF BUSINESSES WERE "HIGHLY PREPARED" FOR THE IMPACT OF THE CORONAVIRUS.**

– Gartner Business Continuity Survey, 2020

The COVID-19 pandemic has put a spotlight on business continuity planning. Indeed, a Gartner business continuity survey[2] of 1,500 businesses in March 2020 found that only 12% were "highly prepared" for the impact of the coronavirus.

"The challenge lies partly in the ambiguity inherent in managing an emerging risk such as coronavirus," according to Gartner. "Organizations often have policies in place to deal with most risks, but they don't activate them until it's too late because no one is owning the risk or taking it seriously until it is fully manifested."

Yet the cost of unplanned downtime is enormous. Indeed, it could put a company out of business! That's why it is critical to be prepared for the unexpected, including the technical aspects such as Disaster Recovery-as-a-Service (DRaaS), backup, security and resilient design, all of which are critical elements of a Business Continuity Plan.

# WHY A BCP IS BUSINESS-CRITICAL

A Business Continuity Plan makes an organization more resilient, no matter what the disruption. Business continuity isn't about planning for specific scenarios, such as a blackout, ransomware attack or pandemic — after all, it's impossible to predict the future. Rather, it's about planning for continuity, regardless of the specific scenario.

That said a BCP should define all the processes and eventualities that may affect business operation, with courses of action for each. For example, if a manufacturer's main supplier of certain parts is offline due to a natural disaster, what is the process to obtain the parts from backup suppliers?

The IDC *State of IT Resilience* survey found that most organizations surveyed have experienced business disruptions, "which resulted in material impact in terms of either cost, direct loss of revenue, permanent loss of data, or damage to company reputation. Even more concerning is that many organizations are seeing new forms of disruptions, such as ransomware, cause considerable downtime."

The BCP itself is project-driven, typically developed by business analysts and enterprise architects at the executive level, with input from department managers. Solution architects then design the technical components to support the BCP, which should be updated and tested regularly, as frequently as every quarter.

"A BCP is a business plan that involves much more than IT resilience and DRaaS," says Kwong Lum, Lead Architect, Cloud at Aptum. "It involves all of your business processes, identification of possible business disruptions, what to do in each scenario and how you will continue to operate. How do you deal with suppliers? How do you deal with personnel, HR and payroll? What about health and safety? It's a true business plan."

While business continuity planning will naturally lead to an architectural conversation, it is about organizational readiness and involves myriad aspects that aren't technical. For example, in the case of COVID-19, bricks-and-mortar shops and restaurants had to suddenly shutter their doors during mandatory lockdowns. While pre-existing Business Continuity Plans didn't outline a strategy specifically for coronavirus, a BCP would outline impacts such as having your staff or premises unavailable.

A Business Continuity Plan must identify key areas of the business, critical functions within those areas, dependencies between those functions, acceptable downtime for each function, and a plan to restart or maintain operations.

**A BUSINESS CONTINUITY PLAN IS BUSINESS-CRITICAL BECAUSE IT IS ALL-ENCOMPASSING, INCLUDING ANSWERS TO CRITICAL QUESTIONS LIKE THESE:**

- How will IT staff continue to manage technology systems?
- How will they access data and applications?
- How will employees continue to work, and from where?
- How will sales, support, HR and other departments continue to operate?
- If you fail over to your DR site, how will your DNS be managed?
- How will employees access the data in the DR site?
- What is an acceptable restoration time for critical workloads, and does this align with business expectations?

# THE 'NEW NORMAL' FOCUSES A NEW LENS ON BUSINESS CONTINUITY

The Gartner Business Continuity Survey in March 2020 found that 56% of businesses rated themselves "somewhat" prepared for the disruption of coronavirus. But importantly, just 2% of respondents believed they were fully prepared, and their business could continue as normal.

The pandemic forced many organizations to deal with issues like reduced staff numbers, supply chain disruptions and demand downturns due to lockdown, quarantine and physical distancing measures. Even organizations with a pre-existing Business Continuity Plan found that it needed to be updated and revised in the face of what now appears to be the 'new normal'.

In its Guide for Pandemic Planning and Response[3], the Uptime Institute recommends a tiered-response plan as part of an overall BCP. That plan should include details on operating with reduced staff (including work from home requirements), the business impact on both critical and non-critical work, and the impact on service levels, as well as health and safety policies.

The plan should also identify critical IT assets, maximum acceptable downtime or recovery time for IT systems, disruption/failure response procedures, minimum acceptable staffing levels (and designation of alternates if staff are sick or quarantined) and acceptable levels of critical on-site activities. While these are best practices for pandemic planning, they also serve as best practices for a variety of unplanned disruptions.

The Uptime Institute also recommends preparing for other related disruptions, since the shift to more Internet-based activities such as e-commerce, remote monitoring and telecommuting will put increased stress on networks and bandwidth. "Management should anticipate disruptions on multiple fronts. Understand the network paths of mission-critical IT applications and workloads. Review and revise backup/disaster recovery plans as necessary," recommends the Institute.

All of this should be included in your Business Continuity Plan to reflect the latest best practices in pandemic planning, for both now and the future.

[3] Uptime Institute Pandemic Planning and Response: A Guide for Critical Infrastructure, 2020

# IMPORTANT FIRST STEPS: ASSESSMENT AND ANALYSIS

A risk assessment and business impact analysis (BIA) are important first steps in the business continuity planning process, particularly for organizations with remote or hybrid workforces. If you don't know what you're protecting, or which workloads are mission-critical, then your Business Continuity Plan has a higher likelihood of failure – or it will cost more money and take more time to recover from a disruption.

A BIA identifies potential impacts if you suddenly lose business functions – typically these are quantified in dollars. By conducting a BIA, you determine which business functions are most important and determine acceptable downtime for each of those functions.

A risk assessment includes human concerns, process considerations and IT issues. It starts with assessing risks to various assets – from mission-critical to non-critical – and validates any controls already in place. This assessment should reveal any gaps that exist, and where you may need additional controls.

Part of the risk assessment process involves determining the criticality of each system, and tolerance for data loss. How critical is it to the organization? What will it cost if it's down for five minutes? What about five days? Are there dependencies with other systems or business functions? Is it used by customers or employees? Answering these questions helps develop a strategy for IT resilience and remote workforce access as part of an overall Business Continuity Plan.

For example, if your payroll system goes down, the business won't immediately grind to a halt. But if an online transaction system goes down — one that processes thousands of customer transactions every minute — the business stands to lose revenue with each moment that passes.

> "When you assess the criticality of all the workloads, you can determine if the current solution meets your needs. If it doesn't, you need to rearchitect the solution. If a mission-critical system can't be down for more than five minutes, you'll need to introduce scale and resilience, replicate that, distribute traffic, and use multiple sites."
>
> – Martin Poirier, Cloud Solutions Architect, Aptum

Assessing criticality involves understanding the importance of each workload and analysing the impact if it goes down. Once you understand criticality, you can determine the appropriate service level agreement (SLA) for that workload. A payroll system that can be down for five days won't require the same SLA as an online transaction system that can't be down for more than five minutes.

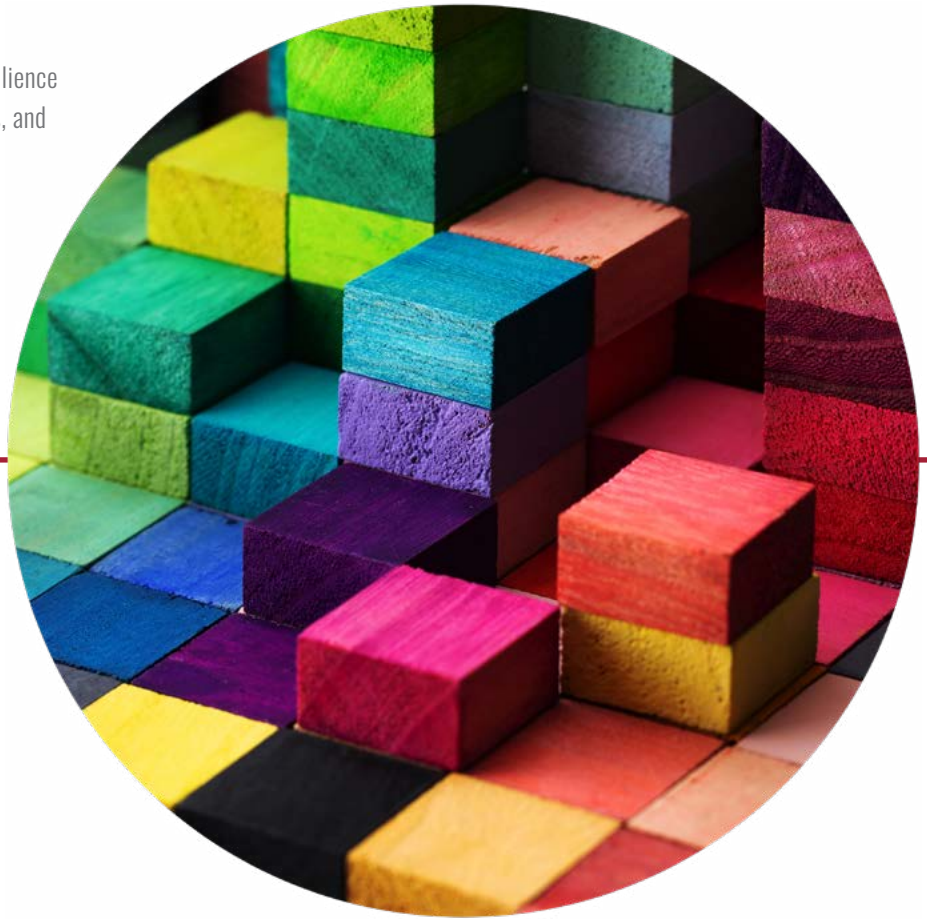
# THE TECHNOLOGY BUILDING BLOCKS OF A BCP

There are many moving parts to a Business Continuity Plan, which can be supported by IT strategies, technologies themselves, and business processes. For example, moving data to the cloud, rolling out virtualized desktops, or migrating from an on-premise to co-location data centre all help eliminate dependency on location — both the local aspect of data, as well as the presence of on-site employees.

In its *State of IT Resilience* report, IDC outlines three key tenets of IT resilience – the abilities to protect data during planned disruptive events, effectively react to unplanned events, and accelerate data-oriented business initiatives.

From a technology perspective, IDC states that "IT resilience includes traditional disaster recovery and backup tools, and also incorporates advanced analytics and security capabilities necessary for the success of any digital business in the 21st century."

Technology is a critical component of IT resilience, which supports business continuity. There isn't a single tool or toolset that will ensure continuity; rather, it's a combination of technologies that enable a business to become more resilient and ensure continuity, such as Disaster Recovery-as-a-Service (DRaaS), backup and archiving tools, replication to the cloud and data protection services.



DRaaS, for example, replicates your data and hosts it on virtual servers in the cloud, providing rapid failover of your production environment in the event of a man-made or natural catastrophe. A managed DRaaS solution can help minimize recovery point and recovery time objectives (RPO and RTO), so data loss is negligible. DRaaS also enables point-in-time rollbacks to protect against malware and ransomware, and offers a remote disaster recovery site without the up-front costs associated with a second infrastructure stack.

But from a data recovery standpoint, DRaaS is not enough – you also have to protect the data itself. A common mistake many organizations make is assuming that because their data is in the cloud, it is pervasively available. Recovery will depend on your long-term backup and retention strategy, and ensuring your data is protected, available and immutable (so it can't be altered).

A checklist is a common BCP tool. It should include a list of all critical IT systems, the location of data backups and backup sites, and contact information for backup site providers.

## DRaaS DELIVERS 8-SECOND RECOVERY FOR BUSINESS CONTINUITY

Disaster Recovery is one important aspect of any Business Continuity Plan. An Aptum customer needed a DR solution to accelerate their cloud-first strategy, reduce costs and create more geodiversity between their production and DR sites. Using a DRaaS solution, they replicated and migrated key applications to the cloud, reduced hardware costs by migrating data from multiple disk-based backup appliances to the cloud, and achieved a recovery point objective of 8 seconds. This kind of DR solution fits seamlessly into a Business Continuity Plan.

# LEVERAGING CLOUD FOR BUSINESS CONTINUITY PLANNING

In Aptum's *Global Cloud Impact Study*[4], which surveyed 400 senior IT decision-makers in the U.K., U.S. and Canada, a huge majority (89%) see cloud as essential to business continuity.

That's not surprising. Compared with traditional methods, cloud can make it easier, faster and cheaper to get your business back up and running after a disruption. It should be considered a key component of an effective Business Continuity Plan.

Replicating data to another data centre is costly and complex. "Very few organizations have the financial means to build a complex solution like that, so the cloud makes it more accessible — it democratizes data so it becomes a commodity. That makes it easier to support business continuity," says Martin Poirier, Cloud Solutions Architect at Aptum.

There are a number of ways to leverage cloud as part of your overall Business Continuity Plan. For example, Amazon Simple Storage Service (S3) and Azure Cool Blob Storage allow you to replicate your data and protect it in the cloud. Azure enables you to seamlessly extend SAN storage to the cloud, or you can set up local S3 object stores to keep an immutable copy on-site, and then replicate that to the cloud.

Regardless of the approach, this should be part of your overall cloud adoption framework. And with this comes the concept of availability zones. "When you're building a solution in the cloud to maximize IT resilience, you want to make sure the application or solution is redundant," says Kwong Lum of Aptum. "That way, for example, if one Microsoft data centre goes down, your solution remains available in another Microsoft data centre in that same availability zone. Design it for local redundancy *and* geo-redundancy."

If you're moving from a legacy application such as an ERP or HR system, consider whether you may be better off deploying a software-as-a-service (SaaS) application. Ask yourself … can you decrease your IT administration costs and enable a highly available application in the cloud as a software service? In some cases, you may be better off deploying a SaaS solution rather than implementing a private application you have to customize — while building resilience that contributes to business continuity.

[3] Aptum Global Cloud Impact Study

# PREPARING YOUR NETWORK FOR SEAMLESS BCP IN THE CLOUD

Using cloud for a Business Continuity Plan hinges on the design of your enterprise IT architecture. For example, you might have an application that is resilient, but the network behind it is not. By understanding your requirements, you can design an architecture suited for BCP, such as ensuring the network has sufficient capacity and there are no bottlenecks or flaws in connectivity.

When designing BCP in the cloud, a critical consideration is security. Since public cloud works on a shared security model, hypercloud providers like Azure and AWS provide a secured platform with the necessary certifications, which takes a lot of effort out of designing your solution. But whatever you build on top of that platform also needs to be secured.

How are your users accessing data remotely? What devices are they accessing it from? "That's where a cloud access security broker (CASB) comes in," says Kwong Lum. "It's hugely important these days, especially with the world of BYOD, and should be integral to your IT resilience plan for data protection, and part of your Business Continuity Plan."

A web application firewall is also essential, because the more data you move into the cloud, the more you expose the network. If you decide an application can be accessed publicly, then you expose that application to more security risk. Security is a component of business continuity, and complementary technologies such as hybrid cloud management can help.

While technology provides the building blocks of a Business Continuity Plan, it needs to start with strategy. "Look at it strategically. Think strategy first. IT resilience, disaster recovery, business continuity — they're all strategic before being technical achievements, and they're driven by strategy," says Martin Poirier of Aptum.

> "Think strategy first. IT resilience, disaster recovery, business continuity — they're all strategic before being technical achievements, and they're driven by strategy."
>
> – Martin Poirier, Cloud Solutions Architect, Aptum

# BEST PRACTICES FOR BCP IN THE CLOUD

"It's misleading to think that taking a workload and moving it to cloud will give you a Business Continuity Plan — that is just your old processes on new technology. You have improved your situation slightly, but you haven't leveraged the full potential of the cloud," says Martin Poirier.

Organizations that do not have time pressures in moving to the cloud may choose a staged adoption or slower migration, where they start with small, easy projects and build on their successes. Each time they move a workload, it's where it's supposed to be with the right design for business continuity.

But in many cases, organizations need to "accelerate" migration, meaning they make the move as quickly as possible. Usually there's a reason for this – they're moving to another physical location, or they're faced with a data centre closure. Once they move, they must go through an optimization phase to build in business continuity planning and retrofit resilience requirements.

"There are two approaches here. It's not that one is better than the other — usually it's because of the motivation and critical constraint at the beginning," says Poirier.

Regardless of the approach, Poirier says it's important to take the time to do a proper assessment, discovery and rationalization of your assets. Understand which stage an application is at, where you want it to be, and how it can be optimized to get there. If possible, your first project should be one that's low risk and gives you an opportunity to learn, manage your costs and understand how governance works in the cloud.

"Cloud adoption isn't about moving as fast as possible. It's about giving yourself the time to train and learn what you're doing when you go to the cloud," says Poirier. "We've seen some businesses that moved so quickly, they didn't understand they chose a service with no SLA — they simply chose the cheapest server. It looked like a bargain, but down the line they're performance-choked and have no guarantee of availability."

"It's misleading to think that taking a workload and moving it to cloud will give you a Business Continuity Plan — that is just your old processes on new technology. You have improved your situation slightly, but you haven't leveraged the full potential of the cloud."

– Martin Poirier, Cloud Solutions Architect, Aptum

Moving workloads to the cloud doesn't inherently ensure resilience. You still have to design those workloads to provide it. Some legacy applications won't scale well in the cloud, so if you have problems with them on-premise, you will likely still have the same problems in the cloud.

Ensuring you have the right design and Service Level Agreement will go a long way to making your data truly resilient in the cloud. Evaluate your Business Continuity Plan and update it where necessary to ensure your workloads are resilient, no matter where they reside.

# MAXIMIZING THE BENEFITS OF CLOUD FOR BCP

The COVID-19 pandemic was a business continuity learning experience for many organizations. But one interesting fact came to the fore – 95% of companies used cloud computing models in some way to mitigate the effects of the health crisis, according to Aptum's *Global Cloud Impact Study*.

But many companies aren't truly realizing the benefits of cloud, such as the ability to add new computing and storage resources on demand — even after they make the transition to the cloud. In fact, many respondents to the Aptum study are only partially or mostly successful in realizing specific benefits. For example, only 35% of respondents in the study reported complete success with business continuity in the cloud.

Taking full advantage of the benefits of cloud, including its value for business continuity, involves investment and planning. The more sophisticated a cloud migration project, the more intricate the design and development choices. Solutions require expertise that companies often simply don't have available in-house. But organizations can take their cloud strategies to the next level by partnering with experts who understand the nuances of cloud transformation.

For example, you can leverage platform-as-a-service (PaaS) from a cloud provider to make cloud achievable and available, at an affordable cost. While there's no such thing as a one-size-fits-all, off-the-shelf Business Continuity Plan, an expert cloud provider can help you 'bake in' the business continuity every organization critically needs.

# APTUM PARTNERS TO ENABLE BUSINESS CONTINUITY IN THE CLOUD

Aptum's experienced professionals provide expert guidance to leverage the cloud as key to a Business Continuity Plan.


We contribute to a robust Business Continuity Plan, leveraging the cloud to architect resilient solutions, so you'll withstand any disruption to your business.

## For more information on Business Continuity Planning in the Cloud, visit the Aptum Cloud Hub.