

BEST PRACTICE REPORT

Best Practices For Financial Services In Cloud

Your Financial Services Peers Are Moving Forward
With Advanced Cloud Plans

Updated February 12, 2026

By Lee Sustar, Meng Liu with Lauren Nelson, Sophia Barrett, Marissa Fritz

FORRESTER®

Summary

As the financial services industry accelerates its major digital transformation, public cloud has reached massive scale for a variety of use cases, including generative and agentic AI. Today, cloud is the preferred primary deployment model, changing both business-critical and frontend operations to enable a more customer-focused and digitally engaged organization. Today's financial services organizations are no longer hesitant to move mission-critical workloads to the public cloud. This report outlines the drivers, challenges, and approaches that financial services institutions are taking to the cloud.

Financial Services Are Accelerating Their Cloud Adoption

Historically, financial services organizations have heavily funded technology initiatives but found themselves hampered by rigid and evolving regulatory standards. Subsequently, infrastructure strategies meant investment in private cloud, maintenance of aging mainframe estates, and some modernization efforts. Early public cloud usage was limited to low-consequence key digital services and high-performance computing scenarios such as fraud detection. Today, however, traditional players are undertaking massive initiatives. Yet challenges remain: Regulatory compliance is difficult, and establishing a proper governance framework is complex. Financial services companies are heavy [SaaS platform users](#), and **97%** are adopting or planning to adopt public cloud (see Figure 1). Over a third of cloud decision-makers at financial services enterprises (**34%**) report \$25 million or more in public cloud spend by their firms in the past year (see Figure 2). A number of factors are driving this change:

- **A renewed push for transformation.** Fueled by growing customer demand, banks launched transformation plans for areas such as cash management, trade finance, and working capital solutions. Across the board, financial services are using cloud to rethink their engagement with customers, spanning marketing, onboarding, payments, transactions, and more. A few notable examples: [JPMorganChase](#) plans to migrate 70% of its 6,000-plus applications to multiple public cloud providers. [Wells Fargo](#) embarked on a hybrid multicloud strategy, combining private cloud with public cloud efforts such as an [agentic AI rollout with Google](#). Danske Bank migrated 16,000 servers, 60,000 containers, and 25 PB of data to Amazon Web Services (AWS). UBS is migrating more than half of its applications to Azure and [cocreating AI assistants](#) for client advisors.
- **The need for operational efficiency.** Fintechs and digital-first service providers are disrupting markets with modern practices and platforms, including containers, agile-plus-DevOps methodologies, and cloud platforms. Large financial institutions are undertaking their own innovations to fend off fintechs. U.S. Bank partnered with Microsoft for payment and personalization capabilities on Azure. [Ryt Bank](#) in Malaysia looked to Alibaba Cloud for digitalization and AI enablement.
- **The imperative for collaboration and efficiency.** Digitalization and cloud are reshaping the internal operations of financial services institutions and bringing new efficiencies. Fintechs challenge banks not just by offering easier retail payment experiences, but also by leveraging efficient, cloud-native platforms to keep operating costs low. Large banks are countering with their own cloud

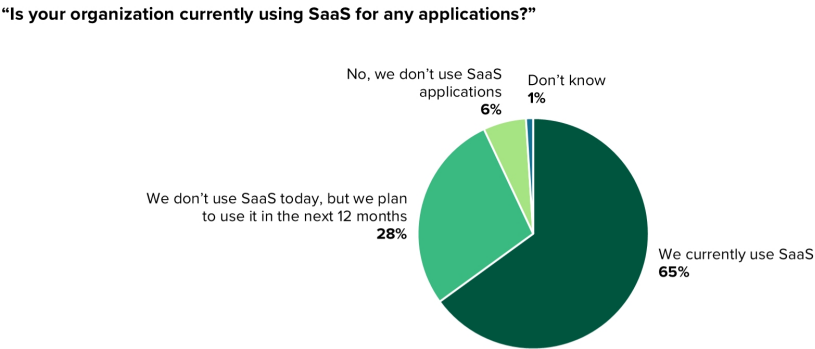
efficiency efforts. [Barclays](#) rolled out Microsoft 365 Copilot to its 100,000 employees to improve access to information and enable self-service for business functions and HR tasks. [JPMorganChase](#) tapped AWS to build LLM Suite, a generative AI agent to improve client engagement. Internal efficiency imperatives led [Deutsche Bank](#) to use Google's generative AI capabilities to check and process financial documents, among other applications.

- **A surge in digital payments.** Digital engagement — such as touchless payments using online banking, mobile banking apps, and automated transfers — are now central to the battle for market share among big banks and fintech challengers. Globally, [non-cash transactions](#) grew 17.4% percent between 2024 and 2025. Digital payment vendors also saw massive gains: [PayPal](#)'s total payment volume reached \$1.68 trillion in 2024; for [Stripe](#), the figure was \$1.4 trillion. Banks still need services for physical locations, but online and mobile banking have enabled cryptocurrency and decentralized finance, diminishing the role of physical locations. In many cases, these digital technologies are more efficient. The increased use of digital transactions accelerates banks' shift from data centers to cloud technologies as they work to provide more scalable dynamic resources to meet customer needs.
- **An expansion of financial exchange offerings and partnerships.** Industry cloud solutions and partnerships for financial services are now well established. Microsoft launched Cloud for Financial Services (February 2021) as a digitalization platform, later adding AI. The company has also partnered with LSEG since 2022; in 2025, Microsoft introduced AI agents into its platforms using LSEG-licensed financial data. AWS announced a collaboration with Nasdaq in 2021; in 2025, the two companies unveiled [Nasdaq Eqlipse](#), a market infrastructure platform. In 2021, Google Cloud announced a \$1 billion, 10-year investment agreement with CME Group; in 2024, the companies [announced](#) a new private Google Cloud region.
- **A greater acceptance of open source as a standard.** Banking regulations often call out vendor lock-in and single-supplier vulnerabilities. Many want a documented exit plan from technologies, with some even indicating that funds must be set aside to facilitate this. Open-source technologies are stepping up as an industry standard, allowing financial services companies an easier exit plan. Financial services companies can adopt and manage an open-source distribution themselves or even lean on public cloud vendors offering managed versions (e.g., Amazon EKS, Azure Kubernetes Service, and Google Kubernetes Engine are all based on Kubernetes). Given the technology commonalities, exits (and simultaneous multicloud for a single workload) are easier to manage. Although customizations don't make an exact match, it's similar enough that the burden is

Forrester Report Copy Prepared Exclusively For Clara D'Silva With Korcomptenz Inc.. Distribution and reproduction are prohibited. For more information, see the [Terms Of Use Policy](#) and [Ways To Share Research](#).

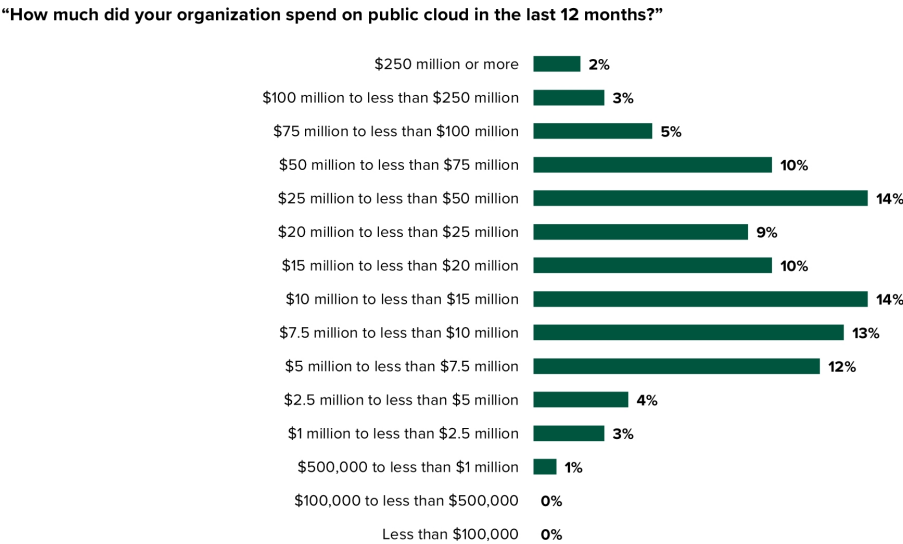
notably less. These same technologies are also powering modernization efforts and emerging technology trials.

Figure 1
More Than Half Of Financial Services Organizations Use SaaS



Note: Percentages do not total 100 because of rounding.
Base: 212 software decision-makers at financial services enterprises
Source: Forrester's Industry- And Customer-Supporting Software Survey, 2025
© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2
Over One-Third Of Financial Services Firms Spend \$25 Million-Plus On Public Cloud Yearly



Base: 212 cloud decision-makers at financial services enterprises with seniority level of vice president or above whose organization is adopting public cloud platforms
Source: Forrester's Cloud Survey, 2024

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Cloud And Other New Technologies Create Unique Challenges For Financial Services

While financial services firms appreciate cloud’s value, many organizations still have deeply entrenched legacy infrastructure and workloads. The difficulty in migration, along with regulatory compliance concerns (e.g., data residency rules, cloud security, payment and transaction process across different regions), makes adoption via modernization and migration a very difficult hill to climb.

- **Long-standing leaders may have extreme risk aversion.** Historically, it wasn’t unusual for long-tenured technology executives at major financial services companies to resist cloud adoption. This approach echoed conservative technology approaches and was often justified by the stringent regulations that enterprises faced as well as a “not on my watch” aversion to risk. Early innovative examples in this industry were often led by executives new in their position or by individuals who had transitioned from other sectors. Individuals advocating for change and wider cloud adoption often find that their greatest challenge is battling

traditional leaders who have been in their roles a long time.

- **Legacy systems are hard to get rid of.** Traditional, large financial services firms have gigantic IT systems that are usually on-premises. Massive capital investment often leads to technology debt (legacy infrastructure, versions to maintain, skill sets, and value measurements) and [technical debt](#) (legacy code that's timely to update). Tech debt is a competitive disadvantage for traditional players, as they compete against digital and cloud-native players such as fintechs and digital-only banks. Paying down this debt via infrastructure and modernization investment doesn't happen overnight. Generally, legacy IT systems must coexist with new or refactored cloud-based applications for years. This complicates tech stacks, operations, measurements, and processes with hybrid/multicloud architectures.
- **Financial services firms are major targets for data breaches.** New and complex hybrid/multicloud architectures, paired with high-value incentives (i.e., valuable data to steal), make financial services companies likely targets and more vulnerable to data breaches. In the past decade, major data breaches — in each case, compromising data across tens of millions of customers — occurred at companies such as Block, Capital One, Desjardins, Equifax, Experian, First American, and Flagstar. The root cause of many breaches is poor identity and access management (IAM) and auditing across internal and external organizations and suppliers. Cyberattacks and war have prompted the Financial Services Information Sharing and Analysis Center (FS-ISAC) to periodically raise its threat level from guarded to elevated in recent years.
- **Regulations are stringent and slow to evolve.** For financial services firms, failure to comply with regulations can mean, at best, heavy regulatory fines and, at worst, loss of licenses or revoked charters. In the past few years, regulatory concerns have been shifting from financial to nonfinancial risks, including geographic boundary issues that limit data to specific availability zones or regions covered by the EU General Data Protection Regulation (GDPR) or, in some Asian countries such as China and Indonesia, by regulations that ban financial services firms from deploying core functions in the public cloud. The Digital Operational Resilience Act (DORA) requires financial services firms to have operational resilience during a major outage.

Inconsistencies between regulatory and supervisory expectations across country borders add extra complexity. The European Banking Authority (EBA) requires financial services organizations to notify their government authority when outsourcing critical functions to the cloud. However, in Luxembourg and the UK, EBA regulators require periodic reporting of all outsourced functions and pre-

authorization of all critical activities.

- **Unique challenges face each subsector.** This industry includes many subsectors, including banking, exchange services, insurance, wealth management, and lending — each with its own challenges. Banks require uninterrupted access, exchanges need fast analysis and response rates for traders, insurance deals with significant differences by region and sector, wealth management prizes top client experience, and lending faces new digital competitors and operational improvements. Each challenge brings unique fallout, hundreds of questions, and answers that are hard to come by (even by specialty boutique consultancies).

Succeed With Cloud Through Industry-Specific Tooling And Open Source

Forrester has worked with hundreds of financial services organizations over the past decade on various aspects of their cloud strategies. Through these interactions, organizations have shared recommendations and lessons learned. To help financial services adopt cloud services at scale, we've compiled these best practices to power the next iteration of your organization's cloud usage.

- **Start with digital services.** If you're early in your cloud journey, digital services is likely the best place to start, as it provides a new, highly valuable service that's customer-facing. The value of the initiative is easier to prove, and the red tape that typically accompanies change will be less time-intensive.
- **Use accelerators.** The major cloud providers have been building out offerings specifically for financial services to gain an audience in the industry. Platforms such as Microsoft's Cloud for Financial Services help firms build customer-facing applications, particularly in retail banking. With AWS' Industry Quest: Financial Services, you can learn how to build different financial services scenarios such as fraud prevention, serverless deposit accounts, and data lakes that use AWS services. Google Cloud's Dual Run helps organizations in highly regulated industries such as banking with their mainframe modernization and migration initiatives. After all, the hyperscalers are committed to providing high availability through multiple availability zone scenarios to meet stringent regulator needs. Microsoft has certified its Azure Stack HCI for some financial services regulations, and financial services organizations may find that this saves time and resources to meet on-premises regulations versus cobbling together a custom stack.
- **Use open-source technologies to mitigate lock-in and power innovation.** If you're facing difficult and expensive regulations regarding vendor lock or plans to

exit a technology, look to open-source technologies. Even if you select a vendor distribution or managed offering, the switch between solutions is less challenging than if the solution were entirely proprietary to that vendor. Similarly, organizations use common open-source solutions to power multiple emerging technology efforts (e.g., cloud-native ecosystems to power edge, AI/ML, and other new innovation projects).

- **Scale your modernization plans quickly.** Some financial services organizations isolate cloud-native teams, which can accelerate success but may have limited impact. Leading organizations blend cloud-native development efforts with their traditional development teams, such as mainframe. This not only expands modernization efforts and creates operational efficiencies for more teams but also provides a more rewarding experience for your traditional developers. Traditional technologies are increasing support of integration between their solutions and modern frameworks (e.g., IBM Z supports Linux and Red Hat OpenShift).
- **Involve the security team early.** Overcome app and data insecurity and governance concerns by involving the security team early in the planning process. Use this team for direct feedback on your governance frameworks and security processes and guidelines. Use [Zero Trust protocols](#), as most financial services organizations will have a hybrid strategy that requires data transfer between on-premises and public cloud environments. Prioritize microsegmentation as a part of network topology security strategy, as it reduces implicit trust in the network. Consider other [cloud security best practices](#), such as using cloud security posture management (CSPM) solutions to discover all configuration artifacts. Use cloud identity entitlement management (CIEM) to perform automatic and manual access reviews based on access patterns.
- **Check your regulations and legal frameworks.** Make sure your regulatory team is familiar with all relevant rules and regulations. Ensure that their knowledge is up to date on the latest changes and the exact boundaries of laws and regulations. In Canada, financial services firms commonly assume that they're required to keep customer data in Canada. However, private sector privacy laws don't have data residency requirements. Some Canadian legislation, such as The Bank Act and the Insurance Companies Act, do have place-of-record requirements that are narrowly applied. However, most data residency requirements are a result of standards that an organization imposes on itself. Similar misperceptions around data residency rules may exist in other countries and regions.
- **Ask for help.** Work with managed service providers (MSPs) or global systems integrators (GSIs) to help with major cloud initiatives, whether you're tackling agile-plus-DevOps, cloud migration, or major custom app modernization. Exclude

consultancies that lack substantial financial services cloud experience, and ask for customer references. These are large-scale, multipronged efforts that require clear prioritization, iterative implementation, tight feedback loops, and regular assessments. Support from the C-suite is critical.

Supplemental Material

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.



We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

[Learn more.](#)

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

[Learn more.](#)

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

[Learn more.](#)

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com