Financial Institutions Need to Pursue Their Own Path to the Cloud

MAY 05, 2021
By Matthew Leybold, Hrishi Hrishikesh, Benjamin Rehberg, Filippo Scognamiglio, and Marc Sterman

Cloud adoption—including hybrid and multicloud adoption—is expanding fast among private and public sector organizations of all sizes. At the enterprise level, BCG estimates that two-thirds of companies already use multiple clouds and that, by 2025, up to 60% of consumer-facing applications, almost 40% of data warehouse and analytics workloads, and more than 30% of core business applications will be running on public clouds operated by the likes of Amazon, Microsoft, and Google. Traditional on-premises technology will handle no more than a third of these workloads.
Except in financial services. Instead of rushing to the cloud, banks, credit card and payment companies, and insurers are likely to move toward it at a measured pace over several years or more, and the pathways of adoption will include banking software vendors as well as large cloud service providers. This cautious approach may at first seem counterintuitive for an industry that is both digitally mature and data intensive, but several clear signposts already point to a different type of cloud journey for financial institutions.

This is not to say that CIOs at banks and other institutions should cancel their public cloud plans and build more data centers. For most financial institutions, the cloud will be an important part of their future. But banks and others face a complex, hybrid, and fluid tech landscape that will demand a mix of infrastructure, skills, capabilities, and partnerships to navigate. Each company’s size, business mix, data and technology strategy, and ambitions will shape its journey. Here we look at the trends and developments in several areas and address four questions that will help financial institution technology executives better understand the landscape, determine how best to reduce or remove obstacles to cloud adoption, and identify the best ways to take advantage of the cloud’s strategic and innovative benefits.

THE CURRENT STATE OF PLAY

In response to internal demand for increased agility, scale, and speed, as well as external competitive signals from peers and new digital rivals, financial institutions of all size and types have tested various approaches to the cloud. These efforts have ranged in scope from launching limited pilots to moving major workloads to cloud services providers (CSPs). In the long term, only major banks—because of their scale—are likely to retain substantial data center footprints. Other institutions will have at least partially migrated to CSPs and will manage their legacy workloads in co-located facilities operated by specialist third parties.

In the interim, however, cloud adoption will be more deliberate. Well-publicized data breaches have raised caution flags. For industry-unique reasons—including mainframe technology, regulatory frameworks, and organizational digital maturity—financial institutions have been slower than businesses in other industries to move their core
infrastructure workloads to CSPs. This will change as leading CSPs establish more offerings for the financial industry to reduce the barriers to adoption and as all but the largest institutions face decisions about whether to build new data centers, upgrade existing ones, or seek alternative solutions to expanding needs and rising costs. Sooner or later, most will embrace some form of hybrid model.

CIOs need to address four questions:

- What are CSPs doing to address the needs of financial institutions?
- Which parts of the financial institution tech landscape are best suited for public clouds?
- What are the principal roadblocks to adoption, and how can they be overcome?
- How can CIOs and others best plan for future trends in cloud architecture and operating models?

CSPS AND THE NEEDS OF FINANCIAL INSTITUTIONS

With the increasing commoditization of infrastructure as a service (IaaS), CSPs are competing more on higher-value platform-as-a-service (PaaS) offerings. Overall workload adoption on public clouds in the commercial and public sectors continues to grow. Today, according to Gartner, approximately 25% of all workloads reside on public cloud infrastructure.

Most CSPs are pursuing strategic partnerships with major financial institutions to address industry-specific needs and requirements. Amazon Web Services is supporting construction of bespoke solutions (such as the online bank Marcus, with Goldman Sachs) and incorporating financial-institution-compliant controls and security within its overall configurations. Google Cloud Platform is pursuing its Anthos application management platform through partnerships with HSBC, PayPal, and KeyBank, among others. It has formed a ten-year partnership with Deutsche Bank to pursue new business models. Azure recently released a new set of industry-specific cloud services, including one for financial
institutions. IBM is partnering with Bank of America to develop a public cloud platform that complies with relevant regulations and security controls.

“CSPs are realizing that they cannot just provide the tech; they need to understand the bank’s core business. Their appetite to collaborate and solve business problems is growing,” said one banking technology executive.

FINANCIAL INSTITUTIONS AND THE TECH LANDSCAPE

Our research shows that most financial institutions have mature private cloud capabilities, but most of them rely on public cloud adoption for no more than 15% of their core IT workloads. The industry as a whole has focused primarily on SaaS adoption and IaaS adoption for certain targeted use cases.

Core versus Noncore Systems. So far, the financial institution applications and workloads that companies are migrating to or building natively on public clouds consist largely of noncore systems of engagement (SOEs)—front-end systems that interface with customers and business partners (such as digital channels, mobile apps, and online banking). The cloud is a common choice for many SOEs, including the following:

- New digital capabilities and applications
- Data and analytics platform use cases
- Digital channel use cases (such as websites and mobile apps)
- Fraud and risk use cases (such as risk analytics and reporting, and machine learning and cloud workloads for anti-money laundering)
- Reporting use cases (such as risk analytics and reporting)

Most systems of record (SORs)—such as core computing and mission-critical systems and workloads—remain on-premises on classic IT infrastructure (often mainframes), with no current plans for public cloud adoption. Our research finds that this is true for regional and super-regional banks, credit card and payments companies, and global systemically
important banks (GSIBs). We have yet to see a practical and viable cloud option successfully employed for such traditional mainframe workloads at scale.

“Core banking systems are the heart that makes the bank work, and any hiccups will be critical to the business. There is too high of a risk to migrate to the public cloud,” said a former banking cybersecurity executive. “We are so heavily invested in the private cloud [that] the overhaul of the core banking systems has to be a business-led transformation,” said a former CIO.

In addition, many financial institutions that custom-build their own proprietary infrastructure environments also use a significant number of off-the-shelf core-banking and mission-critical financial services platforms (such as digital channels, commercial and treasury, card and payments networks, and loyalty and rewards programs) provided by software vendors. A large majority of these customers have expressed the intention to follow their software vendors’ cloud-native glide path on the premise that by doing so they will obtain a cloud-native, mature solution that is already on their vendor’s upgrade path. These institutions are looking to adopt a public cloud in a way that is consistent with their existing vendor partnerships and commercial best practices and that lowers the risk of going it alone on a complex and costly journey.

Internal Considerations. CIOs grapple with a number of internal factors, many of which slow the pace of cloud adoption, especially for core systems:

- **Lack of a Major Business Driver.** The technology benefits alone do not outweigh the risk and the costs in the absence of a clear business catalyst to drive the change.

- **Risk.** “The core banking system is the backbone, and a single mistake can cripple everything,” said a former major bank CIO.

- **Cost.** “It took my team two years to refactor and re-architect a vendor’s software. I cannot imagine how complex it will be for a core banking system,” said a former solutions architect.

- **The Resiliency of Mainframes.** “We assessed our core banking systems and determined that the mainframe is still a viable and stable solution,” said a former
When financial institutions do choose public cloud solutions, the primary drivers are not cost, but productivity and flexibility. Banks and others are constantly gauging the merits of identifying long-term strategic cloud infrastructure partners and adopting a cloud-native model against the significant risks they perceive of vendor lock-in. One result is that we see a rise in cloud-agnostic and best-of-breed models, especially at the platform layer, as institutions look for capabilities that are consistent across environments, adopt open standards, and limit exposure to vendor-native services that lock in both the architecture and workload residency.

Despite widespread aspirations to achieve low cost of switching, no institution that we looked at in our research has managed to build a single workload multicloud solution at scale in which one workload runs seamlessly on multiple clouds. Nor does any true hybrid cloud solution yet operate at scale. Those that have tried have ended up pivoting to multiple-cloud solutions, running different workloads on different clouds in response to resiliency and lock-in concerns.

Meanwhile, financial institutions have invested massively over the past three to five years in private cloud development. Banks and others are reticent to make another major move without fully realizing the ROI for their private cloud investments, unless it is truly synergistic.

Some key themes are emerging in cloud adoption among various industry subsectors. Among regional and superregional banks, cloud adoption is most prevalent in players that lack substantial scale (less than $500 million in annual tech-related operating expenses). These institutions see the cloud as an option to rent scale for both cost and productivity gains. GSIBs, which have the scale to support on-premises data centers, tend to use cloud solutions selectively for edge computing and for storage and noncore (SOE and customer-facing) use cases. Many nonbanking institutions, such as asset managers, are open to a more comprehensive move to the cloud, especially if they are already in the midst of a program to modernize their technology platform.
Card and payments companies, which focus heavily on internet-facing applications and other customer services, are moving SOE workloads to the cloud. Some of these solutions—such as web and mobile applications and new digital capabilities—are digital native, so they are easy to move. Many card and payments companies use these workloads to gain experience with cloud adoption and to build runways for an eventual modernization strategy for their legacy SORs.

OVERCOMING THE CHALLENGES TO BROADER CLOUD ADOPTION

A number of specific technical challenges impede wider cloud adoption in the financial industry. These include latency, data residency and transactions, personally identifiable information (PII) and regulatory risk, and resiliency.

**Latency.** The geographic distance between the data centers of a financial institution and a CSP affects latency and performance. Mission-critical and core banking workloads, such as credit card authorization round-trip time, often require ultra-low latency, which becomes a key criterion for assessing the suitability of a public cloud. Shifting systems from data centers to public cloud environments may introduce extra latency to end-to-end processes and transactions, especially when engagement systems are decoupled from record systems.

Recognizing the importance of high performance and reliability to the financial sectors, CSPs are developing multiple creative solutions, and latency issues are already becoming less of a barrier to cloud adoption. One approach is co-location with dedicated cloud network connections. Some CSPs are establishing new regions and availability zones that accommodate physical proximity and even facility co-location with major customers. Another option is service level agreements (SLAs) designed to mitigate latency and performance issues across private networks by connecting data centers to public clouds. All major CSPs offer dedicated and private connectivity arrangements, and enterprise customers can negotiate with willing CSPs to adjust physical footprints and regional boundaries to remove the latency dependency. (See Exhibit 1.)
Data Residency and Transactions. The location of data raises multiple issues of “ownership” (on-premises data center or public cloud) and geography (US, Europe, or elsewhere). Regulatory requirements impose further constraints. Many institutions face voluntary or externally mandated limits on where they can store data of certain types. In addition, new cloud environments and configurations—such as hybrid and multicloud—introduce a network medium as well as transaction requirements for data sharing, both of which raise technical challenges and potential costs.

Distributed data models for cloud solutions are not yet fully mature, but companies are testing them for a broadening set of use cases (such as consolidated data lakes for analytics). Most public CSPs charge little to nothing for data ingress, but they have variable corresponding egress or outbound charges for data transfer, introducing tradeoffs and lock-in considerations.

PII and Regulatory Risk. Financial institutions have various security concerns, but regulatory issues related to PII have been a particularly challenging barrier to broader cloud adoption. In any event, securing PII in the cloud is not just a CSP and technology
issue. Breaches often result from the lack of maturity within internal cloud-native cybersecurity controls and processes.

CSPs have been easing the concerns of regulators and financial institutions through third-party security certifications and attestations (such as ISO 27000) and alignment to customer-centric guidelines (such as those promulgated in the US by the Office of the Comptroller of the Currency and the Federal Financial Institutions Examination Council). For their part, financial firms are experimenting with various models to meet regulatory and security requirements.

In fact, the risk profile of cloud providers is no longer a significant point of difference between the public cloud and on-premises data centers. There are few regulatory restrictions for CSPs and few hard limitations on PII storage, and regulators generally apply same standards to CSPs as to outsourcing vendors.

**Resiliency.** Outages are always a major concern, especially for mission-critical workloads. The two main areas of risk are infrastructure availability and service availability for applications built on the infrastructure.

Most infrastructure outages are caused by the same factors responsible for outages in traditional IT environments, including human error and power failures. Most cloud outages have been restricted to one availability zone and generally have been limited to specific services, although some outages have affected multiple zones. Only a couple of recorded instances have involved outages that affected more than one region.

That said, availability issues have led many financial institutions to abandon their attempts at multicloud adoption and to fall back on either private or single-cloud models. CSPs have been working hard to improve, and most major cloud services now base their SLAs on a monthly target of 99.99% availability for computing. Actual uptime varies by availability zone. If CSPs fail to meet their SLAs, they apply service credits against future payments; the credits can range from 10% and 100% of the monthly total, depending on the downtime. A well-designed cloud setup can protect against more disasters than a traditional IT setup can.
PLANNING FOR A FUTURE IN MULTIPLE CLOUDS

Despite the challenges, CIOs at financial institutions are looking toward eventual hybrid and multicloud operating models. Since no multicloud architecture is perfect for all purposes when it comes to tooling, service selection, and sourcing models for each layer of the technology stack, CIOs need to make decisions on a couple of levels. First, they need to determine what their strategy should be with respect to hybrid or multicloud. Second, they need to figure out how to implement their strategy with respect to tooling (open standards versus off-the-shelf commercial solutions), operating model (hybrid or true multicloud—with CSP vendor agnosticism and workload portability—versus multiple clouds that operate independently), and sourcing model (CSP agnostic versus CSP native adoption).

We have found that financial institutions have a continuum of choices, with differing architectural tradeoffs that they must consider in the context of the organization’s broader IT and business strategy.

At the strategic level, the industry has yet to reach a consensus view on hybrid or multicloud usage, and institutions’ experiences and results vary. Some companies have set aggressive goals for the next three to five years, but we are not aware of any that have spread a single workload across a multicloud environment. Three models—enterprise to CSP, co-location to CSP, and CSP to co-location—are seeing a fair degree of experimentation. (See Exhibit 2). Each model has its own plusses and minuses, and each institution needs to make different tradeoffs to serve its strategy and priorities.
FOUR TRUTHS WILL SHAPE THE JOURNEY

Whichever route an institution chooses, four truths are likely to shape its journey.

Adoption will be slower than most observers predict. The cloud will not replace data centers in the next three to five years. Most institutions can continue to operate their current data centers while they work with core banking software vendors on future offerings.

The future is hybrid. Institutions need to be thoughtful about how to make hybrid and multiple-cloud solutions work.

The industry has its own cloud challenges. The design and technology choices that institutions ultimately make must reflect the particular challenges of the industry, including latency, operational resiliency, security, and compliance. Companies should also be thoughtful about enabling end-to-end automation, orchestration, and integration.

Every institution needs to build some muscle in cloud. Even hybrid solutions entail building a set of in-house skills to work with cloud partners. For organizations that want
to lower the risk and cost of cloud adoption, training staff and building capabilities are just as important as pursuing a specific outcome or benefit.

Financial institutions need to plan for a future in the cloud, but their emphasis—particularly with respect to SORs—will be on getting the integration right rather than making the transition fast. A cultural shift away from long-established approaches to technology that have served financial institutions well will be a big part of the challenge. Each institution will move at its own pace, and leveraging others’ experience can help. The four truths referred to above can serve as guideposts for business and technology leaders as they manage the transition.

Authors

Matthew Leybold
Platinion Managing Director
New York

Hrishi Hrishikesh
Partner & Director
New Jersey

Benjamin Rehberg
Managing Director & Senior Partner
New York

Filippo Scognamiglio
Managing Director & Partner
New York

Marc Sterman
BCG Platinion Managing Director
New York
Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

© Boston Consulting Group 2023. All rights reserved.

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and Twitter.