White Paper

Backup as a Service

Peace-of-mind with greater cost efficiency, predictability, and flexibility

Table of contents

2 Why cloud-based backup?

3 The promise of cloud

4 Cloud backup service models

5 Developing a cloud backup strategy

7 Selecting the right CSP

8 Getting started: HP CloudAgile Service Providers

8 Learn more

Data center of the future

Cloud-based backup services promise to improve data protection, while relieving organizations of the burdens of backup and recovery.

With downtime no longer an option, many small and medium businesses are looking to the cloud. Is Backup as a Service the answer to today's data-protection challenges? What should organizations look for in a cloud service provider?

Why cloud-based backup?

It's no exaggeration to say that data is the lifeblood of business. Conversely, data corrupted, lost, or even just temporarily unavailable can mean the loss of business—lost revenue and lost customers. Data loss can also be costly—in terms of regulatory non-compliance, liability, and damage to brand and reputation.

Ensuring data integrity and availability is increasingly difficult—especially for small- and medium-size businesses (SMB) with limited budgets and in-house resources.

In a recent study, 85% of 500 SMBs polled said they struggle with the costs of data backup and recovery; 80% with the complexity; and 83% with a lack of internal capabilities.[1] The survey found 41% of SMBs reporting the cost of downtime to their business was $150,000 per hour or more, with a typical outage costing $600,000 or more.[2]

Bigger data, smaller windows
Perhaps the biggest data-protection challenge SMBs face is rapid and unrelenting growth in the amount of data. According to various estimates, the volume of business data worldwide doubles every 12-18 months—a rate predicted to accelerate as mobile apps, social media, multimedia, and big-data analytics are increasingly integrated into everyday business.

Besides dramatic growth in the amount of data that needs to be protected, the playing field for data backup is also changing. With new types of content, new sources of data, and the 24/7 demands of applications, users, and customers, the criticality and size of data keep growing while backup windows shrink. As a result, organizations are finding that traditional approaches to data protection are no longer adequate.

Growing complexity, cost, and risk
New business demands, content sources, and data formats add to the complexity of backup and recovery environments that are already difficult to manage. Businesses are struggling to provide the right level of data protection with limited budgets and resources. Complicating factors include:

- Applications with different backup and archiving requirements
- Multiple platforms, multiple backup and recovery methods, multiple tools
- Aging legacy infrastructure, backup devices, and software
- Unpredictable workloads and data growth rates

Changing regulatory requirements
Industry-specific regulatory requirements further complicate how backup and recovery are implemented. For example:

- Healthcare regulations, such as HIPPA and HITECH in the U.S. and the European Observatory on Health Systems and Policies in the EU, mandate very strong physical, software, and procedural data-protection solutions. In fact, HITECH makes off-site backup and recovery a requirement for protected health information (PHI).

[1] http://www.computerweekly.com/news/2240185363/Backup-and-recovery-challenges-most-small-businesses-study-shows

[2] Technavio, "Global Disaster Recovery-as-a-service market," doc #IRTNTR2883, November 2013.

- Financial services industry regulations both in the U.S. and globally have very stringent recovery point and recovery time objectives (RPO/RTO) that make it nearly impossible to meet with traditional near-line or off-line backup solutions.
- Local and federal government agencies in most industrialized countries—as well as businesses contracting with government agencies—are subject to restrictions and policies for backup and recovery and accountability that must be followed. In fact, although the U.S. has a wide range of laws that aim to uphold data privacy, the European Union and the European Economic Area, Canada, Argentina, Hong Kong, and Australia tend to have the most comprehensive data-protection laws.

In addition to making sure backup and recovery procedures comply with industry regulations, staff and systems must keep pace as regulations are added or updated.

Underestimating the challenges

While the backup of data to secondary or off-site media storage protects against data loss, businesses must be able to quickly restore data and recover operations to stay up and running. Designing, managing, and administering in-house backup and data recovery solutions has become a challenge for even the most proficient IT professionals. In fact, organizations do not typically invest the time and resources in disaster recovery planning and testing to ensure smooth recovery from data backups. Most organizations significantly underestimate how long it will take to get back online after an unplanned outage.

Limited resources and expertise

For IT professionals who wear many hats, acquiring the expertise and finding the time to improve data backup procedures can be extremely difficult. Businesses are often reluctant to divert technical resources from strategic initiatives that generate business value to improve backup and recovery.

As a result, improvements that could significantly improve data protection, simplify operations, and cut costs often get pushed to the back burner. For example, many organizations are aware that their legacy backup processes and technologies are duplicating and storing copies of the same unchanged data over and over again. But no one internally has the time or expertise to perform the mailbox management, deduplication, compression, storage optimization, and other best practices necessary to maintain a manageable data footprint. As a result, duplicate data that could be deleted consumes considerable storage capacity and human capital and makes backup and recovery more difficult, costly, and complex.

The promise of cloud

Given the challenges of in-house backup and recovery, it's easy to understand the appeal of cloud-based backup services that promise to improve data protection, while relieving organizations of the burdens of backup and recovery. At a high level, backup as a service from the cloud can provide greater peace of mind, cost efficiency, predictability, and flexibility.

Cloud-based backup services enable businesses to do more with less—less time, budget and resources. A secure, off-site, online backup resource improves recovery point, and recovery time objectives, shifts spending from capital investment (CAPEX) to operational expense (OPEX), improves service levels at a reduced ongoing cost, and supports backup and recovery requirements for emerging trends such as mobility, bring your own device (BYOD), big data, and social media. When done effectively, cloud-based backup services enable a return on investment (ROI) to the power of three: return on infrastructure, return on information, and return on individuals. Specific benefits include:

- Automatic, online backup to off-site infrastructure
- Affordable data protection and recovery, even in the event of a regional disaster
- SLA-based commitments
- A predictable price for service, leveraging a pay-per-use scenario
- Retirement of outdated backup and media technologies
- Expertise and support to address the data-protecting challenges of emerging trends
- Reassigment of internal resources to work on more strategic business initiatives

Proper planning
While the promise is great, making the move to a cloud-based backup service is not a decision to make lightly. The security and protection of mission-critical data assets are vital. The ability of authorized users to identify, manage, control, and search data across the business must not be compromised.

Making the right decision starts with researching options and mapping services to business requirements.

Cloud backup service models

While the details of individual service offerings can vary widely and span private, public, and hybrid options, our focus will remain on hybrid and public cloud backup services.

Both models provide the added security of storing copies of data in the cloud that can be accessed for restore as needed. The models share other commonalities as well. For example, both can:

- Reduce the size of backup through deduplication services
- Provide long-term archiving in addition to backup services
- Enable organizations to retire old and costly legacy hardware, software, and media
- Extend the economies of scale and advantages of virtual and converged platforms to provide greater agility and cost efficiency, while also enabling more sophisticated analytics, search, and data mobility

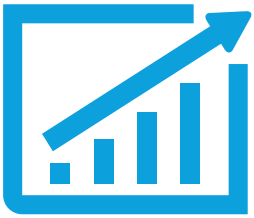
A hybrid cloud model
In this service model, organizations continue to manage their own backups, sending copies of data to provider-managed backup infrastructure in the cloud and retrieving that data from the cloud, if necessary, for a restore.

Internal staff continues to perform backups using their own company-owned backup software. The cloud service provider (CSP) manages the performance, capacity, and security of the remote backup infrastructure (hardware, software, media) removing the need for traditional tape collection methodology. Backup as a service using a hybrid model often includes these services:

- Continuous monitoring of the backup processes
- Proactive alerting in the event that backups fail
- Assistance in restoring and recovering data
- Version management

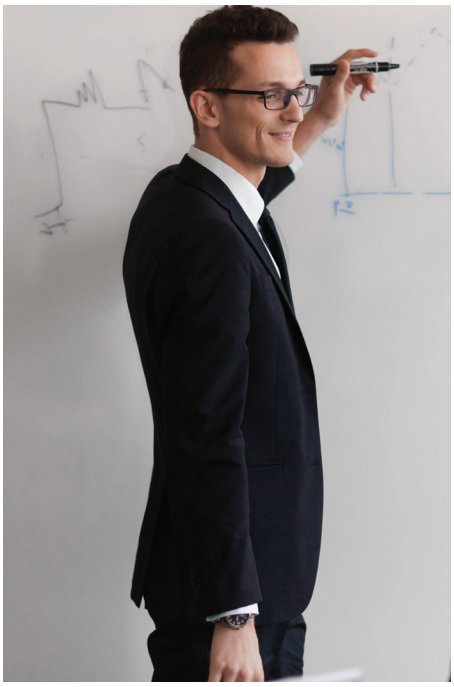
Adopting a hybrid model tends to work best for those companies that desire to minimize internal errors and keep costs down, while maximizing the efficiencies of their infrastructure. The advantages of a hybrid approach include:

- Added data protection and peace of mind with backup of data in a remote location, enabling data recovery even in the event of disaster
- Reduced costs through cloud-scale economies for infrastructure
- Freeing of staff from tedious backup and backup-infrastructure maintenance tasks (for example, taking backup media offsite, changing tapes, labeling CDs).
- Greater agility and on-demand scalability/elasticity in response to need
- Minimal change to existing processes, policies, and procedures required
- Removal of tape methodology



Power of ROI

Cloud-based backup services promise a triple return on investment (ROI): return on Infrastructure, return on Information, and return on Individuals.



A public cloud model
In this service model, organizations completely outsource the backup and recovery function to a CSP. The CSP works with the organization to help determine requirements and develops, implements, and manages all aspects of backup and recovery. Primary responsibilities of the CSP typically involve meeting RPO and RTO as defined in their service level agreement (SLA).

CSP-owned backup software and hardware, residing in a CSP-managed gateway at the customer's sites, works with backup software and hardware in the CSP data center. The local and remote backup solutions work together to mitigate any connectivity issues and provide redundancy with no single point of failure. The CSP performs all backup and recovery tasks and provides the business with a completely managed service to meet its RTO, RPO, and other objectives.

The advantages of this approach include the added data protection, peace of mind, and agility gained from backing up to a remote location. Additional benefits include:

- Complete backup and recovery planning, design, implementation, and management
- CSP-owned assets, enabling the transfer from a CAPEX to an OPEX model
- Defined SLAs
- No single point of failure
- End-to-end modernization, standardization, performance management, and optimization
- Simplified operations management
- Internal staff freed from all backup and recovery responsibilities to work on more strategic projects

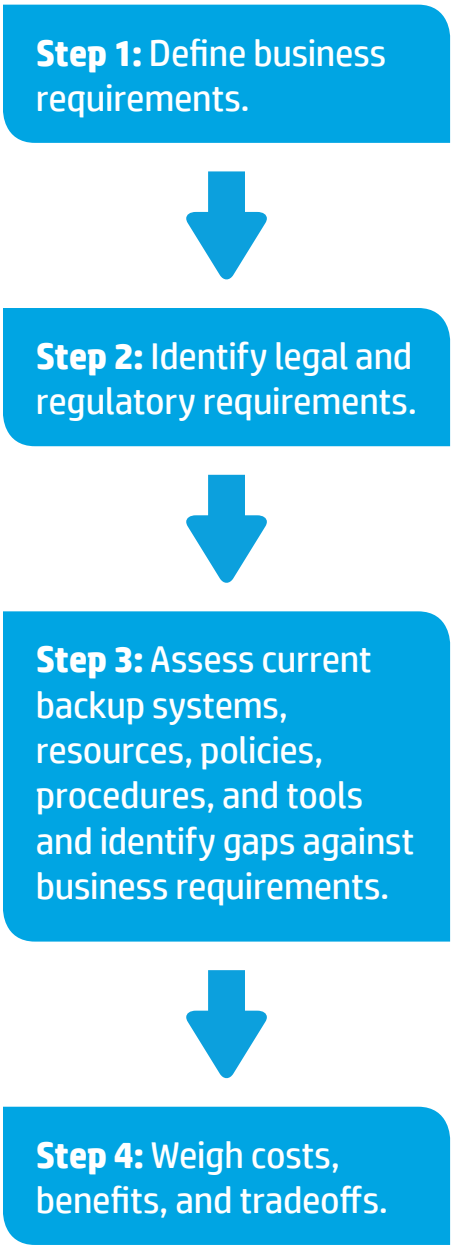
Developing a cloud backup strategy

Deciding how to move forward with a cloud-based backup service requires careful consideration and proper planning. It starts with a thorough review of business requirements and considers how these objectives may change over time.

Step 1: Define business requirements.

- What are your recovery time objectives (RTO)?
- Which data is critical to continued business operations?
- How fast is data growing?
- Do different applications require different levels of data availability?
- What types of users need to be able to locate and restore specific data?
- What level of performance do current workloads require?
- What level of dynamic agility is required to respond to changing workloads and business growth?
- Is data security or compliance a concern?
- How must data, backup, and recovery processes be monitored, managed, and tested?

Figure 1. Developing a cloud backup strategy in four easy steps



Step 2: Identify legal and regulatory requirements.

- What business and industry regulations govern privacy, disclosure, and legal discovery?
- What specific backup and recovery capabilities are required to meet regulations?
- How long must you retain data?
- What associated accountability requirements must be enforced?
- Are specific credentials required to design, implement, or manage data backup or recovery?

Step 3: Assess current backup systems, resources, policies, procedures, and tools and identify gaps against business requirements.

- Are data protection goals aligned with business objectives?
- Are current solutions meeting those objectives today?
- Can they expand and adapt as business needs grow and evolve?
- What is your organization's ability to recover data in a timely manner?
- Has there been a recent data loss or outage? How long did it take to restore operations?
- Are there issues with backing up data in remote sites, branches, or offices?
- What level of expertise is available internally?
- Is it difficult to recruit/retain the expertise you need?
- How much data is being backed up?
- What portion of backup data is duplicate data?
- How many copies of backup exist across the organization?
- How much is your organization investing in developing IT staff data-protection skills and knowledge?
- Is tape still being used for primary backups?

Step 4: Weigh costs, benefits, and tradeoffs.

- Can you quantify the current costs of backup and recovery?
- What costs would be associated with a transition to a cloud backup model?
- What level of change can your organization tolerate?
- What are the relative tradeoffs of different cloud backup service models for the business? Will backup infrastructure as a service deliver the capabilities required or serve as an interim step? Or is complete outsourcing of the backup and recovery function needed?
- Are there monitoring and management tasks that could or must be kept in-house?
- Are there legacy technologies that should be retired?
- How important is cost predictability?
- What would the payback on moving from a CAPEX to an OPEX model be?
- How would outsourcing backup and recovery or backup infrastructure management enable people and budgets to be shifted to strategic projects and growth initiatives?

Cloud Service Providers (CSP)

CSPs manage the performance, capacity, and security of the remote backup infrastructure (hardware, software, media).

Selecting the right CSP

Even with a clear understanding of business requirements, data-protection objectives, and an enterprise strategy for cloud-based backup in-hand, finding and selecting the right CSP can be a challenging task.

Gartner reports that hundreds of service providers worldwide offer recovery as a service. Provider capabilities, service levels, and management responsibilities vary significantly among providers.[3] Beyond that, the number of providers is likely to increase with the market projected to grow at a compound annual growth rate (CAGR) of 55% to $5.7 billion by 2018.[4]

At the same time, it's a market destined for churn as leaders emerge and others fall by the wayside. Therefore, researching the reputations, track records, and financial viabilities of potential CSP partners becomes as important as evaluating the services they offer. Industry associations, certifications, customer references, trade press, analyst reviews, and current IT partners can be valuable resources. Researching and identifying providers that align with your specific business requirements is a critical step in effectively migrating to a cloud-based backup model.

As part of the process, evaluate providers with careful scrutiny. Consider the following:

- **Reputation—**Consider the reliability and reputation of the CSP. A CSP must be able to provide a reliable and secure environment in the most scalable, cost-effective, and simplest manner.
- **Infrastructure and technology—**How robust is the CSP's datacenter network? Does it have enough data centers in enough different locations to ensure availability of your data? Does it have a robust and highly available environment powered by leading IT infrastructure? What hardware and software are used by the CSP to power the backup solution? Is the technology reliable, industry-accepted, and validated? How is it rated in terms of security?
- **Professional services—**Does the CSP offer consultative and support services to help you build a business case and make a smooth transition to cloud-based backup services? Does it offer a range of managed and professional services to help you develop, migrate, and maintain optimal performance?
- **Best practices—**Ensure that its backup solution is built on a foundation you can trust. What is the provider's own backup and recovery strategy?
- **User experience—**Consider overall user experience and how this varies from provider to provider. Does the CSP enable the proper level of controls and layers of access that you require? Does the CSP have any restrictions for multi-user access?
- **SLAs—**Review the fine print. Understand its support model to ensure that its published SLAs fall within your tolerance level, and understand the CSP's guarantee on availability.

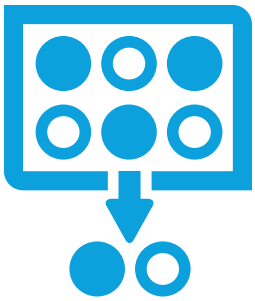
Next, compare your requirements to the CSP's offering. Evaluate it based upon your requirements. Map your strategy to its offerings to see if there is a fit. For instance:

- **Your workloads—**Evaluate your workloads to determine if the CSP delivers the performance, security, and resilience your business requires.
- **Your industry—**Does the CSP understand your industry? Does it understand regulatory requirements that apply to your industry? Do its policies comply with your industry's requirements?
- **Your security—**Does the CSP offer the security your business needs and the credentials your industry mandates? What level of encryption is it providing? Do you have specific industry requirements for encryption, and if so, is it abiding by those requirements? For instance, in healthcare, the CSP must ensure "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt".[5]
- **Your dymanics—**How flexible is the CSP in terms of coping with your dynamic business needs?
- **Your data—**How will your data be managed, monitored, and tested?

[3] Gartner, "Critical Capabilities for Recovery as a Service," November 2013. gartner.com/technology/reprints.do?id=1-1PORHDC&ct=140117&st=sb

[4] Technavio, "Global Disaster Recovery-as-a-Service Market," doc #IRTNTR2883, November 2013.

[5] Healthcare in the US, for example, requires "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt." US Department of Health and Human Services. 2014. hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html



HP StoreOnce Backup

HP StoreOnce Backup with StoreOnce Catalyst is a single, agile, efficient, and secure backup and recovery solution. Reduce costs and keep pace with data growth, confident that your SLAs are securely met and your valuable data is not at risk.

Getting started: HP CloudAgile service providers

Find the right match by seeking out an HP CloudAgile service provider. They leverage HP technology to offer state-of-the-art backup services, ranging across varying markets, geographies, industries, and domain expertise. They provide access to service offerings that are flexible, reliable, secure, and cost-effective.

You can trust that you are getting the most out of your investment. HP CloudAgile partners meet demanding SLAs and offer the right mix of in-house and off-site computing resources without locking you in so that you can balance your business assets with a backup solution that offers you agility and optimal operating efficiency.

HP CloudAgile partners offer backup services that are powered by trusted HP technology—built with proven, leading storage solutions, servers, management software, and services. Many incorporate a range of HP solutions from HP 3PAR, HP StoreOnce, and HP StoreOnce VSA for federated deduplication designed to work at the source of data, forming the backbone to a solid backup. Many rely on HP Data Protector for efficient, simple, and secure data management. And many rely on HP's trusted BladeSystem and Software-Defined Networking to help simplify and align IT to your business demands, all backed by industry-leading support and services.

Together, HP CloudAgile partners and HP provide a key way to streamline backup, recovery, and archiving for organizations of all sizes.

Learn more

For more information, visit HP's Cloud Partner Solution Navigator:

hp.com/go/cloudnavigator

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA5-4108ENW, August 2014