



Overcoming 7 Cloud Misconceptions in Financial Services



Introduction

While financial services firms' core offerings like investments, insurance, loans, and banking have remained relatively unchanged since the start of the industry centuries ago, the way they're delivered has evolved significantly. Companies adopted digital methods that allow customers, vendors, and partners to handle onboarding, transactions, and other needs online—which drastically changed customer expectations.

The shift to digital allows financial service firms to serve more clients, vendors, and partners without expanding physical locations or adding staff. But not all financial services organizations have modernized, and for those that have, continuous improvements are necessary to keep pace with technology and customers' changing expectations.

Technology advancements and cultural shifts continue to increase the amount and complexity of data. As a result, financial services firms need scalable, secure, and cost-effective data storage solutions.

Cloud storage offers numerous advantages over traditional on-premises storage. However, misconceptions about cloud technologies prevent many financial institutions from fully embracing its potential.

This whitepaper aims to dispel these myths and provide a clear understanding of the benefits of cloud storage in the financial services industry. By addressing common concerns, including security, reliability, and cost, we hope to enable IT, operations, and compliance professionals to confidently navigate cloud adoption and seize its growth opportunities.

1. Cloud Storage Is Less Secure Than On-Premises

A common misconception among financial services firms is that cloud storage is less secure than on-premises solutions. This stems from the concern around data privacy, with the perception that multi-tenant environments lead to the co-mingling of data and an elevated risk of data breaches. What it doesn't consider are the cloud providers' advanced security measures that not only prevent co-mingling, but also proactively monitor and protect their customers' sensitive data.

These include:

- **Data and network security:** Advanced network security controls, such as firewalls and authentication and access controls isolate data among tenants, and intrusion detection systems, data loss prevention (DLP), and encryption protect data at rest and in transit.
- **Physical security:** Protecting data centers with advanced physical security measures, such as surveillance, access controls, and environmental monitoring.
- **Security standards:** These include meeting stringent cybersecurity standards like ISO-27001 for information security management systems.

Many cloud providers offer more advanced security than on-premises environments, especially considering the significant funds they can allocate. In fact, a study by the World Economic Forum found that 95% of cloud security breaches are caused by user error, not cloud provider vulnerabilities.¹

Even though there's proof that cloud storage is secure, there are several steps that financial services firms should take to improve their overall security posture:

- **Evaluate cloud providers:** Carefully assess potential cloud providers' security measures and certifications to ensure they meet requirements.
- **Implement strong security controls:** Establish and enforce security policies and procedures, including access controls, encryption, and data loss prevention.
- **Regularly assess and monitor security:** Conduct regular security assessments and audits to identify and address potential vulnerabilities.
- **Leverage cloud provider security features:** Take advantage of the security features offered by cloud providers, such as encryption, breach reporting, multifactor authentication, and compliance certifications.

By leveraging the security features inherent in the leading cloud solutions and proactively adopting company procedures to improve data security, financial firms can confidently adopt cloud-based solutions, bolstering their security posture rather than diminishing it.

¹https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

2. Cloud Storage Isn't Compliant With Regulations

Along with security concerns, financial firms need to consider regulatory compliance when evaluating new technologies.

Financial services companies have strict data privacy and sovereignty requirements, with the potential for regulatory fines and business disruptions if regulations aren't followed. According to a study by Google Cloud, over 88% of financial services firms believe the cloud will assist with business operations. However, 78% say that regulatory uncertainty over the use of public cloud prevents their organizations from adopting cloud technologies.²

Regulators updated data privacy guidance and mandates for data privacy and security, giving regulated firms explicit direction and confidence for implementing new technology solutions. In addition, cloud providers that support the financial services industry have invested heavily to support compliance with various regulatory frameworks.

These include regulations like:

- **PCI DSS:** The Payment Card Industry Data Security Standard sets standards for cardholder data security.
- **SEC 17a-4:** This Securities and Exchange Commission (SEC) rule requires broker-dealers to maintain records in a non-erasable, non-rewriteable format.
- **FINRA Rule 4511:** The Financial Industry Regulatory Authority (FINRA) rule requires member firms to maintain electronic records for a specified period.
- **HIPAA:** The Health Insurance Portability and Accountability Act sets standards for the privacy and security of protected health information (PHI).
- **GDPR:** The General Data Protection Regulation sets standards for protecting personal data in the European Union.

In addition to building solutions that comply with industry regulations, cloud providers often conduct regular audits to ensure they keep up with changing mandates. They also offer data sovereignty features that help organizations comply with data residency laws. These capabilities support financial services firms in meeting stringent regulatory requirements, enabling secure and compliant adoption of cloud technologies.

²<https://cloud.google.com/blog/topics/inside-google-cloud/new-study-shows-cloud-adoption-increasing-in-financial-services>

3. Cloud Storage Limits Control and Visibility

In an industry that handles the most sensitive and sought-after data, it makes sense that regulators address governance requirements to control, monitor, and report on access. Even firms with less specific mandates seek to ensure proper access control and visibility to limit vulnerabilities.

The result is that IT and compliance professionals worry about giving up control and losing data visibility when moving from on-premises to the cloud. There's a certain amount of comfort for IT professionals to walk into a server room and know all of their data is there. However, that proximity also comes with risks. Many IT professionals can tell horror stories, their own or others, of fires, natural disasters, air conditioning units failing, and more, that have brought down entire operations for days. Remote site disaster recovery sites are an option, but that can lead to excessive up-front and recurring costs (more on that in Misconception 6).

Additionally, on-premises servers only allow for controlling data in that environment. Control is lost after documents or data are sent outside the organization and, to a certain extent, even after they're downloaded onto an individual's computer.

Cloud providers not only control data within their system, they can expand control and visibility to files shared outside an organization, including notifications, version control, and even removing access.

The cloud natively provides more detailed, automated data access and governance controls, such as:

- **Access controls:** Dynamic and more granular access controls that can be defined and applied based on conditions such as time, device, IP address, and user behavior through cloud-native identity and access management (IAM) tools.
- **Data classification:** Automated and integrated with cloud services to classify and tag data based on predefined rules or AI/ML models.
- **Data retention:** Native data lifecycle management tools that automate data retention policies based on time, access patterns, or compliance requirements.
- **Monitoring and reporting:** Advanced capabilities with real-time monitoring and alerts, including detailed logs and automated user and service activity analysis.
- **Native and API access:** Easier integration with external systems and support for hybrid and remote workforces with the ability to dynamically manage access policies based on changing conditions and environments.

While some of this functionality is capable on-premises, it requires additional third-party tools that add complexity, cost, and management.

In order to maximize their data governance without enacting so many controls that slow down the business, organizations should:

- **Evaluate features:** Conduct a needs analysis and verify potential cloud providers' control and visibility features to ensure they meet needs.
- **Implement strong governance policies:** Establish and enforce data governance policies to facilitate.
- **Leverage tools:** Take advantage of the control and visibility tools offered by cloud providers, such as access controls, monitoring, and reporting.

Concerns about losing control and visibility when moving to the cloud are understandable, especially in the highly regulated financial services industry. However, modern cloud solutions maintain and often enhance these capabilities through granular access controls, comprehensive governance tools, and advanced monitoring features.

4. Cloud Storage Lacks Flexibility and Scalability

Financial services firms' data storage needs constantly evolve due to regulatory changes, market growth, and the increasing volume of financial transactions. As a result, they worry about the flexibility and scalability of cloud storage solutions, whether due to vendor lock-in, the ability to integrate with existing systems, or concerns about accommodating accelerated growth periods.

However, with multiple storage options, hybrid and multi-cloud capabilities, and the ability to expand storage capacity, cloud solutions can replicate an on-premises experience and exceed the experience of expanding capacity and locations.

Many cloud providers support mix-and-match storage options, allowing a customized solution to suit a company's needs. For instance:

- **Storage for all data types:** This includes object storage for large volumes of unstructured data, like images and videos, block storage for structured data such as databases and applications, and file storage for organizing files and folders in a traditional format.
- **Hybrid cloud solutions:** These combine on-premises and cloud-based infrastructure, allowing organizations to maintain legacy systems on-premises while leveraging cloud-based storage for new applications or data.

This flexibility helps provide fast access to critical files. Because cloud storage doesn't depend on a company's hardware, it allows organizations to quickly scale up or down based on changing business needs. In fact, a study by McKinsey found that cloud-based applications can be scaled up or down by up to 100% within hours, while traditional on-premises infrastructure can take weeks or even months to scale.³

While flexibility and scalability are inherent in cloud storage solutions, there are several considerations companies can take to optimize their performance, including:

- **Architecture:** Design an architecture that may include hybrid or multi-cloud environments that support adding or removing storage capacity as needed.
- **Tools:** Use autoscaling and right-sizing tools to allocate resources and optimize performance dynamically.
- **Forecast:** Leverage predictive analytics to forecast storage needs and proactively adjust capacity.

Flexible cloud solutions allow firms to adapt to new requirements quickly. At the same time, scalable storage ensures they can handle large data spikes, optimize costs, and maintain performance without constant infrastructure upgrades.

5. Cloud Storage Isn't Reliable

Many financial services firms are required by their regulators to have business continuity plans to maintain operations no matter what happens. Even those not mandated by regulation require system reliability to sustain business operations and provide the highest levels of customer service. Given these pressures, it's no wonder that companies are concerned with data loss and service disruptions.

Fortunately, cloud providers invest heavily, well beyond what an individual firm could allocate, in reliability and redundancy to ensure the availability and integrity of data, including:

- **Data replication and redundant infrastructure:** Replicating data and hardware across and within multiple data centers to protect against data loss and downtime.
- **Access optimization:** Edge computing solutions and block caching for fast file access across global IT infrastructures.

³<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization>

- **Disaster recovery:** Implementing strong disaster recovery plans to ensure business continuity in the event of a service disruption.
- **Monitoring and maintenance:** Continuously monitoring and maintaining the cloud infrastructure to ensure optimal performance and reliability.

Through their service level agreements (SLAs), cloud solutions give financial services organizations confidence in business continuity with a certain level of availability and performance. For example, Google Cloud Platform offers a 99.99% uptime for its storage services.⁴

While almost all providers offer SLAs, they don't all provide the same guarantees. As part of any cloud solution search, firms should:

- **Evaluate cloud provider reliability:** Review reliability features and SLAs to ensure they align with operational expectations.
- **Design a resilient architecture:** Develop a resilient and fault-tolerant cloud storage architecture that minimizes the impact of service disruptions.
- **Leverage features:** Take advantage of the advanced reliability features offered by cloud providers, such as data replication and disaster recovery.
- **Monitor and test reliability:** Regularly monitor and test the reliability of cloud storage solutions to identify and address potential issues.

These features, backed by service level agreements (SLAs), give financial organizations the confidence to maintain operations even during disruptions, ensuring data availability and business resilience.

6. Cloud Storage Is Too Expensive

Concerns about recurring subscription costs, overprovisioning resources, hidden costs, and complex pricing models have led many professionals to consider cloud storage too expensive compared to on-premises solutions. However, when examining the total cost of ownership (TCO) for on-premises solutions, including investments such as hardware and software, maintenance and resources, and energy costs, many organizations find cloud solutions comparable to or less expensive than on-premises solutions.

⁴<https://cloud.google.com/compute/sla>

Most cloud storage solutions offer a flexible, cost-effective pricing model with minimal upfront investment and predictable growth costs. Cloud providers often offer pay-as-you-go pricing models with incremental storage expansion. This eliminates the need for upfront capital expenditures and reduces the TCO.

A few benefits of the cloud to keep in mind:

- **Scalability:** The ability to scale storage capacity up or down as needed can help organizations avoid overprovisioning and reduce costs.
- **Efficiency:** Cloud providers often have more efficient data centers and storage technologies, which can lead to lower energy costs passed along to customers.
- **Reduced management overhead:** Cloud providers manage the underlying infrastructure, which can reduce the need for in-house IT staff and associated costs.

To ensure that cloud storage is cost-effective, financial services organizations should consider the following steps:

- **Conduct a TCO Analysis:** Compare the total cost of ownership of cloud storage to on-premises storage solutions to identify the most cost-effective option.
- **Negotiate:** While some cloud providers may try to convince otherwise, companies can negotiate pricing and terms, especially for larger deployments.
- **Monitor and manage expenses:** Regularly monitor and manage cloud storage costs to identify areas for optimization and cost reduction.

With the right approach and proper management, many financial services organizations can realize cost parity or even savings versus their current on-premises solution. The 2023 Business Value Report from Egnyte found that companies had an annual savings and value of \$130,000 moving from on-premises to the cloud.⁵

7. Moving to the Cloud Is Too Complex

Many IT departments rely on small teams and limited resources, making moving to the cloud seem too complex or time-consuming. They worry about the technical challenges involved in migration, the potential for disruption to business operations, and the need for significant organizational changes.

⁵https://www.egnyte.com/sites/default/files/2024-05/2023_Business_Value_Report-Final.pdf

While it's inaccurate to say cloud migration requires no work, it's far from daunting. Cloud providers offer a range of offerings to simplify migration, such as:

- **Migration tools:** Automated tools to help organizations migrate data and applications to the cloud.
- **Professional services:** Expert consulting and implementation services to assist organizations with the migration process.
- **Partnerships:** Partnerships with technology vendors to provide comprehensive migration solutions.

Furthermore, cloud providers often offer phased migration approaches, which can help organizations minimize disruption to business operations and reduce the overall complexity of the migration process. To ensure a smooth and efficient cloud migration, financial services organizations should:

- **Assess migration readiness:** Conduct a thorough assessment of organizational readiness for cloud migration, including technical, managerial, and business factors.
- **Develop a migration plan:** Create a detailed plan outlining the scope, timeline, and resources required for the migration process.
- **Leverage cloud provider tools and services:** Take advantage of the tools and services offered by cloud providers to simplify the migration process.
- **Conduct pilot migrations:** Conduct pilot migrations to test the migration process and identify potential challenges.
- **Provide adequate training and support:** Ensure staff has the necessary training and support to migrate to the cloud successfully.

These resources simplify the process, minimize operational disruption, and reduce the strain on IT teams, allowing firms to transition smoothly and efficiently to the cloud while maintaining business continuity.

Egnyte: A Trusted Partner for Cloud Storage

Trusted by over 2,200 financial services industry firms worldwide, Egnyte is a hybrid/multi-cloud storage, security, and governance platform that enables firms to deliver more value for their customers, reduce risk, and respond to evolving business needs. The platform is purpose-built with the financial services industry in mind and addresses all financial services firms' concerns with cloud adoption and optimization.

Security

Egnyte enhances security beyond traditional on-premises solutions with advanced encryption, access controls, and real-time monitoring and auditing. The platform meets stringent compliance standards like ISO 27001 and PCI DSS, offering robust security for data at rest and in transit. These capabilities help protect against breaches while ensuring organizations maintain control of sensitive information.

Regulatory Compliance

The platform is built to comply with industry-specific regulations, including FINRA, SEC 17a-4, GDPR, and more. It provides the governance needed for regulatory compliance, including tools to manage data residency, audit trails, and records retention. With regular audits and compliance reporting, Egnyte makes it easier for financial services firms to meet their regulatory obligations.

Control and Visibility

Through capabilities like tracking and detailed reporting on data sharing, even outside of an organization, Egnyte offers granular control over file access. Its integrated access controls and monitoring tools across hybrid and multi-cloud environments enable full visibility into user activity and ensure compliance with governance policies. The platform also supports secure, centralized data governance for seamless management and visibility.

Flexibility and Scalability

Egnyte supports hybrid and multi-cloud architectures, allowing firms to maintain legacy systems on-premises while seamlessly scaling storage in the cloud as needed. With support for multiple data types and integration with existing systems, Egnyte enables financial services firms to adjust to rapid growth or fluctuating demand without sacrificing performance.

Cloud Reliability

Data replication, redundancy, and disaster recovery protocols ensure a highly reliable cloud solution with a 99.99% uptime guarantee to support business continuity.

Cost

The cost-effective, pay-as-you-go model offered by Egnyte reduces upfront infrastructure investments and scales as an organization grows. By eliminating the need for costly hardware, energy, and in-house IT resources, Egnyte can help reduce the total cost of ownership. Its efficient management tools help firms optimize storage costs and avoid overprovisioning.

Ease of Adoption

Egnyte simplifies cloud migration with an easy-to-adopt platform supported by professional services, automated migration tools, and expert guidance. This allows firms to move their data securely and efficiently, and the familiar letter-drive experience with desktop, web, and mobile access seamlessly integrates into existing business processes. Egnyte supports phased migration to minimize disruption, offering training and support to ensure a smooth transition.

By integrating robust security with operational efficiency, Egnyte empowers financial services organizations to navigate the complexities of today's digital landscape confidently on any device, anywhere.



Conclusion

Cloud storage represents a transformative opportunity for financial services organizations, including cost savings, enhanced security, and ease of compliance with regulations. By overcoming the seven cloud misconceptions and leveraging the benefits outlined in this whitepaper, firms can unlock new possibilities, improve efficiency, and drive innovation, positioning themselves for long-term success into the next century of the industry and the technology advancements it brings.

[CHAT WITH SPECIALIST](#)



Egnyte combines the power of cloud content management, data security, and AI into one intelligent content platform. More than 22,000 customers trust Egnyte to improve employee productivity, automate business processes, and safeguard critical data, in addition to offering specialized content intelligence and automation solutions across industries, including architecture, engineering, and construction (AEC), life sciences, and financial services. For more information, visit [www.egnyte.com](#).

Contact Us

US: 1-877-734-6983
EMEA-UK: +44.20.3356.3714
www.egnyte.com