



Kyndryl Private Cloud Offers Secure and Compliant Modernization for Financial Services Firms

*“Banks have enormous competitive threats—from virtually every angle.
... We must get faster and be more creative.”*

— Jamie Dimon, CEO, JPMorgan Chase & Co. [in a letter to shareholders, April 2021](#)

Established financial services firms

are facing unprecedented new challenges, ranging from increased regulatory scrutiny to cryptocurrency and a wave of financial technology (fintech) competitors. Those are among the reasons banks, brokerages, investment firms, and others in the business of managing money are marching deliberately toward the cloud.

Despite getting a late start, financial services companies are making up for lost time. In a Celent survey of financial services firms conducted in late 2019, one-third of the respondents said they [expect to have 75% of workloads running in the cloud](#) within three years, and another 21% expect to reach that milestone within five years. The Cloud Security Alliance’s February 2020 [“Cloud Usage in the Financial Services Sector”](#) report found that 91% of the surveyed financial institutions were actively using cloud services or planned to do so within the next six to nine months, a figure that has doubled since 2016.

Numerous forces are driving this migration.

Better customer experience. The need to deliver better and more personalized customer experiences is fueling investments in data-intensive analytics and AI applications, which are themselves rapidly moving to the cloud.

Mobile services. Customers’ growing use of mobile services demands that financial institutions adopt cloud platforms to serve customers anytime and anywhere on any device.

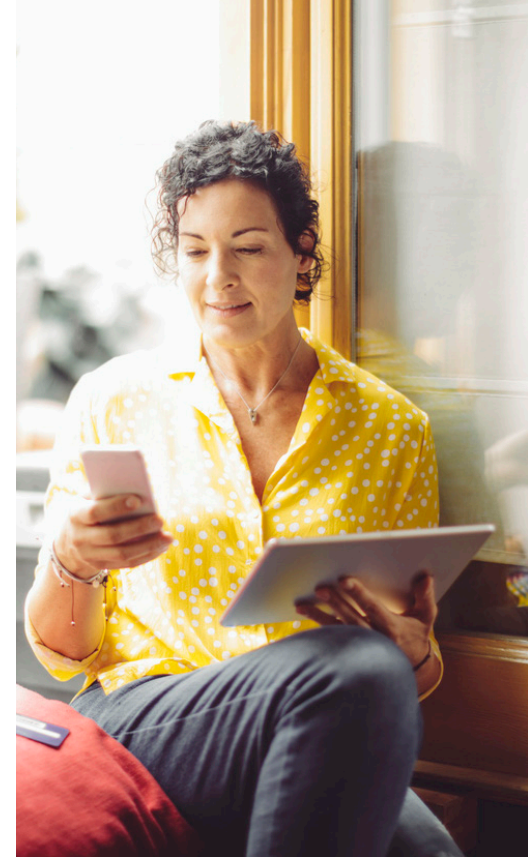
Industry pressure. Financial firms are expanding into each other’s space, with banks offering advisory services and insurance and stock trading firms opening banking practices.

Digital customers. Consumers’ growing preference for digital interactions, versus branch visits, is pressuring banks to find ways to differentiate their services—especially since all online banking sites look pretty much the same. This is fueling investments in mobile apps, kiosks, and self-service capabilities powered by AI and delivered from the cloud.

Competitive pressure. Fintech firms [attracted more than \\$105 billion](#) in investment in 2020. They pose an existential threat to some established financial firms but also represent a partnering or acquisition opportunity.

Digital currencies. Many financial firms are investing in new infrastructure to support blockchain-based transactions and digital currencies such as bitcoin.

Cost savings. The ongoing need to reduce costs makes cloud’s operating expense model an attractive alternative to the large capital costs of on-premises computing.



Consumers’ growing preference for digital interactions, versus branch visits, is pressuring banks to find ways to differentiate their services.

CLOUD AT THE CENTER

At the same time, the global pandemic has underlined the value of flexible infrastructure that can accommodate use surges and enable rapid application deployment. Many businesses that were largely dependent on on-premises legacy infrastructure were caught flat-footed by lockdowns that deprived them of critical staff and mandated social distancing within their data centers. With high levels of automation in place, cloud providers and their customers were impacted to a much lesser degree.

Cloud computing offers a path to agility by enabling firms to tap into technologies such as microservices, machine learning, cloud-native development platforms, and data lakes. These technologies can help enterprises speed the delivery of new services, support mobile transactions, and gain customer insights that open up new lines of business.

“A standard cloud platform creates an even playing field where companies can seamlessly integrate capabilities into existing applications, bolt on new features, and remove them when they’re no longer needed,” says Matt Milton, President of Kyndryl US.

Platforms based on cloud-native technologies such as containers, microservices, and application program interfaces (APIs) give financial firms a way to make their business more agile and flexible at a cost that’s equivalent to or lower than that of legacy infrastructure.

THE BENEFITS FALL ALONG SEVERAL LINES

Unified compliance and security practices make reporting and administration simpler. Having high levels of automation on cloud platforms enables access control and identity management via policies versus manual intervention. Cloud providers also have significant experience in emerging security practices such as zero trust and secure access service edge (SASE), which means that their customers don’t have to develop those skills internally.

Customer experience is a critical consideration, particularly in consumer markets. Respondents to the Celent survey rated customer experience the third-most-important driver of cloud migration. As they move to the cloud, many businesses adopt agile development techniques to deliver clean, consistent, and extensible customer interfaces that flex to accommodate new services and advances such as AI-assisted customer service across multiple platforms.

New functionality can be deployed from cloud marketplaces or via software as a service (SaaS). Either is vastly superior to the often-months-long practice of installing, testing, and deploying packaged applications. Modern cloud applications are also updated continuously, eliminating the need to maintain backward compatibility with legacy software.

Application development can be overhauled and streamlined to enable faster delivery and greater innovation. Agile development using platform-as-a-service (PaaS) tools enables continuous development and delivery and involves business constituents closely throughout the process. Frequent code releases and a “fail fast” dynamic encourages experimentation and promotes innovation. “The cost of failure has never been lower, and that is significantly driven by the speed and scale nature of the cloud,” Milton says. “You can ramp up quickly, fail fast, and move on to the next opportunity.”

Processes can be improved with a raft of cloud-based tools that research firm Gartner classifies as “hyperautomation.” This includes intelligent business process management, integration PaaS, event brokers, intelligent document capture software, and virtual assistants. Research firm Forrester expects finance and accounting firms to be the **dominant users** of software such as robotic process automation over the next two years.



Cloud computing offers a path to agility by enabling firms to tap into technologies such as microservices, machine learning, cloud-native development platforms, and data lakes.

Streaming analytics enabled by cloud-based platforms enables financial firms to smoothly incorporate real-time trading data into customer-facing platforms and take advantage of advanced security capabilities such as point-of-sale fraud detection.

Cloud platforms protect against obsolescence, by separating code from underlying infrastructure. The risk of being locked into specific platforms or old versions of software is minimized, because extensions are enabled through published interfaces rather than directly in the applications themselves. Companies need to be sensitive to the risk of lock-in, because “what is best today for your workload may not be best tomorrow,” Milton says.

Cloud-based applications consume and deliver services through APIs. This gives financial firms a granular degree of control over how data is exposed and enables them to easily integrate third-party data sources. Having the option to publish data via APIs to business partners and consumers also opens up new business opportunities.

Cloud service providers have already invested in a tried-and-tested technology stack. Maintenance, support, and upgrades are built into the operating cost. Cloud return on investment (ROI) is further enhanced by faster speed to market and lower total cost of ownership.

The IT skills shortage impacts companies in every sector, but the cloud means that IT personnel can be redeployed from low-value activities such as equipment maintenance to tasks that more directly affect the business.

PUBLIC CLOUD IS NOT ALWAYS THE ANSWER

Migrating from legacy infrastructure is a complex and lengthy process, however, particularly when data locality, privacy, and security regulations must be observed in every jurisdiction in which financial institutions operate.

“Financial services businesses constantly battle the need to innovate and differentiate while running in the most complex and regulated environments in the world,” Milton says. “Everybody’s budget is also constrained, so these businesses need to realize the full value of their investments. Public cloud is not always the answer.”

In the US, for example, banks must comply with at least 10 major regulations at the federal level alone. Many states also have their own rules. For firms doing business overseas, the complexity is magnified.

In fact, institutions that do business in multiple states or countries may literally be subject to hundreds of regulatory controls. And the rules are constantly changing. Some companies must complete thousands of compliance-related reports per year, each requiring full documentation and auditability.

Cyberresilience requirements also weigh heavily on technology choices. “Regulatory frameworks outline responsibilities to prevent and protect against cyberattack, but you also need to be able to show that you can sustain your business and get back up and running quickly,” Milton says. “The expectation is that systems always work and are always on.”

Complexity is amplified when a business is working with multiple cloud providers, each with its own policies and procedures in areas such as security and compliance. A multicloud environment, which is used by over 90% of enterprises, spreads responsibility for meeting regulatory goals across multiple platforms, applications, and regions, with the onus being on the financial services business to ensure that rules are obeyed.

The result: Many decisions about placing and securing workloads must be made on a case-by-case basis. Some cloud platform providers also insist on maintaining control over customers’ encryption keys, a requirement that is a nonstarter for tightly regulated financial firms.



“Financial services businesses constantly battle the need to innovate and differentiate while running in the most complex and regulated environments in the world. Public cloud is not always the answer.”

— Matt Milton,
President of Kyndryl US

Data sovereignty policies also vary among providers. Some jurisdictions require that customer data be stored in specific locations, a stipulation that not all cloud providers can accommodate. Data disclosure regulations also vary by jurisdiction and apply not just to where data resides but also to how it is encrypted; what masking controls are in place; and how access is governed for different people, locations, and businesses. And widespread confusion still exists about the shared-responsibility security model that puts some demands on the infrastructure provider and others on the customer.

On top of all this, financial services firms assume greater data protection responsibilities in the cloud than do businesses in other industries. Regulations require that they protect customer data on-premises, in transit, and in the cloud. Not all cloud providers support an end-to-end zero trust security architecture in which all requests for data access are subject to authentication. That leaves it up to organizations to ensure that such controls are in place for each provider.

Not all cloud vendors have the full range of needed controls. Although their services may adhere to major regulations such as Payment Card Industry Data Security Standard (PCI DSS), it is often up to institutional customers to determine and manage how the applications they build, and/or the SaaS providers they use, comply with regional regulations. Some regulations are also specific to subsectors such as insurance or banking and require formal risk mitigation policies.

THE BENEFITS OF PRIVATE CLOUD IAAS

A managed private cloud solution balances the need for control with the goal of cloud enablement. It enables financial firms to migrate applications at their own pace while giving internal development teams access to a vast array of cloud-native tools to build new services and enhance existing ones more quickly.

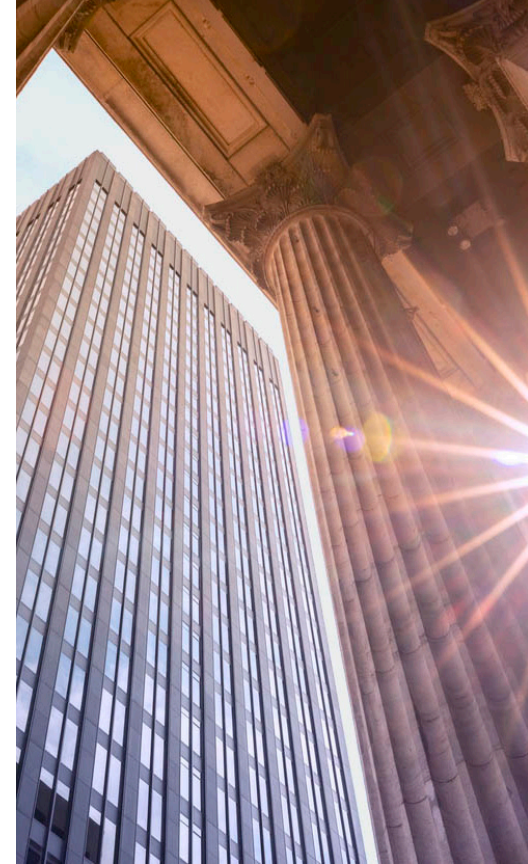
Business managers can immediately leverage cloud analytics to mine value from their existing data. Legacy applications can be fitted with customer-friendly front ends powered by AI. Data and applications can then be migrated to thoroughly vetted cloud providers at the customer's pace. All this is possible without ceding the controls and governance that are so important in a regulated industry.

A private cloud also offers attractive options for modernizing the legacy mainframe applications that are common in established financial services firms. Despite often being decades old, many of those applications are critical to the business and can't be taken offline for rework. Legacy applications also may harbor undocumented or poorly understood interdependencies with other programs. Removing them from production can create a cascade effect of failures, with catastrophic consequences.

Modernizing these applications in the public cloud is often too risky to be practical. A private cloud provides a set of modernization tools that are compatible across cloud platforms and don't require production applications to be taken out of service. That gives businesses the leeway to update on their own schedule and either redeploy on their private cloud or migrate to a public environment.

A private cloud offers a highly available, scalable environment that takes advantage of scale-out elasticity to enable legacy applications to be modernized without being entirely rebuilt. "Private cloud gives you the benefit of some standardization, scalability, and automation. You get a suite of contemporary services and market-tested AI capabilities," Milton says.

Many firms will ultimately want to migrate to public infrastructure to gain even further latitude. "As you move to the public cloud, you get continuously added and updated services, unlimited scalability, and the option to move across regions for growth or disaster recovery purposes," Milton says. "You can then think about decoupling workloads from the underlying infrastructure and taking full advantage of new services." A managed private cloud provides the safest path to that goal.



Financial services firms assume greater data protection responsibilities in the cloud than do businesses in other industries.

PARTNERSHIPS ARE CRITICAL

PwC has estimated that 75% of digital transformations fail to deliver the anticipated benefits. With migration to a cloud environment representing an essential step in transformation, it is critical that financial institutions select a cloud partner with extensive experience managing on-premises, private, and public cloud environments.

A trusted partner can help answer such critical questions as:

- **Which applications** should be migrated and to which environment?
- **Where** should development resources be focused?
- **How should responsibilities** for security and compliance be defined between the customer and the cloud provider?
- **What are the terms** of service-level agreements (SLAs)?
- **Which applications** should be modernized and how?
- **What PaaS capabilities are needed**, and which providers are best equipped to provide them?
- **How will staffing considerations** be resolved, given that new skill sets will be needed and others phased out?
- **How will we transition** to devops and other agile principles?
- **How should stakeholders prepare** for the transition?
- **What key performance indicators** should be put in place to evaluate migration options, ROI, and success?

Kyndryl¹ offers a fully managed private cloud on clients' premises, so critical data remains safe. Kyndryl Private Cloud has a service availability approaching five-nines,

¹ Kyndryl was spun-off of IBM IT infrastructure services in 2021. Kyndryl's global base of customers includes 75 of the Fortune 100 companies. With 88,449 skilled professionals operating from over 100 countries, Kyndryl is committed to the success of our customers, collaborating with them and helping them to realize their ambitions

and Kyndryl services cover technology evolution and selection as well as hardware and software maintenance and monitoring. Customers get a full cloud stack that also provides a choice of products, ranging from operating system and hypervisor to container orchestration with Red Hat OpenShift.

Kyndryl is committed to open platforms that maximize portability options for customers and benefit from the crowdsourced innovation of open source ecosystems. Open platforms evolve more quickly than proprietary ones, provide greater investment protection, and protect customers against obsolescence. "We are focused on every solution we create being open and portable," Milton says.

With long-standing relationships with most of the world's top financial institutions, Kyndryl has a long history of creating and managing complex ecosystems and market transitions. Kyndryl brings deep expertise in all facets of the financial industry and an understanding of the operating models and business processes that must be redesigned and infused with new technologies to help banks transition to new operating models.

THE BOTTOM LINE

Concerns about regulation, cybersecurity, and investment protection need not hold financial services firms back from realizing the benefits of cloud platforms. Public clouds have evolved, with robust options specific to their needs—but managed private cloud delivers many of the benefits of virtualized infrastructure in a fully protected environment. Adopting a private cloud based on open standards gives companies the option of choosing the most appropriate platforms for their needs without fear of being locked in for the long term.

For more information on Kyndryl Private Cloud, visit <https://bit.ly/kyndrylprivatecloud>.



Kyndryl is committed to open platforms that maximize portability options for customers and benefit from the crowdsourced innovation of open source ecosystems.