



Navigating Cloud Risks in the Transformation of Financial Institutions



Introduction

In the last ten years, U.S.-based financial institutions have undergone a remarkable transformation by embracing cloud technologies. This shift, propelled by the COVID-19 pandemic, remote work trends, and evolving customer expectations, has not only streamlined operations but also reduced operational costs significantly. The cloud has become an integral part of how these institutions manage data, interact with customers, launch digital products, and bridge the gaps between previously isolated data silos created by on-premises technologies.

By 2030, the global cloud market for the financial sector is projected to surpass \$101 billion. This surge is driven by the urgent need for digital services and rapid product innovation. For instance, it's estimated that by the end of 2024, over 30% of banks with assets exceeding \$1 billion will introduce banking-as-a-service (BaaS) to bolster their revenue streams.

Big tech companies play a pivotal role in driving the adoption of cloud services within the banking and financial sector, especially concerning infrastructure. Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) dominate the market. Interestingly, many financial institutions opt to use multiple cloud providers simultaneously. Reports indicate that 45% of financial institutions prefer AWS as their primary provider, with Azure closely trailing.



The reality is financial institutions may never make significant progress across the cloud — or reap its benefits — without ensuring they have proper cloud risk and compliance controls in place.

Across the industry, financial institutions are increasingly relying on cloud services for various functions, from collaboration and office applications to sales, marketing, and human resources. Yet, the majority are still in the early stages of migrating their workloads, leaving ample room for acceleration and improvement in cloud enablement.

However, the adoption of cloud computing has brought along a new wave of risks, particularly for organizations operating in hybrid environments or using traditional on-premises security measures that are ill-suited for the cloud. Coupled with the use of disparate systems, most financial institutions have struggled to gain comprehensive insight across the entire enterprise to identify, assess, mitigate, and manage cloud risks effectively or facilitate secure and compliant cloud adoption.

One of the key factors hindering progress in cloud adoption is the complexity of understanding cloud risks and implementing appropriate controls. Furthermore, the dense regulatory landscape, privacy issues, and data sovereignty challenges add to the industry's hesitation. Financial institutions must recognize that proper cloud risk and compliance controls are indispensable for them to realize the full potential of the cloud and navigate these challenges effectively.

Critical Cloud Risks

Understanding and mitigating cloud risks is critical. All cloud-based resources and services must have proper controls in place to safeguard your data and operations. The following are key cloud risks that should be evaluated on an ongoing basis, as these may change over time due to the dynamic nature of cloud environments:

- **Data Loss and Recovery Risk:** Financial institutions are vulnerable to the loss of crucial data and may encounter difficulties in recovering it following an incident.
- **Sensitive Data Exposure:** There is a significant threat of sensitive information being exposed, potentially jeopardizing confidentiality and privacy standards.
- **Configuration Vulnerabilities:** Improperly configured cloud services can introduce vulnerabilities, expanding the potential attack surface for cyber threats.
- **Unauthorized Access:** Financial institutions run the risk of unauthorized individuals gaining access to valuable resources and data within their cloud infrastructure.
- **Network Breaches and Unauthorized Access:** Weak network security can lead to unauthorized access and data breaches, posing significant security concerns.
- **Financial Risks and Cost Overruns:** Unforeseen cost overruns and financial challenges can arise within cloud environments, posing additional risks to financial institutions' operations and budgets.

Increased Industry Regulations

The digital transformation of financial services has not occurred without its share of regulatory hurdles. As financial institutions embrace cloud technologies, the regulatory landscape governing cloud services has evolved in tandem. Regulatory bodies,



such as the U.S. Department of Treasury and the Financial Banking Infrastructure Committee (FBIC), have highlighted key challenges, emphasizing the importance of repeatable risk management processes and effective cloud controls.

Furthermore, agencies like the Office of the Comptroller of the Currency and the Federal Financial Institutions Examination Council (FFIEC) have issued joint statements emphasizing the need for a clear division of responsibilities and risk management best practices in cloud computing environments. Financial institutions are also subject to other industry-specific regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and guidelines from the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC).

State and federal requirements are continually evolving. Regulations like the [Gramm-Leach-Bliley Act \(GLBA\)](#) and the [Sarbanes-Oxley Act \(SOX\)](#) at the federal level, and the [New York Department of Financial Services \(NYDFS\) Cybersecurity Regulation](#) and the [California Consumer Privacy Act \(CCPA\)](#) at the state level, mandate specific standards for cloud data protection, incident response, and customer privacy.

These regulations go beyond mere compliance requirements; they help institutions select and configure cloud offerings in alignment with their risk appetite, ultimately leading to increased profitability.

Common Cloud Risk and Controls Challenges

To realize the benefits of cloud adoption, financial institutions must effectively navigate cloud regulations and reduce risk. Many have yet to adopt a proactive approach to cloud risk management, struggling to understand how to implement adequate controls and establish proper cloud governance processes.

One significant obstacle is the complexity of security and compliance in cloud environments, exacerbated by the dynamic nature of cloud services and the differing security models and compliance requirements of various cloud providers. This complexity is further compounded in multi-cloud or hybrid cloud environments, where a shared responsibility model adds another layer of confusion.

Another challenge lies in the shortage of skilled professionals who understand cloud technologies, security practices, and compliance standards. This scarcity is particularly acute in heavily-regulated industries like banking, where expertise in IT and security is often lacking.

Cloud sprawl is another common issue. Different departments or teams within financial institutions often provision cloud services independently, leading to decentralized resources that are challenging to track. This can result in potential security vulnerabilities, compliance problems, and increased costs.

Disparate cloud services also create siloed data, diminishing an organization's visibility into cloud risk and complicating data governance and privacy efforts. The expanding attack surface further increases the complexity of risk management.

Lastly, legacy risk management practices designed for on-premises environments often fall short when applied to the cloud. These practices rarely align with industry-recognized best practices and frameworks, leaving institutions exposed to risks.

Effective Cloud Risk and Controls Benefits

Despite these challenges, the benefits of cloud adoption outweigh the risks:

Greater Flexibility and Usage: Cloud adoption provides access to industry-leading capabilities like databases and AI, enabling enterprises to become more resilient, secure, and efficient.

Acceleration: Cloud adoption accelerates innovation and growth.

Risk Management: Effective cloud risk management identifies and mitigates risks, enhancing operational resilience.

Enhanced Security: Robust cloud controls protect sensitive data and critical resources from unauthorized access and cyber threats.

Regulatory Compliance: Implementing cloud controls ensures regulatory compliance, reducing the risk of non-compliance fines and legal consequences.

Cost Optimization: Cloud controls optimize cloud resources, resulting in cost savings.

Capital One was founded on the belief that the banking industry would be revolutionized by technology. That by pairing the tech prowess of leading tech companies with the risk management skills of a leading bank we could build great customer experiences delivered in real-time through software, data, and AI/ML. Therefore it's really important to recognize that our migration to the cloud has been a part of a much broader digital transformation that's been going on for close to a decade. [Capital One Blog: Doing the hard things first—lessons from our cloud journey](#)

“Companies stand to gain numerous benefits from migrating to the cloud, such as cost savings, enhanced flexibility, and access to state-of-the-art DevOps tools, databases, and AI platforms. However, successful cloud adoption often necessitates the implementation of robust controls and governance measures. With over two decades of experience, we understand the requirements for long-term success in the cloud.”

— Denis McFarlane, Infinitive CEO

Effective End-to-End Risk Management Practices

To address these challenges and realize the benefits of cloud adoption, financial institutions must implement clear, repeatable processes that integrate cloud security and compliance into their organizational culture. Here are eight steps to establish effective end-to-end cloud risk management practices:

- 1. Cultivate a Risk-Aware Culture:** Foster a culture that values risk awareness and secure cloud practices, gaining executive buy-in to support cloud-related risk management efforts.
- 2. Implement Robust Risk Evaluation Processes:** Develop standardized processes for evaluating cloud-related risks, ensuring comprehensive assessments of new and existing services.
- 3. Thorough Documentation of Controls:** Document control processes comprehensively, providing clear guidance for teams.
- 4. Define Roles and Responsibilities:** Establish clear roles and responsibilities throughout the organization, ensuring everyone understands their role in mitigating cloud-related risks.
- 5. Align with Industry Best Practices:** Align cloud risk management with recognized industry best practices, such as [the NIST Cybersecurity Framework](#).
- 6. Align with Business Continuity Planning:** Integrate cloud risk management with business continuity planning, identifying critical services and enhancing overall business resilience.

- 7. Establish Clear Compliance Metrics:** Define and track metrics for measuring compliance with control requirements, allowing prompt identification of deviations.
- 8. Standardize and Automate Controls:** Standardize and automate controls wherever possible to ensure consistency and effectiveness, reducing human error.

The Infinitive Solution for Developing an Effective Cloud Risk and Controls Program

To effectively mitigate cloud risk and maintain compliance while harnessing the potential of the cloud, financial institutions can partner with companies like Infinitive. Infinitive has helped many organizations improve their cloud risk and controls programs to enhance data security, protect against threats, and ensure compliance with regulations. From conducting comprehensive risk assessments to implementing solutions to providing continuous monitoring, our team ensures that your organization stays ahead of potential risks and regulatory changes. Through proactive guidance and ongoing support, Infinitive enables organizations to enhance overall cloud security posture, strengthen compliance, and optimize cloud resources for maximum efficiency and resilience.

Infinitive offers a suite of next-generation cloud risk and control solutions designed to build scalable processes based on best practices such as:

Cloud Controls and Governance Maturity Assessment: Evaluate your cloud processes against maturity levels and best practices, providing tailored recommendations for improvement.



Cloud Control Lifecycle Support: Establish a dynamic cloud control lifecycle process, encompassing risk assessment, control design and validation, monitoring, and exception tracking.

Cloud Service Enablement: Introduce a structured approach for securely launching cloud services, identifying dependencies, and ensuring alignment with stakeholders.

Governance Policies, Standards, and Procedures: Develop or update policies, standards, and procedures, offering clear guidance on cloud control governance.

Summary

In summary, this eBook delves into the transformative impact of cloud technologies on U.S.-based financial institutions. It highlights the growth of the cloud market in the finance sector and the driving forces behind this adoption. However, it also underscores the risks associated with the cloud, such as cyber-attacks and regulatory challenges.

Financial organizations must navigate a complex landscape where cloud adoption can lead to significant benefits, but also potential pitfalls. To address these challenges, the ebook outlines a comprehensive approach to cloud risk management. This approach encompasses cultivating a risk-aware culture, implementing robust risk evaluation processes, documenting controls, defining roles and responsibilities, aligning with industry best practices, integrating risk management with business continuity planning, establishing clear compliance metrics, and standardizing and automating controls.

Ultimately, effective cloud risk management not only enhances security and compliance but also accelerates cloud adoption, innovation, and cost optimization. To achieve these objectives, financial institutions need to embrace a proactive risk management mindset, aligning their cloud strategies with industry best practices and regulatory requirements. In doing so, they can unlock the full potential of cloud technologies in an ever-evolving digital landscape, ensuring long-term success and profitability.

By partnering with organizations like Infinitive, financial institutions can confidently navigate the complexities of cloud risk management, ensuring security, compliance, and operational efficiency in their cloud environments.



Find out more about
[Infinitive's Cloud Risk and Controls](#)
capabilities and
[Infinitive's Cloud Risk and Controls](#)
[Maturity Assessment](#)



About Infinitive

Infinitive enables Global 2000 companies to transform their businesses by embracing the full potential of their data. Our mission is to modernize, monetize, and operationalize data, enabling the integration of cutting-edge technologies like artificial intelligence (AI) and driving substantial business advantages. Our dedicated team of seasoned consultants specializes in helping companies harness the power of data to unlock new opportunities, enhance decision-making, and fuel growth in the digital age. Established in 2003, Infinitive has been a trusted partner for organizations across various industries, including financial services, media and entertainment, education, retail, hospitality, healthcare, and non-profit sectors.