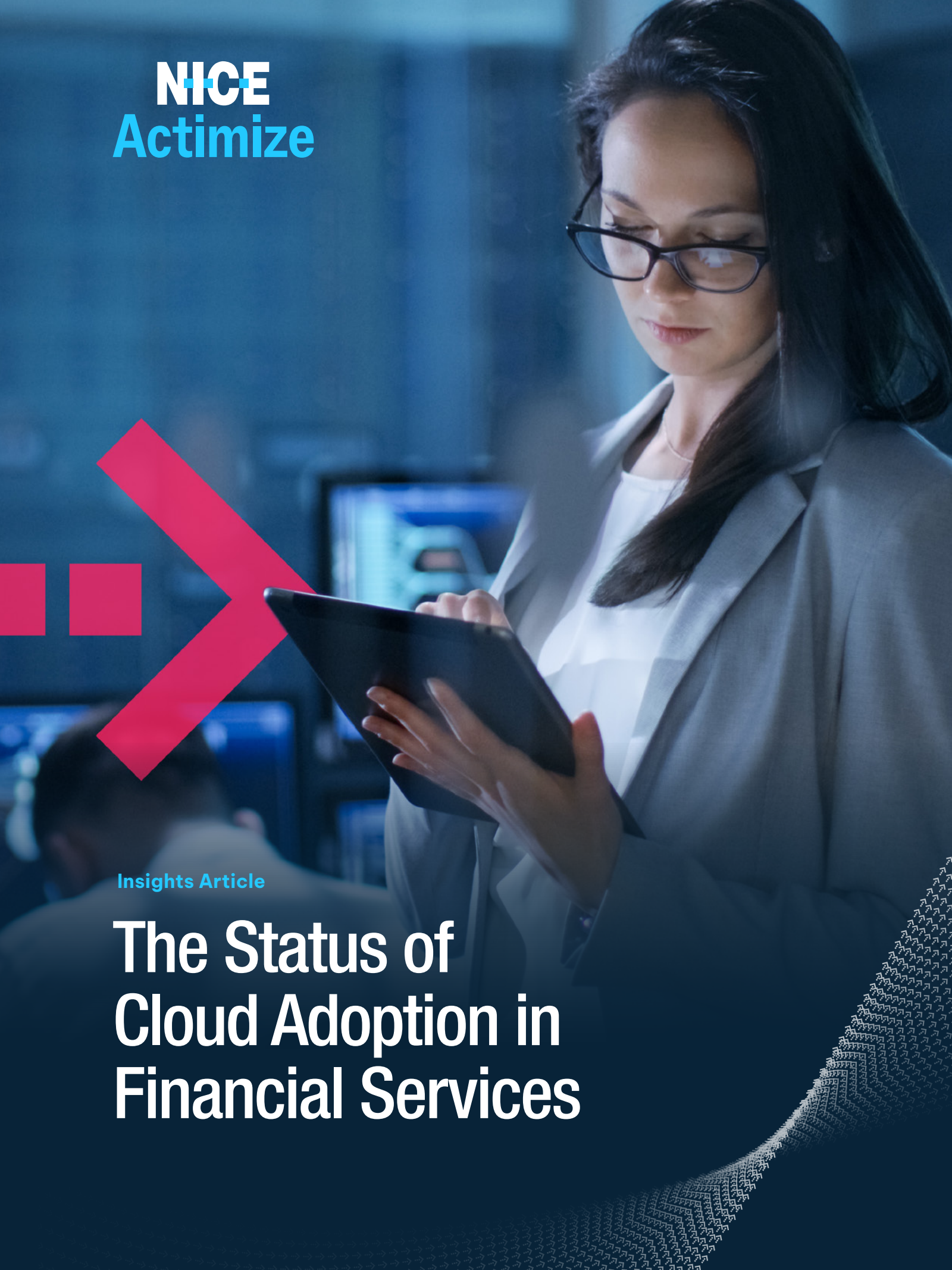
NICE Actimize



Insights Article

The Status of Cloud Adoption in Financial Services

What's the latest cloud development in the financial industry? The U.S Department of Treasury (Treasury) recently released a comprehensive report "The Financial Services Sector's Adoption of Cloud Services", in partnership with the Financial and Banking Information Infrastructure Committee (FBIIC).[1]

Cloud is on the path to ubiquitous adoption across all industries, including financial services, in response to numerous business challenges set into motion by in 2020. Financial firms are leveraging cloud to accelerate IT modernization and business growth, support distributed workforces, reduce costs, improve security and resilience, and shorten new product and service development cycles amidst a backdrop of near-constant economic uncertainty and technological disruption. Meeting customer expectations for fresh digital offerings via cloud-native capabilities, such as AI, machine learning and advanced analytics, also plays a role in the intensified rate of cloud adoption.

The Treasury's report provides its objective perspective of the industry's current position on cloud adoption, acknowledging possible advantages and pain points that arise as adoption grows.

We offer this in-depth overview of key findings in the report. This will help firms in the financial services industry better understand cloud services as a key element of modern technology initiatives and the respective impact on service delivery and operational resilience.

Cloud Adoption Incentives & Cloud Benefits

There's no one-size-fits-all approach to cloud adoption. Small and mid-market financial institutions (FIs) often leverage public cloud and operate their IT infrastructure solely in the cloud. Large FIs often deploy hybrid models that incorporate public and private cloud in addition to their data centers. Other FIs adopt public cloud to minimize the costs and environmental impact of their data center.

Cloud is more accessible to firms of all sizes due to decreasing hardware and component costs and the rapid evolution of virtualization and connectivity. It's also an attractive digital transformation enabler. Why? Because of the cost-effectiveness associated with operating, maintaining, and upgrading services and the minimal amount of management oversight needed for provisioning.

In 2023, Gartner predicts that public cloud services spending will hit almost $600 billion, up from $490.3 billion in 2022.[2] By 2026, IDC expects compute and storage cloud infrastructure spending to comprise 68.6% of overall compute and storage infrastructure spend.[3] When looking at private cloud spending, 49% of surveyed CIOs plan to increase spending vs 72% of respondents who intend to focus investments on public cloud.[4]

A few main incentives driving cloud adoption in the financial industry include the:

- Need to accelerate and scale applications and services via cloud tools, including AI and customer applications
- Ability to address customer expectations for innovative digital products with robust data enabled by cloud services to interact with diverse partner FIs and non-banks
- Goal to strengthen resilience to physical and cyber events with numerous data centers or regions from the same CSP (cloud service provider) and wider use of zero trust models and encryption
- Need to modernize IT infrastructures to support distributed workforce and digital services
- Trend of third-party providers pivoting to cloud and discontinuing on-prem offerings for client FIs
- Opportunity to reduce costs versus legacy IT environments

It's widely acknowledged that if configured, provisioned and managed correctly, public cloud services offers numerous benefits, including more security and resilience. It also provides physical redundancy, which basically means that data or applications, are maintained between different physical locations (data centers). That mitigates potential data loss or service disruption in the event of a natural disaster, power interruption, or similar event.

Additionally, public cloud service security tends to either match or surpass on-premises capabilities. For instance, FIs can leverage cloud services for data encryption in transit or at rest. But FIs are still indicating they'd like more information from their CSPs about how risks to the cloud environment are addressed.

But the means to quickly obtain and commit new resources is a primary benefit for FIs. Cloud services aren't susceptible to the bandwidth restrictions connected with traditional virtual private networks, which enables faster scalability for use cases like risk modeling. The ability to rapidly deploy limited-use resources in IaaS environments also provides more agile testing environments for those FIs that are developing or adapting software.

Types of Cloud Services

Because cloud services are customizable, FIs can either choose or design services that address specific operational, security and business needs. This should be accompanied by a roadmap for their cloud strategy that extends to the type of approach, like hybrid or multi-cloud, alignment with overall business objectives, and an audit of their IT architecture.

For example, an FI might use various cloud vendors in a multi-cloud approach, such as using a CSP for risk modeling and another for productivity services. Or FIs might fully migrate to the cloud to eliminate reliance on on-premises IT architecture. Or they might choose a hybrid approach that mixes on-premises architecture with the cloud.

Per The Treasury's findings, the types of cloud services that FIs are currently using include:

Software as a Service (SaaS)

The most popular cloud services within the banking industry at about 91%.[5] SaaS providers usually manage the cloud infrastructure and software application, but FIs are usually responsible for data transmission and storage, user accessibility and configuration, and monitoring usage. Anti-money laundering tools, office productivity systems, and security monitoring tools are common SaaS applications adopted by FIs.

Platform as a Service (PaaS)

PaaS is being used by FIs for the deployment of security tools and to enable software development, frequently alongside IaaS. Risk management is similar to SaaS models, but FIs also have to address cloud platform resource provisioning and configuration, and manage controls for application development, deployment and administration. The infrastructure and platforms, such as OS or storage, fall under the CSP's responsibilities.

Infrastructure as a Service (IaaS)

IaaS cloud service adoption by banks is only 29% as of 2021.[6] IaaS can support internally developed or obtained core processing platforms, in addition to business recovery and data storage. This model also improves IT infrastructure agility and scalability. Similar to PaaS, responsibility for the provisioning and configuring of cloud platform resources falls within the FIs jurisdiction, as does services, OS, networks, and storage. CSPs manage and maintain all controls associated with the physical data center, like network infrastructure and identity access management.

Challenges Could Diminish Potential Cloud Benefits

Despite the velocity of cloud adoption in financial services, FIs of all sizes may face specific challenges with adoption that can impact the ability to derive meaningful benefits from cloud services.

Limited Due Diligence and Monitoring Transparency

FIs need straightforward information from CSPs to understand the possible risks associated with cloud services and ensure they implement the right mitigation controls. Otherwise, risk management capabilities could be vulnerable to certain threats. Some FIs reported minimal transparency about the amount of data centers they were using until an event happened at the CSP. Also, some FI stakeholders think CSP communication about cyber and operational incidents needs improvement. Lack of transparency surrounding SaaS offerings is another common issue.

Skills and Tool Gaps For Secure Deployment

Security incidents can arise from user misconfiguration of cloud services, such as shortages of cloud-specific skills; this challenge could persist given the imbalance between cloud demand and available expertise. Also, FIs are looking for more insights into baseline configurations and the trajectory of cloud tools, like for security monitoring, due to the frequent disparity between CSP-documented service features and actual feature functionality.

Possible Exposure to Operational Incidents

Like any technology, cloud services can be vulnerable to certain risks, including operational incidents that originate at the CDP. Configurations that are developed by FIs to protect against these risks might be susceptible to an incident impacting numerous geographic regions or services, for example, identity management.

Purpose-Built, Cloud-Powered Risk Management

Cloud adoption will only continue to increase as more FIs look to leverage data analytics for competitive differentiation. A recent ABA survey revealed that over 90% of banks have some applications, data or operations in the cloud, and over 80% were currently in the adoption or early adoption stages.[7]

FIs must ensure that due diligence is exercised when procuring cloud services to prevent possible operational and security vulnerabilities and establish a safe environment for adoption. Organizations should consider their current risk management framework, unique business requirements and vision, and their risk tolerance before embarking on a cloud journey.

Why NICE Actimize

Recognized for industry excellence in financial crime management, NICE Actimize has a proven record of transparency in both design and communication that accelerates adoption of our cloud-based enterprise anti-financial crime and compliance SaaS solutions.

Our advanced AI and machine learning-powered platform is underscored by continual investment in a cloud-first approach that constantly evolves to address the changing needs of modern FIs via the highest level of scalability and performance. With deployment options that include on-premises, cloud, or SaaS, Actimize solutions are designed to meet FIs wherever they happen to be in their cloud migration journey.

Deep domain knowledge is complemented by rich implementation and configuration experience to support solution implementation, deployment, upgrade and migration, performance optimization, and enterprise integration. Standard deployment and configuration models ensure appropriate configuration to streamline and expedite cloud adoption. Actimize is also committed to durability and disaster recovery to ensure stable functionality regardless of potential disruption, and dependable data access at all times.

Cloud is more than a trend. It's the conclusive technology of this generation. Ensure that your cloud partner is positioned to help you capitalize upon the complete spectrum of cloud benefits and achieve faster business results.

For more information on NICE Actimize cloud-based solutions:

Contact us

[1]The US Department of Treasury. The Financial Services Sector's Adoption of Cloud Services.
[2]Gartner, Inc. (2022, October 31). Gartner forecasts worldwide public cloud end-user spending to reach nearly $600 billion in 2023. www.gartner.com https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023
[3]IDC. (2022, March 31). Cloud Infrastructure Spending Closes Out the Fourth Quarter and 2021 with Strong Growth, According to IDC. www.idc.com https://www.idc.com/getdoc.jsp?containerId=prUS48998722
[4]Barclays Equity Research, Cloud Wars; Vendor Positioning and Private vs. Public, by Long, Tim; Wang, George; Shreves, Alyssa (May 2022).
[5]American Bankers Association, Cloud Computing in the U.S. Banking Industry (Jun. 2021).
[6]Ibid.
[7]ABA Cloud Computing.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com