T: 0844 247 2 327 E: info@fantasticcs.co.uk

FANTASTIC Cloud Services

Cloud Backup, Disaster Recovery and Business Continuity provider.

What You Need to Know About Cloud Backup and Disaster Recovery:

Your Guide to Cost, Security, and Flexibility

Disaster Recovery Planning & Infrastructure

Fantastic Cloud Services

POWERED BY Asigra.

White paper: What You Need to Know About Cloud Backup and Disaster Recovery:
Your Guide to Cost, Security, and Flexibility

Over the last decade, cloud backup, recovery and restore options have emerged as a secure, cost-effective and reliable method of safeguarding the increasing amounts of corporate information being generated daily, especially with regards to recovery. But switching to a cloud-based backup system is a significant decision that requires a clear understanding of how such a solution will integrate into your business. This document addresses the most common questions that companies are asking about cloud backup and will help you determine what role a cloud backup and disaster recovery solution can have in your business.

Section A: Exploring the Cloud.

What does public, private and hybrid cloud actually mean?

Distinguishing between various cloud models will help you better determine the type of backup system that your organisation requires. A public cloud is a managed solution that involves an off-site data centre to provide flexibility and scalability for compute and storage needs. A private cloud occurs when a company builds and manages its own data centre that operates behind a corporate firewall. A hybrid cloud offers a mixed approach to infrastructure that links together two unique data centres, one private and the other public.

The type of cloud deployment you are considering can impact your backup and disaster recovery solution. With a public cloud, your backup solution should optimize data capture and storage in order to help minimize bandwidth demands on the corporate network. A public cloud backup solution will typically require the services of a cloud backup service provider that can supply both the infrastructure and the necessary backup and disaster recovery software and operational skills/expertise.

With either a private or hybrid cloud, you might require a cloud backup service provider in order to provide your company with the necessary software platform to manage backups in your private cloud. In the case of a hybrid cloud, your company will have the option of switching between a private data centre and a cloud based storage option depending on your backup needs.

What are the common steps required to implement a cloud backup and disaster recovery solution?

Each cloud backup implementation is unique, as it takes into consideration the particular data protection needs of your organisation. These can include remote offices, laptops and mobile devices such as tablets and smartphones. Any complications involved in moving to an outsourced cloud backup service can be mitigated by selecting the right cloud backup service provider who provides a solution that is hardware and software agnostic enabling you to leverage your existing infrastructure. Engaging with the right service provider will provide you with the guaranteed seamless implementation and ongoing support you require. Outsourcing mundane backup processes to a proven cloud backup expert will enable you to re-deploy existing IT resources to more strategic revenue generating initiatives.

Your cloud backup service provider will be able to guide you through the implementation process and provide dedicated support to help you calibrate and optimize your backup solution for you. To plan for disaster recovery you will need to consider the impact of losing critical business applications and data for a given time frame and analyse the acceptable risk levels and costs to business operations associated. The good news is that once your private cloud backup and recovery solution is in place, it will require minimal maintenance as compared with on-site solutions such as tape backup.

Given the central role that data plays in your organisation, it's critical that your cloud backup service provider has proven expertise in delivering a trusted cloud backup solution. A thoroughly tested implementation will provide your company with assurance that a cloud backup solution will not fail when it is most needed.

Why cloud backup and disaster recovery?

A cloud backup, recovery and restore solution provides you with a cost effective, secure and reliable method of recovering and restoring data — the lifeblood of your business. The system restores data regardless of your location, including individual files in their native format so you can resume business operations immediately. It also provides you with a flexible solution that scales as your storage capacity needs evolve as your business grows.

FANTASTIC
Cloud Services

How does data recovery typically operate with a cloud model?

Two key factors in understanding data recovery are Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). RTO refers to how quickly your business needs to be able to recover after losing data and can be measured in hours or days. RPO refers to how much data your company can afford to lose as measured in hours. So, for example, a Fortune 500 company for some types of data might require an RTO of five hours and an RPO of an hour. The RPO and RTO may vary for different types of data.

Every business needs to determine an RTO and RPO based on their own calculations of risk tolerance and business continuity requirements. As part of this process, it's important to take a hard look at the type of data your company collects and uses on an hourly, daily or weekly basis. Many companies fail to realise how important a fast recovery is to achieving their business objectives — until they experience a serious data loss or IT service outage.

The impact of a data loss or outage event can be significant. A retail operation, for example, is constantly collecting data in order to perform analytics related to pricing strategies, inventory supply and peak periods of demand. This real-time data is essential to remaining competitive.

Many companies can no longer afford to rely on a truck arriving each day to take backup tapes offsite because it potentially puts at risk a full day's worth of valuable competitive business data.

Section B: Understanding Security With Cloud Backups

How can I ensure my availability requirements are being met when my company data is being stored offsite in a cloud?

Your company will continue to assume liability for data security, even when shifting backup responsibility to a cloud backup service provider. You should expect that your service provider enables you to continue to keep a local copy of your most recent backups in case you get disconnected from the cloud. Your cloud backup service provider will also need to demonstrate that it has multiple data centres in order to ensure your data will be protected by an appropriate amount of infrastructure redundancy.

These data centres should also be geographically diverse in order to increase reliability in case of a natural disaster or power outage. Along with a disaster recovery plan for your business too, your service provider should also be able to demonstrate a Business Continuity Plan that outlines how it will handle a variety of contingencies.

How does a cloud backup system guarantee data is being transferred securely?

After selecting files, your cloud backup software platform deduplicates and compresses data in order to reduce transfer time. It is then encrypted at your site before transmission, and during transmission to your cloud backup and disaster recovery service provider, where it remains encrypted. The only key for decryption resides with you, ensuring that the off-premise (cloud) backup and recovery solution is as safe and secure as an on-premise data backup and recovery system.

Since your company data will be transferred via the Internet, the encryption standard used by a service provider is of critical importance. Your service provider should be using the Advanced Encryption Standard (AES) along with FIPS 140-2 certification, which provides third-party validation from the National Institute of Standards and Technology (NIST). FIPS 140-2 is the highest level of trusted third party certification available and indicates that the encryption has been implemented correctly in a way which cannot be defeated.

What assurances do I need to look for to ensure a reliable cloud backup service?

Your company must perform due diligence to ensure your cloud backup service provider will meet your business needs. Basic questions include: how much experience in the industry does the service provider have and have they provided backup services to companies that are similar to yours in terms of vertical market, size and scope. Depending on your compliance requirements, your cloud backup service provider should be familiar with relevant industry terminology and standards that impact your business.

One of the most common methods of ensuring that your expectations are met is through a strong Service Level Agreement (SLA). This document will outline your desired operational levels and describe the consequences if the SLA is not met. Your SLA should also provide you with the assurance that your cloud backup service provider is a credible, trusted business partner who holds certifications that enable you to maintain compliance requirements.

Along with an SLA, your chosen service provider should make allowances for a termination agreement. A cloud backup service provider that locks you into a long-term contract has less motivation to offer high levels of customer support than a vendor that must face periodic service renewals. Don't get locked into any cloud or cloud backup service provider. Your cloud backup service provider should provide you with the flexibility to move from a private or hybrid cloud to a public cloud deployment should your business needs change over time. Also, your cloud backup service provider is only the custodian of your data, you own and control your data. The service provider is obligated to provide reasonable access to your data with assistance to migrate your data elsewhere should you need to. For example, if you want to move your money from one bank to another, there is no lock in and no penalty for moving your assets elsewhere. The same circumstances should apply with your cloud backup service provider.

Section C: The Cost and Ongoing Operations of Cloud Backups

What level of IT resources will be required to setup and maintain a cloud backup solution?

For most companies, a cloud backup and recovery solution will eliminate, or significantly reduce, IT resources related to the mundane task of backup and disaster recovery and allow your resources to be redeployed to more strategic projects. Working with a trusted cloud backup service provider enables you to leverage your existing network infrastructure while transferring the responsibility of backup to an outside expert. This can be even more important considering the challenges some companies are facing hiring experienced IT backup administrators for on-premise solutions especially in smaller cities or remote geographies. It also enables CIOs to focus on spearheading significant transformational projects rather than backup implementation, which typically has a lower prestige value within most organisations.

Once you determine the appropriate settings, backups are automated, creating a "set-it and-forget-it" scenario. You will however, need to ensure that your cloud backup service provider is equipped to monitor your backups to identify and correct any possible problems. The price of your backup service will reflect the amount of responsibility you maintain versus your cloud backup service provider. Low cost service offerings could mean that you will be provided with marginal support, minimal senior technical resources and the ongoing burden for monitoring and managing your backups.

How is my data stored in the cloud?

Not all data is created equal therefore your cloud backup service provider will work with you to take a comprehensive approach to reviewing, assessing and classifying your data to gain a better understanding of your business needs and your recovery time objectives for your young versus old data. Your cloud backup service provider should understand that organisations don't value older data the same as younger, more critical data. Operationally critical data requires more frequent backups with a better SLA. Less critical backups are relegated to less expensive, lower SLA standards to save costs. In most companies, more than 50% of data is older, of less value, and should cost less to protect. Your service provider should help you to align the value of your data with the cost of protecting it.

Other pertinent questions to consider are the physical locations, resilience, security and the quality standards of the data centre. It is important to ensure that your provider is using data centres that meet ISO 9001 quality standards. Your chosen data centre should also be designed to Tier 3 standards to offer a high level of uptime, with appropriate security levels in place such as biometric systems and authentication protocols.

It appears as though a monthly subscription fee for cloud backups is equivalent to implementing a traditional tape backup system. Is this true?

Comparing the cost of a cloud backup solution against an equivalent tape system can be a tricky calculation. The best way to approach the issue is to consider total cost of ownership for both systems.

To determine the total cost for a tape backup system you will need to consider:

- Hardware
- Software
- Ongoing maintenance for both hardware and software
- Initial setup costs for configuration
- Time and resources for managing backup and restore, including periodic recovery drills
- Future scalability and costs of additional infrastructure

For a cloud-based backup service, costs to consider include:

- Recoverability assessment
- Initial implementation
- Pay-per-use for capacity

Your cloud backup service provider should have access to a ROI calculator that you can use to determine the cost savings over a multi-year period of a cloud backup and recovery solution as compared with an on-premise system. Many companies will discover that the total cost of ownership for a cloud backup and recovery system is significantly lower.

Along with total cost of ownership, there are other associated financial advantages of a cloud backup service including:

- Lower operating and administrative costs due to automated backups
- Built-in scalability which makes it easy to evolve with new business needs
- Cloud backup software that scans your data for integrity or corruption issues and alerts your company immediately, preventing costly problems in advance
- Deployment of IT resources in more strategic innovative initiatives that enable greater competitive advantages
- Simple disaster recovery drills for peace of mind

Why cloud backup and disaster recovery?

These answers should provide a better picture of what the switch to a cloud backup, recovery and restore solution involves. Given the reliability, affordability, security and manageability associated with cloud backup, many companies are now moving to the cloud. The reasons include:

- **Ability to leverage existing infrastructure** — a cloud backup and disaster recovery solution doesn't require buying or installing expensive equipment as it takes advantage of your existing corporate network
- **Set it and forget it** — once you select a backup schedule, company data is saved automatically, providing a transparent solution
- **Tape backup shortcomings** — tape backups are often expensive, vulnerable to obsolescence and can be lost or stolen when being transported off-site
- **Improved recovery time objectives** — by using a managed backup service, the speed and reliability of your recovery and restore will be governed through your SLA
- **Smarter use of IT resources** — a cloud backup and disaster recovery solution will allow your business to redirect IT resources to more pressing challenges within your organisation
- **Backup Lifecycle Management** — a cloud backup and disaster recovery solution aligns the value of your data with the cost of protecting it. As the value of your data declines over time the cost of protecting it also declines providing you with additional cost savings.
- **Enable offsite recovery of IT systems** – utilising software with dependable cloud infrastructure in high quality data centres enables business to bring not just data, but full IT systems, back online very quickly without the need or cost of in house resources

Section D: Disaster Recovery In the Cloud

In addition to the utilising the cloud to back up business data and applications, service providers should also be able to offer Disaster Recovery as a Service (DRaaS). As the service providers have data backed up it makes sense that they can offer Disaster Recovery using cloud based technology solutions.

Analysts Gartner expect that by 2018 the number of organisations utilising DRaaS will exceed the number of organisations using traditional recovery systems. As an immature market, the requirements that organisations have for DRaaS typically revolve around post disaster recovery operations, but there is an evolving requirement to selectively fail over production applications into the cloud in order to support IT service continuity.

When considering service providers that will utilise cloud solutions to provide disaster recovery, you should be considering;

- Can the service be easily scaled to include DRaaS
- What degree of downtime can your organisation tolerate
- What would be the financial risk of not being able to recover from disaster
- Does my IT infrastructure align with a DRaaS platform
- One provider for your cloud backup and DRaaS solution means you requirements are met by one trusted provider maintaining security and simplicity