The Evolution of Hybrid Cloud in Financial Services

Designing for Financial Services Requirements with Intent

January 2025

Virginie O'Shea

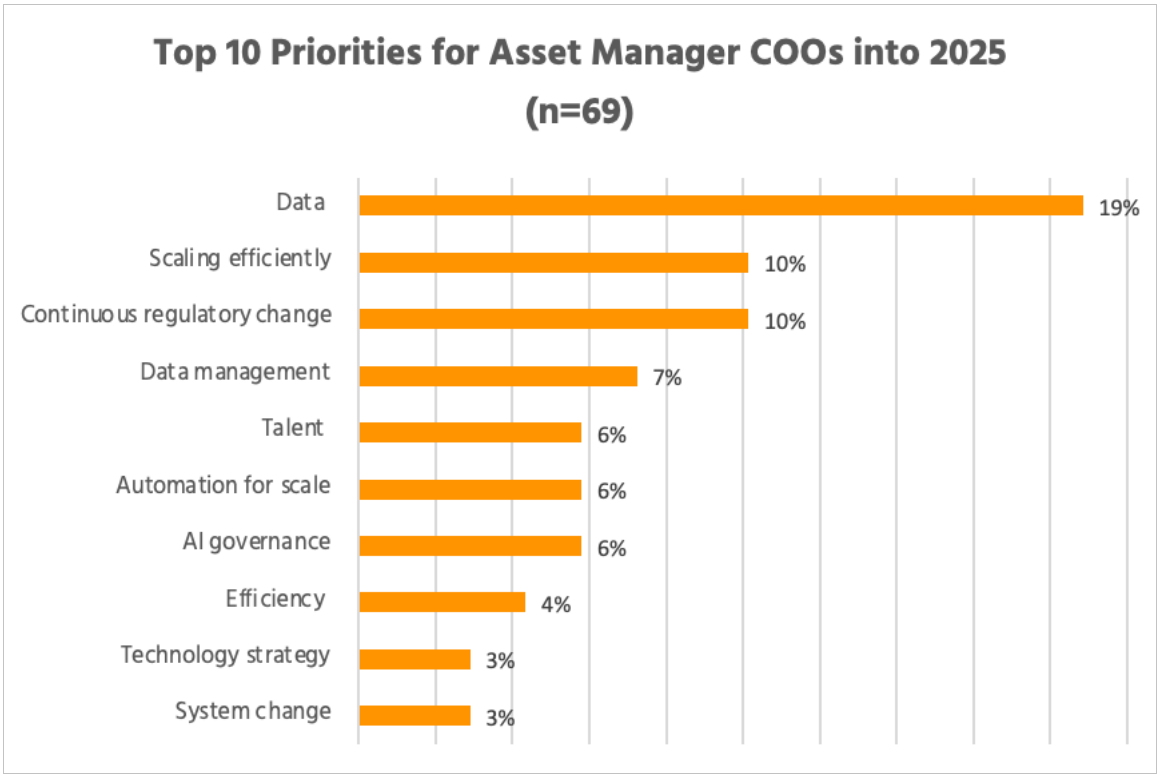
fintechfirebrand.com

The Hybrid Cloud Adoption Drivers

The financial services industry's adoption of cloud native technology has been well-documented over the last couple of decades, as firms have sought to modernize and update their technology environments in line with changing market requirements. The need to scale operations to reflect rising data and transaction volumes via a more elastic approach to processing power, as well as the requirement to support faster time to market for new product development have necessitated the rollout of more flexible cloud-based technology environments. These environments can be spun up and down as necessary and can support a wide range of data and application requirements across the various financial services sectors.

The banking sector took some time to embrace the cloud but the asset management community has long been an advocate for technology deployments in the cloud via software as a service (SaaS) models. The focus on developing more robust data strategies within both buy-side and sell-side communities has increased the dominance and reliance on cloud architecture, especially cloud-hosted data lakes such as Snowflake. These platforms enable greater democratized access to data across an organization and even between organizations, although they have necessitated the introduction of data lake houses to introduce a translation layer between the data and the end user.

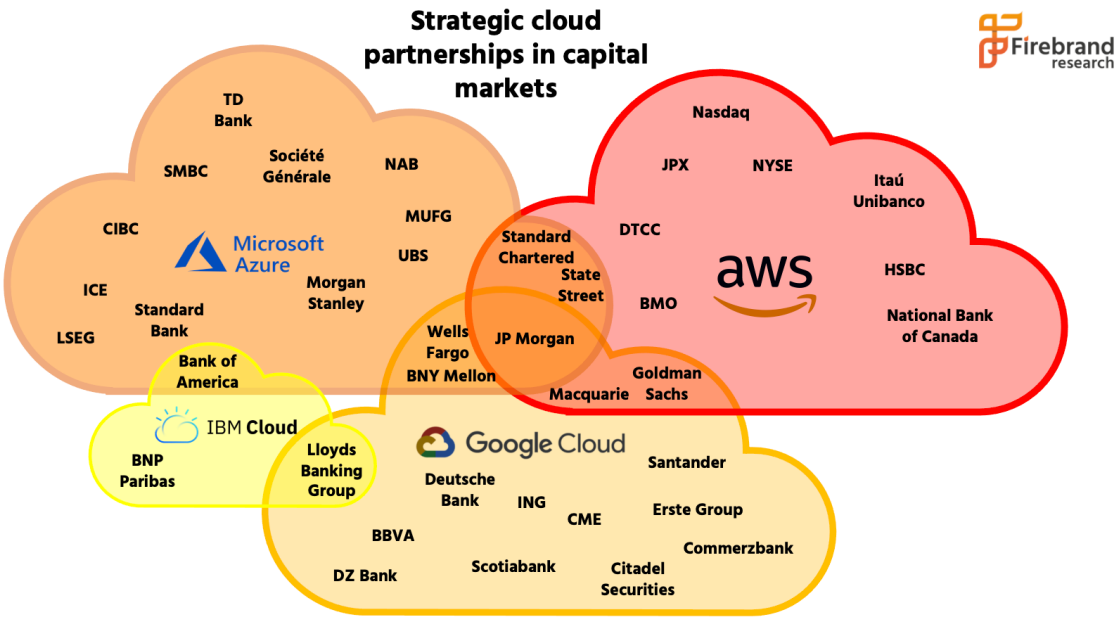
This focus on data strategy is part of a long-term plan, as highlighted by the chart below, which shows responses to a poll of asset management firm chief operating officers (COOs) and heads of operations at a buy-side conference in London in September 2024. Data related topics were cited a third of the poll respondents as their biggest operational priority into the next year and beyond, with "data" as first out of the top ten phrases used in the free-format responses. One of the greatest challenges these firms face is how to turn these strategies into reality and turn data into a true asset for the business.



The building of data services for end clients requires a more open data environment within a firm, where application developers and lines of business can access the right data at the right time, with minimum friction and latency in the process. However, sensitivity around data privacy and data ownership has increased over time, alongside financial regulation targeted at protecting client data such as the European General Data Protection Regulation (GDPR). The regulatory community has also focused upon improving the industry's operational resilience via regulations such as the Digital Operational Resilience Act (DORA), which comes into force in January 2025.

These regulatory developments have highlighted the need for greater focus on cybersecurity and business continuity measures such as backup and disaster recovery plans. They have also thrown a spotlight on the concentration risks posed by cloud services providers (CSPs), who have strategic relationships with a large number of financial institutions as highlighted by the graphic below. Some banks have established relationships with multiple CSPs, but many currently have only one strategic cloud

partner and face challenges due to the competitive pricing dynamics of being locked into one vendor relationship.



The evolution of a hybrid approach to cloud reflects the ongoing modernization of financial institutions' technology stacks in combination with the need for firms to right-size their environments for their various functional areas. The cost model of cloud native technologies has been a challenge to manage for many firms due to the metering of data usage, which has altered how data consumption is charged back to end business units. As noted by head of data analytics at a large global investment bank, the economics of cloud-hosting has caused some functions to revert back to on premises storage, especially for functions that are non-revenue generating.

The Hybrid Cloud Challenges

Hybrid cloud environments necessitate a spilt approach to managing both types of technology, cloud native and traditional on premises data center-based legacy platforms, which can cause talent challenges from an IT staffing perspective. Unless legacy support staff are retrained and upskilled, these teams can come into conflict and operate in an

inefficient manner. Legacy on premises infrastructure needs to be modernized to operate as a private cloud infrastructure, allowing for a more automated data infrastructure with application programming interfaces (APIs) connecting the various upstream and downstream applications and platforms.

Technology teams also need to understand the gravity of data, which means the tendency of large data sets to attract other data, services and applications. Data access therefore needs to be seamless for end users and applications, whether they reside close to the data or in a centralised manner. The environment in which data and applications reside cannot impact operations and cause friction, it needs to be platform agnostic. The environment overall also needs to be scalable from a data perspective, given that artificial intelligence (AI) is increasingly being deployed across the financial services sector and AI models require a high volume of quality data on which to be trained.

Another important aspect to the transformation of the financial services industry is the move to a more sustainable business model in the face of climate change. Banks, market infrastructures and asset managers are all under increased scrutiny around their plans to reach net zero by a defined date, which means energy consumption and technology choices must also factor in sustainability metrics. Environmental, social and governance (ESG) scores can impact the share price of financial institutions and negative publicity around environmental issues can have a damaging impact on client relationships. This means that sustainability has become a core part of the business decision-making process when it comes to the deployment of new technology or infrastructure.

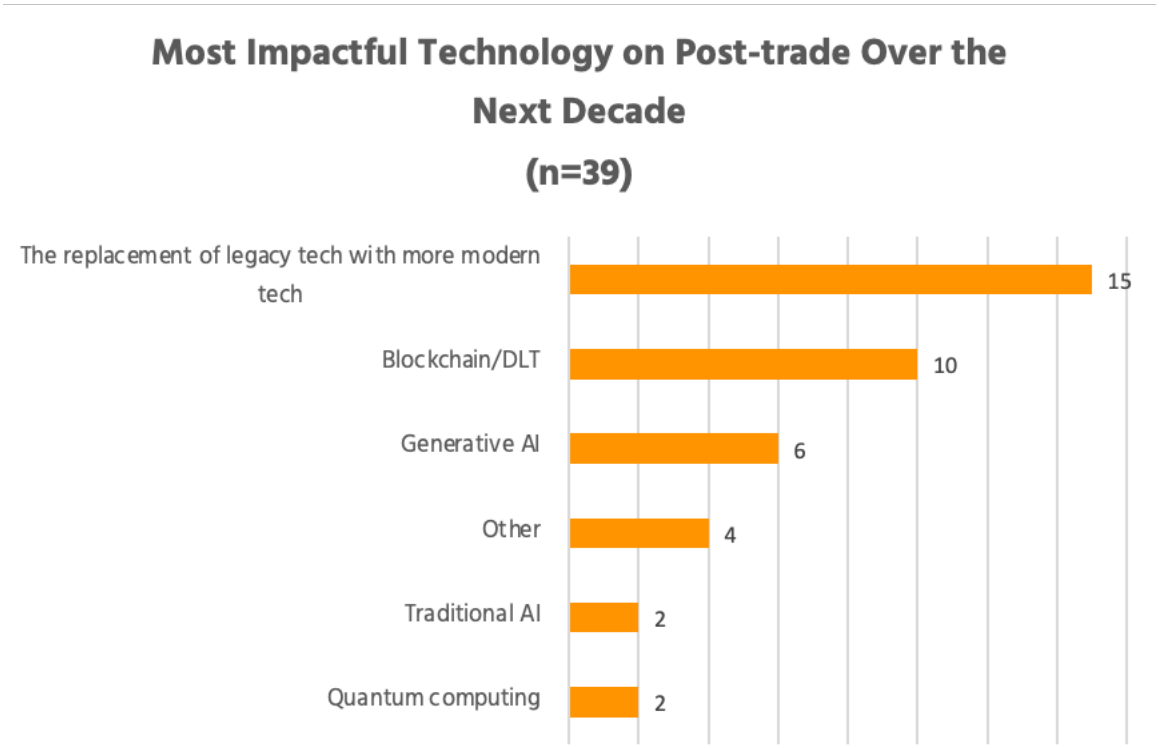
Overall, the challenge for these, often heavily regulated firms is balancing innovation with risk management, ensuring that compliance requirements are met without degrading speed and agility of research, development and deployment of new products and applications. Financial institutions must ensure that their internal architectures are optimized to support:

- **Increased scale:** The ability to meet current and future market, client and business requirements.

- **The adoption of more data-intensive technologies:** Support for higher volumes of clean and high-quality data.
- **A more real-time environment:** Financial institutions are being compelled to support more real time access to data for decision-making from front-to-back-office processes.
- **Greater levels of transparency:** Clients and regulators are keen to access and understand the data underlying decisions and to interrogate that information for various purposes.
- **Higher levels of resilience:** Operational risk and resilience management is key to remaining out of the regulatory spotlight.
- **A more sustainable future:** Technology environments must also be assessed based on their sustainability.

Operational Best Practices for Hybrid Cloud

Firms have made a lot of investment in cloud and on premises technologies over the last couple of decades and therefore they need to retain the benefits of these investments without creating unnecessary costs. The overall goal of modernizing the technology estate is a high priority item for financial institutions over the few years, especially in their middle and back offices. The modernization of the post-trade technology environment is even more important to firms than the deployment of next generation technology pilots such as distributed ledger technology (DLT) or AI, as highlighted by the chart below, which is based on a poll of bank operations executives conducted in September 2024.



This prioritization of legacy modernization means firms must get to grips with the costs and opportunities of a hybrid technology stack, including the licensing changes recently made in the virtualization platform arena. Firms will have to consider the move of these technologies to private cloud container environments if they haven't already begun moving in that direction. The ephemeral nature of containers, which means they are typically short-lived and therefore be easily created and destroyed, is challenging from a data ownership, governance and privacy perspective. This necessitates a different approach to data security and compliance, especially when it comes to meeting obligations such as those related to GDPR or operational resilience regulation.

There has been an ongoing focus within financial services on improving efficiency overall via operational process automation and reducing costs by eliminating duplicative systems, which fits with the right-sizing approach to cloud technology that a hybrid environment facilitates. Moreover, financial institutions that have yet to make strategic decisions about their approach to cloud have a unique opportunity as they are being

compelled to review their technology environments overall as part of the global regulatory operational resilience agenda.

A strategic evaluation of a firm's architecture begins with an assessment of the existing people, process and technology environment in terms of data requirements, workloads, skills and how technology is consumed across the business. Not only are current business requirements in scope, chief technology officers (CTOs) also need to build-in scale for future market structure and business changes that may impact processing capacity or data storage requirements. The cost of supporting all of these developments needs to be factored strategically into every business and technology decision, taking into account current and future workloads in each functional area.

The rising costs of data centers due to the changing environmental considerations and sustainability requirements in various jurisdictions that are compelling data center providers to rebuild and significantly alter their premises have contributed to costs over time. Cost therefore needs to be baked into the process of support and cost minimization needs to be a feature of the technology environment. Workloads need to be automatically allocated to the most appropriate environment rather than relying purely on manual decision-making and IT intervention. Support needs to be automated as much as possible to enable for a dynamic environment that matches business needs as they change and that responds to pricing changes as they occur.

However, the financial services industry sensitivity around data, especially personally identifiable information, also needs to be taken into account from a storage and access standpoint. Most financial institutions have placed data is at the heart of their businesses and moved from a siloed product-centric view of the business to a more data-centric view, which has necessitated a more open architecture. Financial institutions need to be able to face-off against increased competition from the fintech sector by delivering a more consistent and data-driven service to clients.

Enabling the business to access data from wherever it is stored within an organization as and when it is required is a key priority for chief data officers and their teams. Data access

therefore needs to be seamless for the end user community, but it also must be permission based, so that protected data assets are controlled and monitored. Internal and external cybersecurity risks must be strictly managed, including both insider threats from staff and outsider cybercriminal activities.

The operational resilience agenda reflects this emphasis on cybersecurity but it also places emphasis on the scalability aspect of a financial institution's technology as outages and downtime are a serious regulatory and reputational risk. Firms need to demonstrate to regulators and their clients that they are able to bounce back from an operational outage or a cybersecurity breach. Understanding and mitigating dependencies on single providers for critical functions is one aspect of this, but so is having a game plan in place for how to respond if and when these incidents occur.

Open-source technology environments are perfect for firms seeking to adapt quickly and flexibly to changing market and competitive conditions. They can enable also firms to avoid vendor lock-in and the competitive and operational resilience disadvantages that are inherent in depending on one provider. However, the adoption of open source comes with numerous challenges from a cybersecurity and governance perspective. Firms need to ensure that they are aware of the provenance and security of any open-source code they are using.

Firms don't have to go it alone on the journey to delivering a truly hybrid architecture. Working with an external partner that has both the capabilities and the experience to support firms evaluating, transitioning to or supporting a hybrid cloud environment can ease the burden. Hybrid cloud experts can help to ensure that decisions are informed by industry best practices and that environments are designed for a more devops approach to data to support changing business, client and regulatory requirements.

Key Takeaways

- **Modernize on premises legacy technology to bring it into line with public cloud:** Firms will need to ensure that their on-premises technology is fully compatible and seamlessly connected to their cloud native architecture. Existing gaps and inefficiencies need to be addressed by transforming legacy IT into a private cloud architecture and therefore delivering a truly hybrid cloud environment that can scale and support future business needs.

- **Evaluate the risks of these new approaches to cloud infrastructure:** A hybrid cloud environment means data is moving between on premises and cloud technologies and this means a different approach to data security and monitoring is necessary. Open-source software-based environments allow for greater flexibility, resilience and avoidance of vendor lock-in, but they need to be implemented carefully to avoid increasing cyber-risk. The provenance of code needs to be carefully traced and governance frameworks need to be in place for developers across the firm.

- **Firms need to strategically rethink their application platforming approach:** Industry licensing models are changing for virtual machine infrastructure and this means firms need to understand the impact of those changes and any others as part of a wider strategic re-evaluation of their overall cloud infrastructure environment. Operational resilience requirements may be causing financial services firms to immediately assess CSP dependencies, but this strategic evaluation should extend to the full environment and the related underlying costs. Firms need to decide how to reduce dependencies on virtual machines as necessary such as adopting open-source technology and/or moving to containers.

We're passionate about capital markets research

Our expertise is in providing research and advisory services to firms across the capital markets spectrum. From fintech investments to business case building, we have the skills to help you get the job done.

- The voice of the market
- Independent
- Built on decades of research
- Practical not posturing
- Diversity of approach
- Market research should be accessible

For more information visit fintechfirebrand.com or email contact@fintechfirebrand.com