Requirements Checklist for Choosing a Cloud Backup and Recovery Service Provider

POWERED BY Asigra.

Requirements Checklist for Choosing a Cloud Backup and Recovery Service Provider

As the importance and value of corporate data grows, complex enterprise IT environments need more sophisticated strategies for backup, recovery and restore. Cloud backup and recovery service providers can provide a wide range of support to an enterprise, from acting as experienced consultants who provide recommendations for private cloud deployment models to providing fully managed outsourced services.

Regardless of your specific IT environment, it's important to work with a service provider that has the technology and experience to adapt to new requirements as your strategy evolves.

This checklist provides a comprehensive list of critical requirements enterprises should consider in a cloud backup and recovery service provider. Use this resource as a starting point to guide your evaluation of potential vendors and to form a more detailed assessment of their capabilities.

Business Fit

Engaging with any external service provider requires a careful evaluation of its capabilities, business practices and long-term stability.

Does the service provider have:	
☐	Experience in related industries and/or business verticals
☐	Customers of a similar scale and environment as yours
☐	Experience helping with data disaster recovery under conditions seen in your business
☐	Familiarity with laws and compliance standards of your industry
☐	Testimonials and/or end user references
☐	Analyst recommendations and recognition
☐	Industry affiliations

Professional Services

A backup and recovery service provider should provide an enterprise with a wide range of professional services that offer value beyond a technology platform.

Does the service provider offer:	
☐	Audits of enterprise data to provide recommendations for cloud backup and recovery deployment models
☐	The ability to deploy a public, private or hybrid cloud
☐	24x7 support capabilities
☐	Support for backup and recovery in different geographies, time zones and user types
☐	Tiered services to manage data lifecycles including: ▪ Data segmentation of critical young data vs. older data ▪ Archive of obsolete generations, deleted data and old data ▪ Periodic copy archiving ▪ Data destruction (with certificate) ▪ Offsite replication options for additional redundancy and compliance

☐	Reports that identify: ▪ Mission-critical and non-critical data ▪ Opportunities to reduce backup window time ▪ Storage abuses before conducting costly backup ▪ Ways to increase server availability and performance
☐	A fully managed and secure backup location for backup replication and disaster recovery
☐	Managed cloud services for mobile devices such as laptops, tablets and smartphones
☐	Managed cloud services for remote office locations
☐	Self-service options for enterprise customers to reduce management costs

Cloud Architectures

Many enterprises are assessing how cloud technologies can help optimize their infrastructure and simplify data management. A backup and recovery service provider should be in a position to offer a mix of cloud deployment models to help address your current and future business requirements.

Does the service provider support:	
☐	Private cloud—owned by an enterprise and controlled and managed inside your firewall
☐	Public cloud—secure offsite data storage managed by the service provider
☐	Hybrid cloud—two or more private and public clouds that work together to enable data and application portability

Selecting a heterogeneous enterprise platform and service provider that supports a range of cloud architectures makes it possible to switch between backup deployment models as your business needs evolve. Look for a well-defined process on how to migrate from one cloud deployment style to another which can help you optimize operating expenses and capital expenditures while still preserving the recoverability of your data.

Security and Compliance

It is critical that a cloud backup service provider is able to meet the security and compliance requirements of your organization.

Does the service provider make updated documentation available that details its adherence to:	
☐	Advanced Encryption Standard (AES) 256-bit in-flight and at-rest data encryption
☐	NIST Federal Information Processing Standard (FIPS) 140-2
☐	Legislated regulatory standards for your industry (e.g. SOX, HIPAA, Basel II)

Does the service provider make available:	
☐	Business continuity plans that document an ability to continue operating as a business under extreme conditions
☐	Documented evidence of planning, preparation and drills for all contingencies including natural disasters, epidemics, labor disputes, etc.

Technology Platform

Enterprises need to closely examine the type of backup and recovery software platform a service provider uses to ensure it can meet not only the present-state requirements, but also potential future changes in its backup and recovery strategy. Here are technical requirements that an enterprise should demand in the backup and recovery platform.

Does the service provider's platform provide:	
☐	Agentless architecture to reduce complexity
☐	Ability to recover into virtual machines
☐	Support to both file-based and image-based recoveries (locally and remotely)
☐	Ability to use existing infrastructure (hardware agnostic)
☐	Ability to leverage disk-based storage (DAS, SAN or NAS)
☐	Support for virtualized environments
☐	Options for a bare metal restore
☐	Deployment as standalone or High Availability (NA) N+1 configuration
☐	Offsite replication for additional redundancy and disaster recovery
☐	Backup file validation
☐	Autonomic data healing
☐	Data reduction through deduplication and compression
☐	Incremental server backups and change block tracking

Do upgrades to the backup and recovery platform require:	
☐	End user intervention
☐	Systems re-starts
☐	Scheduled downtime

Does the backup and recovery platform support:	
☐	Servers
☐	Virtual machines
☐	Desktops
☐	Laptops
☐	Tablets
☐	Smartphones
☐	Remote offices
☐	Cloud-based applications such as Salesforce, Google Apps, etc.

Does the backup and recovery platform support the following systems:	
☐	Your company's line of business and custom applications
☐	VMware
☐	XenServer
☐	Hyper-V
☐	MS SharePoint
☐	MS Exchange
☐	MS Outlook
☐	MS SQL Server
☐	Oracle
☐	DB2
☐	PostgreSQL
☐	Sybase
☐	Lotus Notes and Domino
☐	GroupWise
☐	MySQL
☐	Windows
☐	Linux
☐	Unix
☐	NovellNetware
☐	Mac OSX
☐	System i
☐	Apple iOS
☐	Android

Disaster Recovery

You don't want to wait until a crisis occurs to learn whether your backup and recovery service provider is ready to help you weather the storm. Here are several key indicators that a backup and recovery vendor is adequately prepared for disaster recovery.

Does the service provider demonstrate:	
☐	Regular auditable recovery tests with simulated drills to ensure Recovery Point Objectives and Recovery Time Objectives can be exceeded
☐	Key recovery and restoration processes and milestones based on multiple scenarios
☐	Tiered recovery of most critical data first
☐	At least one redundant data center in a geographic location unlikely to be affected by a common natural disaster
☐	Ability to perform automatic failover to a redundant data center with replicated data
☐	Identical security measures enforced at redundant data center(s)

Service Level Agreement

Always read the fine print in your Service Level Agreements (SLAs)—it is the blueprint for the contractual service responsibilities of your service provider. In the case of backup and recovery SLAs, there are some key aspects to carefully review.

Does the SLA include:	
☐	Specific penalties or credits for failure to meet the SLA
☐	Information on how non-performance on the SLA outside of a data disaster is measured
☐	Negotiable RTOs and RPOs that can adjust based on changes in your organization's business impact analysis and continuity plan
☐	Different pricing options for different types of data (standard pricing for critical or young data required for daily business operations, and lower pricing for archival or older data stored for regulatory compliance)
☐	Clear language that describes an organized transition out of the contract if you want to change service providers, including what the service provider must do to help you, and what are your obligations
☐	Identical security measures enforced at redundant data center(s)

To find out more about our solution, visit our website or call us today.

POWERED BY Asigra.