



# Cloud outages happen. How does your company prepare for a crisis?

## 6 Steps to Better Cloud Data Management

Cloud outages – stemming from a wide variety of unforeseen problems such as undetected software bugs, equipment malfunctions, and natural disasters – can happen at any time. And they can cause significant damage to your business if it's not adequately prepared. For example, cloud downtime hurts your customers, resulting in lower customer satisfaction and revenue loss.

Unfortunately, infrastructure can never be 100 percent fail-proof. Even the largest cloud providers in the world suffer from unplanned outages. That's why it's vital for your IT management department to be prepared; to minimize costly downtime and ensure immediate restores.

### Is your company prepared not only for business continuity but also for business resilience?

The pandemic has highlighted the significant differences between organizations prepared to adapt to rapid change or crises and those unable to pivot quickly. Those IT teams that had long invested in both building and exercising business continuity plans as well as continually updating and modernizing them have operated with less disruption and are now well positioned to accelerate digital investments for business resilience. In contrast, those with legacy solutions and processes have been struggling to keep up.

If your organization is in the latter group, all is not lost. You and your organization can quickly catch up by taking the time now to understand cloud adoption and legacy data management shortcomings, then preparing to handle them in more efficient and effective ways.



#### 1 Understand cloud outage risks and create a mitigation strategy

Organizations under appreciate that cloud outages pose a higher business risk than even security breaches. When cloud outages occur, not only is customers' data inaccessible during downtime, but in severe cases, data may be lost or become irrecoverable. Businesses that invest in cloud solutions should assess the risks associated with cloud outages and concurrently determine effective risk mitigation strategies to cover the expected cost of losses. This may entail creating a business case outlining your data protection challenges and needs.



#### 2 Protect your business with guaranteed SLAs from providers

To protect your business in case of a failure, it's wise to ask cloud service providers for data center configuration information or to obtain a service-level agreement (SLA) guarantee. If your business doesn't have one in place, negotiate one – and fast. Every one of your cloud vendor contracts should ensure that you are well protected and the service provider is accountable for any downtime.



### 3 Adopt a multi-cloud strategy to avoid significant data loss

Adoption of a multi-cloud strategy is the most effective solution to prevent considerable data loss damage. It hedges your data against a single point of failure. Moreover, a multi-cloud strategy can reduce vendor lock-in and enable your organization to optimize your cloud investments by providing the best available options regarding reliability, support, features, and other service factors that can positively impact business decisions.

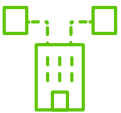
Since multi-cloud strategies distribute your resources across different service providers or locations, this cloud strategy adds resiliency and redundancy to your network, and can reduce the chances of cloud downtime and data loss. In case of a data center failure, your workload(s) will failover to the next location safely.

A multi-cloud strategy also can increase application performance by physically bringing traffic closer to your end users, which enhances throughput. Moreover, with a multi-cloud strategy, your organization improves quality of data and reduces the chances of occurrence of unexpected downtime.



### 4 Ensure cloud provider networks are automated

Regardless of how reliable your cloud services from hyperscalers and other cloud providers are, unexpected errors do occur. Ensure their operations are automated to reduce the likelihood of downtime. Automation not only helps enhance productivity, it also helps providers reduce manual tasks associated with human errors. Take a closer look at the IT model your business and providers ascribe to and know their weaknesses. Eliminate weak links to strengthen your business continuity and resilience.



### 5 Plan ahead for data recovery

Accidents happen. Being prepared to recover quickly is what sets agile businesses apart. Forward-looking IT leaders consider contingencies and the capabilities they have to use them. One essential attribute of effective fall-back plans is to maintain data replicas across various availability zones. This protects organizations against cloud downtime and helps move relevant data across multiple locations during cloud outages. Know about data locality (aka data sovereignty) so you can pinpoint data that is affected by a cloud outage, and as needed, recover in a different location with ease.



### 6 Ensure the availability of a reliable communication channel

Accidents happen. Being prepared to recover quickly is what sets agile businesses apart. Forward-looking IT leaders consider contingencies and the capabilities they have to use them. One essential attribute of effective fall-back plans is to maintain data replicas across various availability zones. This protects organizations against cloud downtime and helps move relevant data across multiple locations during cloud outages. Know about data locality (aka data sovereignty) so you can pinpoint data that is affected by a cloud outage, and as needed, recover in a different location with ease.

## Build a Plan Now to Be Prepared for Later

Cloud downtime is a reality, and something all businesses should prepare to handle in advance. Ensure your business has the best strategies and crisis management approach in place to accelerate business resilience.