Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

December 3, 2021

Bank Use of Cloud Technology

The banking industry has been a prominent, if sometimes skeptical, adopter of cloud technology. Proponents promise scalability, flexibility, and cost savings, among other benefits. However, the technology also introduces potential operational risks and policy concerns, such as systemic risk. Banking's steady, but not advanced, adoption of this technology (as shown by its position along the "adoption curve" in **Figure 1** below) reflects this trade-off.

What Is the Cloud?

Put simply, cloud users pay cloud service providers (CSPs) to use CSPs' computing resources (e.g., servers and mainframes), rather than purchasing and maintaining their own. According to the National Institute of Standards and Technology, cloud computing is a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources." By the same definition, the five hallmark characteristics of the cloud are (1) on demand service; (2) broad network access; (3) resource pooling; (4) rapid elasticity; and (5) measured service, or the ability to monitor or limit quantities used.

Transferring the maintenance of computing resources to a CSP allows banks to avoid certain administrative tasks (such as patching and backups) and investment costs. Cloud services also allow a company to quickly grow and then shrink with demand, paying only for what it used.

There are four ways banks and other companies may deploy cloud technology, often called cloud deployment models:

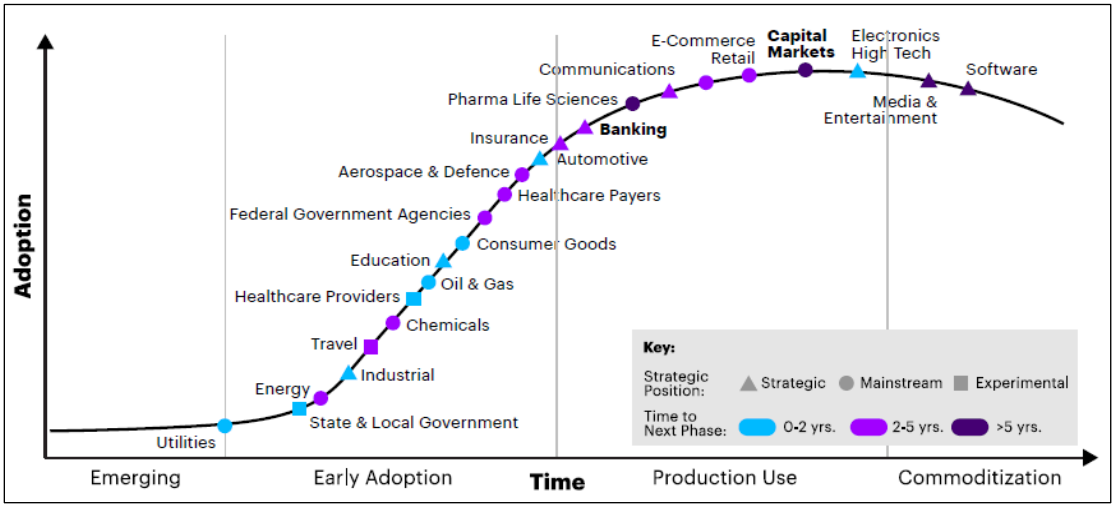
(1) **Private cloud:** resources are dedicated to and for sole use of one company. These services can be hosted on premises or off-site, and may be managed by the company or a third-party provider.
(2) **Public cloud:** companies share resources in the same data center and possibly the same physical server at the site of the cloud service provider or a third-party facility.
(3) **Hybrid cloud:** a model that employs both private and public cloud solutions.
(4) **Community cloud:** entities with a similar purpose share cloud infrastructure.

Banks and the Cloud

One survey revealed that, prior to the COVID-19 pandemic, nearly 91% of banks and other financial institutions were using the cloud or considering using it in the near future. Since the pandemic, media reports suggest cloud adoption has increased as banks sought to cut costs, meet public demand for online services, and manage teams of remote workers. Still, while bank adoption of any cloud service is relatively high, the overall percentage of bank workloads in the cloud is comparatively low. One consulting firm that works extensively with banks and other financial institutions has estimated that between 8% and 10% of global bank business is conducted in a cloud environment.

Generally, banks are more likely to migrate to the cloud functions that focus on internal bank business, including finance, legal and regulatory compliance, and human resources (sometimes referred to as enterprise applications). On the other end of the spectrum, core banking services are likely to be among the last to convert. Core banking services refer to the systems that facilitate vital bank business, including processing transactions, updating accounts, and reconciling ledgers.

Figure 1. The State of Cloud Adoption



Source: Accenture.
Notes: Strategic: adoption of cloud is intended to confer a competitive advantage. **Mainstream**: adoption is common among businesses in the industry. **Experimental**: not in full production; business success does not hinge on cloud use.

Benefits to Banking in the Cloud

Banks have migrated to the cloud from on-premises infrastructure solutions for a number of reasons, including saving time and money, improving security, and gaining flexibility. Adopting the cloud can help banks avoid the cost of initial investment and regular maintenance of computing infrastructure. In addition, banks no longer have to designate personnel and physical real estate or account for the associated costs when they outsource solutions to off-site CSPs and data centers, particularly in a public cloud deployment model. Storage of applications and data in the cloud provides enhanced operational resilience for periods of disruption. Some argue that banks are (potentially) safer in the cloud because cloud service providers invest heavily to protect against cyberthreats. Running applications in a "platform-as-a-service" model allows banks to test and deploy application upgrades on a rolling basis instead of through significantly more momentous and time-consuming upgrades. Finally, access to advanced computing power may allow banks to perform advanced analytics on customer data.

Risks

Due to the highly regulated nature of banking and policy focus on safety and soundness, banks have historically been somewhat skeptical about adopting cloud technology, citing potential risks. Cloud use does not generally elevate typical bank risks, including market, credit, and liquidity risk. Instead, cyber, operational and vendor, and associated regulatory compliance risks are bigger concerns.

Cyber risk: Exposures to cyber risk change, and may increase, for banks with increased reliance on advanced information technology (IT) solutions, including the cloud. On one hand, CSPs are arguably more adept at managing certain types of attacks, as they have specialized workers managing security across all their clients. On the other hand, banks are targeted by unique adversaries employing novel attacks because of their high exposure to IT and their role in credit intermediation.

Third-party service provider (TSP) risk: From a regulatory perspective, banks are still responsible for negative consequences that may occur as a result of using a TSP, including a CSP. Moreover, in a shared responsibility relationship, banks and CSPs are responsible for discrete tasks of a shared work stream. It is therefore incumbent on each to know where one's responsibility ends and the other's begins. Failure to do so may cause misconfiguration risk, which occurs if either party fails to satisfy one of its responsibilities, such as selecting the appropriate security settings. Moreover, compliance and operational failures rising from the reliance on TSPs may also create reputational risk.

Policy Issues

Broader risks to bank adoption of cloud technology pose certain policy issues that may be of interest to Congress.

Concentration: The cloud market is concentrated in three CSPs—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud—that collectively account for between 60% and 70% of market share. In its 2019 Annual Report, the Financial Stability Oversight Council discussed the risk that stems from high concentration among few providers, noting that a "service interruption or cyber event at a critical vendor with a large number of clients could result in widespread disruption in access to financial data and could impair the flow of financial transactions." Traditional bank risks such as market and liquidity risks, not normally cloud computing concerns, can rise if the banks' abilities to transact are impeded by cloud-related disruptions.

Antitrust: Obstacles to data portability, such as proprietary technology and restrictive vendor contracts, may make switching CSPs difficult. In addition, barriers to entry for new providers are high because entry into the cloud market requires massive investments in IT infrastructure. Accordingly, competition issues in the cloud industry may be of interest to Congress. Various antitrust bills were introduced in Congress in the summer of 2021 to curb the power of large technology platforms. H.R. 3849—which would impose interoperability and data-portability requirements on certain tech platforms—may be relevant for CSPs, though it is unclear whether the bill as drafted would encompass such firms. In June 2021, the House Judiciary Committee reported the legislation to the House floor. As Congress considers the bill, it may seek to clarify whether CSPs would be subject to its requirements.

Financial Crimes Investigations: Another relevant policy issue is the role that CSPs may play in financial crimes investigations. According to a report from the Federal Reserve Bank of San Francisco's Fintech office, privacy-enhancing technologies typically make it difficult for CSPs to read data under certain circumstances. However, as "detailed information is required to prosecute financial crime ... there is a question as to how much granular identifiable information entities, and service providers, like cloud storage, should be able to provide."

Bank supervision: The scope of bank supervision may expand to CSPs as the cloud becomes more integral to bank operations. This may lead to technical resource mismatches as well as relationship management issues for CSPs that may not be used to thorough inspections. The Federal Reserve Bank of Richmond performed a formal exam of AWS in April 2019. Close integration between banks and cloud providers may accelerate regulators' call for regular examination of CSPs to monitor aspects of their relationships with banks, including security and financial system stability risks.

CRS Resources

CRS Report R46332, *Fintech: Overview of Innovative Financial Technology and Selected Policy Issues*, coordinated by David W. Perkins

CRS Report R46119, *Cloud Computing: Background, Status of Adoption by Federal Agencies, and Congressional Action*, by Patricia Moloney Figliola

CRS Report R46875, *The Big Tech Antitrust Bills*, by Jay B. Sykes

Paul Tierno, Analyst in Financial Economics

IF11985

Disclaimer