CELENT

PUBLIC CLOUD ADOPTION IN FINANCIAL SERVICES

7 KEY CONSIDERATIONS FOR CIOS AND OTHER KEY STAKEHOLDERS

Craig Focardi and Stephen Greer
08 July 2020

This report was commissioned by IBM at whose request Celent developed this research. The analysis, conclusions, and opinions are Celent's, and IBM had no editorial control over the report contents.

OLIVER WYMAN

CONTENTS

EXECUTIVE SUMMARY

Public cloud adoption has been growing steadily in many industries. Financial institution (FI) cloud adoption has been slower, though, because these firms are heavily regulated due to the large amount of confidential financial customer information they possess. FI information security; risk and compliance; and ecosystem management, integration, and control preferences are exceedingly high. As a result, many banking applications in the public cloud today are not mission critical or do not directly expose core systems and databases.

However, banking industry attitudes toward the public cloud are changing. First, large financial institutions have begun exploring public cloud use cases. For example, 19 of the top 20 banks in the US have already announced public cloud initiatives. Second, fintech challenger banks and smaller financial institutions have implemented core banking platforms and other mission-critical systems in the public cloud.

Institutions are examining additional opportunities while addressing any security, risk, compliance, and ecosystem issues. As the business case is made for broader public cloud adoption, banks will have to evaluate a variety of considerations that could influence not only where they deploy technology, but also how they deploy it.

This report focuses on public cloud adoption in financial services, and addresses public cloud adoption to date, market drivers making public cloud more attractive to financial institutions, and issues that financial institutions should assess when planning and executing their technology transformation and public cloud migration strategies. Here are seven critical considerations for public cloud adoption that Celent has identified:

1. Security and trust
2. Risk Management and compliance
3. Ecosystem partner management
4. Customer experience
5. Cost management flexibility
6. Agility to innovate faster
7. Operational efficiency

The focus within financial services is on the banking (lending and payments), risk and compliance, and IT business areas. This report is designed to help CIOs and other senior executives evaluate the merits of a public cloud by highlighting the considerations to include in the evaluation process. The report also balances longer-term trends with the current imperatives created by the COVID-19 pandemic.

Who Should Read This Report?

The report assesses public cloud adoption in financial services and the needs of:

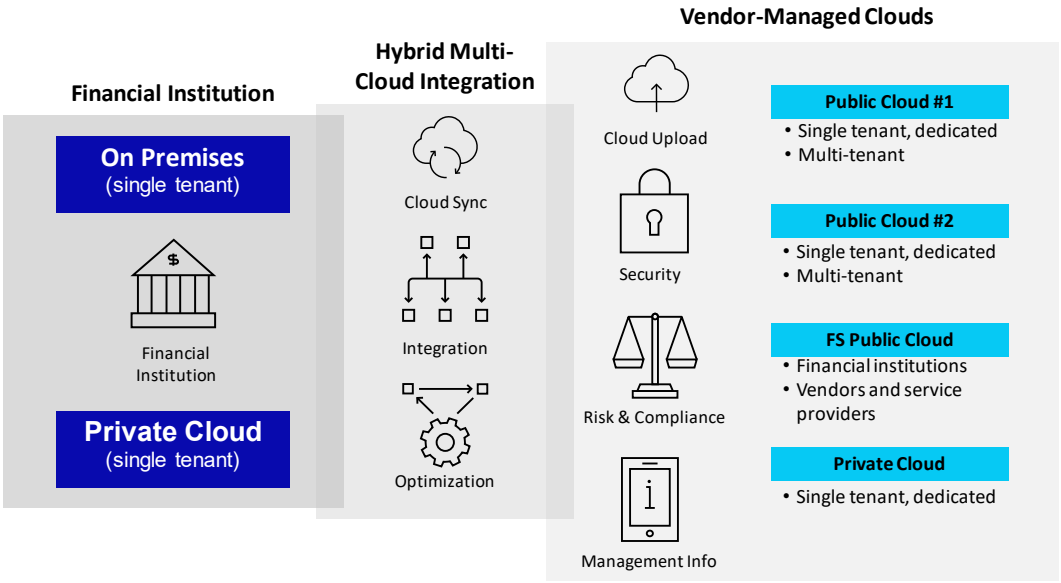
- CIOs: chief information officers and senior staff responsible for long-term technology vision, strategy, development, and maintenance.
- CISOs: chief information security officers responsible for assessing IT risks and other security risks that impact the business.
- CROs: chief risk officers responsible for compliance, operational, financial, asset, and other forms of risk.
- LOBs: line of business heads responsible for revenue generation and the centralized corporate support function.

PUBLIC CLOUD GROWTH IN A HYBRID CLOUD WORLD

Cloud computing, the on-demand availability of computer resources—especially data centers and computing software—has been the source of both vendor evangelization and bank CIO resistance for two decades. Once deemed by some as simply a computer connected to a network, and a technology deployment method with a fancy name in search of a market, cloud computing continues to grow steadily every year.

Most regulated financial institutions were born on the mainframe computer, not in the public cloud. As a result, these two worlds were initially far apart. However, years of evolution—from mainframe computers to personal computers to client servers to n-tier web-based servers and n-tier servers located anywhere—closed the gap between the public cloud and older computing platform environments. This has enabled FIs to migrate to any cloud computing environment. Figure 1 depicts typical computing environments and deployment models present at many financial institutions.

Figure 1: Technology Deployment in a Typical Large Bank



Source: Celent

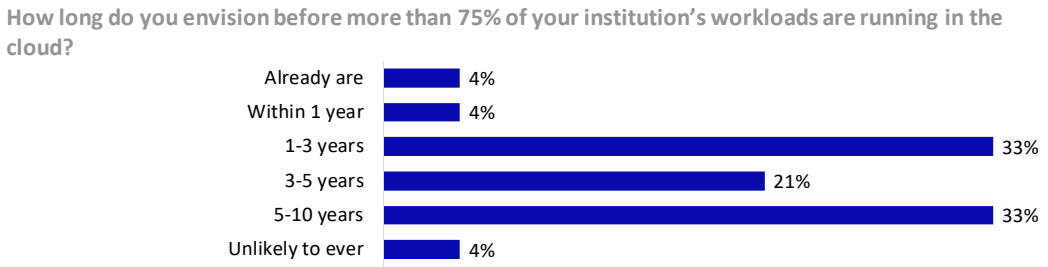
Financial institutions may use a variety of cloud environments:

- **Public**: The cloud services are available to the public, can be used by anyone, and share computing services among different customers. Each customer's data and applications remain hidden from other cloud customers.
- **Financial services (FS) public clouds**: Cloud access and usage are open only to a defined group of entities that share common goals and transact with each other. Cloud usage is managed by one or more group members, and may have a specified set of security, resiliency, regulatory, and compliance requirements.
- **Private**: This is a single-tenant cloud that may be located on premises or at a third-party site.
- **Hybrid multi-cloud**: A firm's deployment is split between public and private cloud locations. Larger FIs are likely to operate in a hybrid cloud environment to support interoperability between on-premises and public cloud applications.

Cloud Adoption Is Growing

Cloud computing is flourishing within financial services and other industries. A typical financial institution computing environment already includes on-premise systems, off-premise systems, and multiple clouds. In the coming years, cloud computing in financial services is expected to grow steadily. In a Celent FI survey, shown below in Figure 2, 33% of respondents indicated that it would only take between one and three years to reach 75% of workloads running in the cloud. Another 20% said it would take three to five years. This means that more than half of financial institutions expect to run their workloads in a cloud within five years.

Figure 2: Workloads Are Moving Rapidly to the Cloud[1]

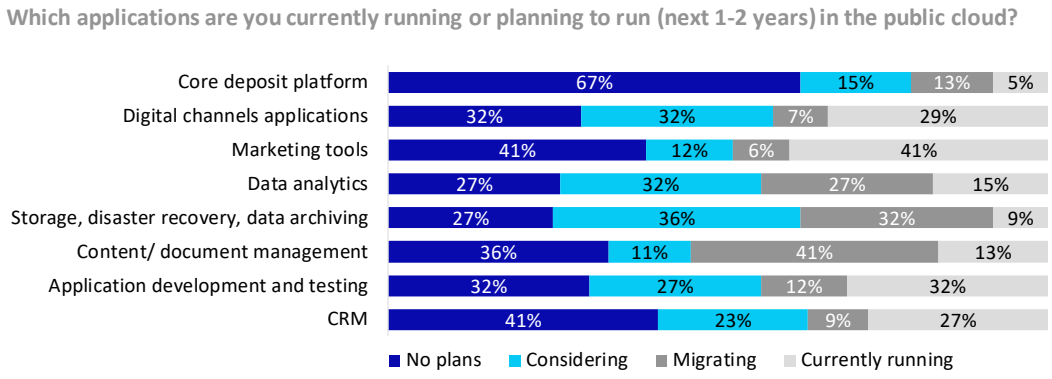


Source: Celent FI Survey, December 2019

Cloud adoption to date and changes in market drivers are making the public cloud more attractive to financial institutions. Consider, for example, that this survey was taken in December 2019 before the COVID-19 pandemic began. The pandemic is now driving firms to operate virtually and digitize the workforce, business models, and technology. The cloud provides an ideal solution for more digital and remote operations.

Figure 3 shows cloud adoption results from the Celent survey based on technology system and function. Celent asked FIs which banking technology applications they are currently running or planning to run in the public cloud within the next one or two years. The results vary considerably by system type.

Figure 3: Cloud Adoption Varies by Application Type



Source: Celent FI Survey, December 2019

Risk and reward have always been at the heart of the cloud adoption discussion. In general, financial institutions (FIs) weigh security, risk, and control against the many

[1] The Celent Survey was completed by 88 financial institutions in December 2019. They ranged evenly from large banks (>$50bn assets) to small community (<$10bn assets), with roles being primarily C-level or head of digital.

benefits. Risk versus reward has been an especially important consideration for FIs who hold vast amounts of confidential financial data for businesses and consumers. The survey indicated that for many FIs, deployment of the core deposit ("core banking") system will be one of the last technologies to move to the public cloud.

Banks are moving to the public cloud, and while there are many considerations, there are also myriad benefits.

The Case for Migration to the Public Cloud

While the public cloud isn't a silver bullet for every banking technology and strategy, it offers some significant benefits when compared with traditional IT deployments. Once hesitant about risk perceptions related to cloud deployment, the financial services industry has aligned the public cloud's tangible and indisputable advantages with an increasing number of applications. In fact, Celent has found that even after conversion, some institutions continue to find value beyond the initial cloud business case. Public cloud won't be right for every application, but Celent sees the following benefits most closely associated with adoption.

- **Infinite scalability.** Cloud allows an application to be "right-sized" and grow as demand requires. Equally, it can be scaled back when not needed. This eliminates the need to invest in unused capacity, where in many banks systems 90% of capacity is typically idle for 90% of the time. Cloud offers scalability beyond vertical or horizontal—such as diagonally—with provisioning for cloud-native applications happening almost instantly.
- **Agility and speed to market**. Cloud enables banks to use standard building blocks to innovate and create tailor-made solutions for their clients. Furthermore, the solutions can be rolled out "on the fly," and the platform itself can be updated in real time as well. In a SaaS deployment model, new enhancements can bring a bank up to date immediately—no more wrestling with downtime and old versions of software. With continuous development and continuous delivery platforms, banks can instantly roll out application enhancements in an agile way.
- **Infrastructure cost efficiency**. While not always cheaper, cloud provides some cost optimization. Cloud service providers have already invested in the technology stack to make it work, and ongoing investment costs are shared by all the users. The maintenance and support of that technology and ongoing upgrades are also part of that cost. In addition, given the competition among cloud providers, that investment is significantly higher than virtually any financial institution could make on their own. The return on investment for applications brought to the cloud is enhanced by the speed to market and lower total cost of ownership (TCO).
- **Security and resiliency**. The cloud vendors have invested significant sums of money to meet all the necessary regulatory security standards and regulations that banks face. With the cloud, security will be stronger and more sophisticated than any single financial institution could devise. Community clouds are being established which provide industry-specific capabilities and solutions, though certain cloud partners may excel more than others.
- **Future proofing**. Change, as the saying goes, is constant. How do you plan for the downstream consequences, or indeed, those we can't even imagine? Cloud computing helps plan for the unimaginable.

Financial institutions across the globe continue to take different paths toward cloud migration. No one deployment model will meet every need—banks will certainly mix and match—but the industry is moving quickly. The following sections explore critical considerations for institutions as they migrate to a public cloud environment.

SEVEN KEY CONSIDERATIONS FOR STAKEHOLDERS

As cloud computing grows from being a small part of a financial institution's computing environment to becoming the dominant computing paradigm, its impact on the entire firm increases. Structural changes to processes, personnel requirements, and technology will prompt new stakeholders to consider the cloud in light of the way they do business.

To address this evolving strategic transition, Celent has identified seven key considerations for CIOs, CISOs, CROs, and line of business stakeholders. Figure 4 outlines these considerations across three broad categories: security, risk and compliance; ecosystem management; and current operations and strategic planning.

Figure 4: Seven Key Public Cloud Expansion Considerations for Financial Institutions

Source: Celent

To put these considerations into context: Security, risk, and compliance remain the most important considerations for any incumbent business that operates at high scale. Operational and strategic objectives provide multiple reasons for undertaking cloud initiatives. Ecosystem management involves using cloud capabilities to speed implementation and provide greater value to customers. Better customer experiences help retain existing customers, acquire new customers, and cross-sell to them.

KEY CONSIDERATION #1: SECURITY AND TRUST

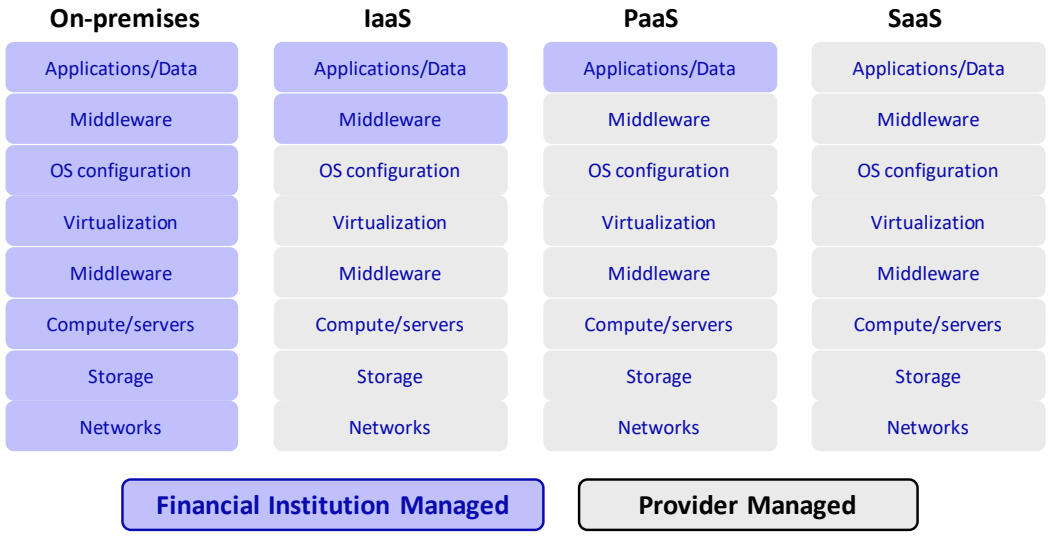
Banks are large and primary targets for some of the worst cyber criminals in the world. Digital financial services, especially in retail banking but also in corporate banking, have only increased the security risks banks face. As such, maintaining a high bar for security is a critical consideration when looking at the deployment of data and infrastructure.

In December 2019, a Celent FI survey found that 54% of respondents said migration to the cloud (public, private, and hybrid) was "very impactful" to their cyber security spend. In the early days of the public cloud, a primary point of concern was the level of security available from public cloud service providers. Most FIs were hesitant to be leaders in public cloud because regulatory scrutiny and risk considerations presented considerable barriers. Over time, the technology and security has matured, and many banks have now

embraced large-scale shifts to the cloud. Even so, considerations around security continue to loom large. Institutions still ask many questions: Is data less secure in the public cloud? Do I have less control? How do I enforce bank-grade security measures? How is security affected by the deployment model?

Figure 5 depicts how the management responsibilities between FIs and cloud providers are assigned for three types of services available in cloud computing. In an on-premise environment an institution has total control and complete visibility over its infrastructure. The location of data, the roles and responsibility of the operators, and other security parameters are clearly defined internally. When an organization shifts to a cloud deployment model, there are additional considerations because both the bank and the cloud provider share responsibility. The way in which an institution adopts the cloud will impact the security and risk profile.

Figure 5: Management Responsibilities Between FIs and Cloud Providers



Source: Celent

Financial institutions need to think about a few main areas around public cloud security:

- **Clarity on security definition and monitoring**: Banks should evaluate the service provider's capabilities in establishing controls for monitoring and defining security requirements, specifically around regulatory needs.
- **Security tools**: Institutions should consider the breadth and depth of tools for cybersecurity. Identification, hardware security, and data privacy protection can be established as services, and each public cloud provider has a different capability set.
- **Control of the data**: Institutions will need to create the proper governance and policies about how data moves around in the cloud and what controls are in place to ensure data integrity and confidentiality. Increasingly, this includes a "Keep Your Own Key (KYOK)" capability which allows the institution to take full control of data encryption end-to-end. However, not all KYOK is alike, and some providers are better than others at meeting bank-grade security standards.
- **DevSecOps deployment models**: Service models will be a determining factor for how an institution approaches security in the cloud. Leveraging DevSecOps will allow organizations to embed good application security practices throughout the application build process. This is an agile framework reinforced with strong security.
- **Operating models around cloud security**: Cloud deployment and migration can create tension between transformation groups and cybersecurity teams. Institutions

will need to evaluate how they build security into the cloud operating model from an organizational perspective as well as around technology.

- **Trust and verify**: Similarly, public cloud may need to leverage a "trust and verify" approach. Cloud teams working autonomously are a must, but considerations need to be paid to identity verification. Trust services from cloud providers can enhance governance and allow for increased visibility.

Increasingly, certain institutions are looking into "community public clouds" as opposed to generalized public or private deployments. These clouds provide an infrastructure which is tailored to a specific industry or need. In the context of financial services, a community cloud can establish the parameters necessary to harden security to financial institution-grade levels. Cybersecurity is one of the biggest areas of risk for an organization and can devastate its reputation and business. That is why securing information in a public cloud is so critically important.

Key Consideration #2: Risk Management and Compliance

Risk management and compliance issues typically encompass an FI's broader risk concerns beyond information security. Currently, the COVID-19 pandemic has heightened these financial risks due to economic uncertainty and intensified crime risks (fraud and money laundering). Shifting to the public cloud also impacts operational risk, regulatory compliance, and other risks. These threats span multiple departments and functions, and therefore require governance, policies, and processes to communicate and align with the responsibilities of key stakeholders: IT, security, operations, compliance, and each line of business. By coordinating risk management and compliance issues across functions, financial institutions will shorten the timelines needed for internal approval to move additional IT applications into the public cloud.

Financial institution CIOs, CISOs, and CROs should focus on the following risk and compliance areas:

- Identify how public cloud expansion impacts the key responsibilities of each stakeholder and consider the people, process, and technology implications.
- Provide other key stakeholders with a framework of issues and questions to address as a result of public cloud implementation.
- Communicate the strategic vision and benefits of public cloud computing across the enterprise.
- Assess, meet, and monitor country-level compliance requirements. FIs need to identify the delta between inhouse and third party regulatory requirements and fill any gaps.
- Monitor risk management and compliance issues. CROs need to keep up with changing regulations and interface with other CxO's on new risk drivers and risk monitoring.
- Monitor and meet security-related compliance. Certifications such as ISO/IEC 27001 or SOC 1/2/3 security standards cover internal controls around data management, and FIs must vet the security, compliance, and engineering teams of cloud partners.
- Examine and evaluate business continuity and disaster recovery plans.

To manage these risks, financial institutions should focus on public cloud platform providers with the capability, experience, and framework to support their risk management and regulatory requirements. The foundation of this framework is built on our discussion in the information security considerations above. In addition, public cloud providers should have experience servicing financial institutions, and a deep bench of banking industry technology, risk management, and compliance experts to support it.

KEY CONSIDERATION #3: ECOSYSTEM PARTNER MANAGEMENT

Financial institutions typically have a large ecosystem of vendors (for software, IT services, and other services) for their on-premise operations. As FIs migrate to the public cloud, some of those vendors will follow them. However, FIs may move at a faster pace than some vendors, and may want to add new vendors. In addition, curating, adding, and managing vendors for the cloud requires additional internal resources. They can outsource this to cloud providers that can also enforce common criteria around security and compliance to enable a safe ecosystem.

Ecosystem management will also be related to how FIs deploy applications into a cloud environment. Whereas the on-premise approach has a high level of internal control, it also takes time. FIs can also outsource all or part of the vendor management function to trusted cloud providers, some who already have a large repository of vendors for financial institutions to utilize. Cloud providers can spread their vendor management costs across all their FI customers, which makes outsourcing attractive.

In addition, key stakeholders should focus on the following ecosystem considerations:

- **Determine cloud strategy by service type**: Which cloud service types will your FI adopt: SaaS, PaaS, and/or IaaS? These choices will impact many facets of ecosystem management, since different models will require different levels of institutional involvement and governance.
- **Consider the partner onboarding effort**: Cloud service providers vet and onboard new third party ecosystems partners to the cloud. FIs should select cloud vendors that they're confident know financial services and FI vendor/partners well. This gives an FI greater confidence in the process. In the context of public/community clouds, this onboarding process must include industry-specific requirements for security and compliance.
- **Include ecosystem migration partners**: It can be difficult to maintain data integrity and operations during a migration from on premise to cloud. In this context, ecosystem partners can provide valuable expertise, especially when they know the industry or company.
- **Establish common security criteria**: In order for an ecosystem to be safe, it needs common criteria for security and compliance to be well defined and communicated. Ecosystem partners need to be carefully managed, but often a trusted third-party can take on this role. Ecosystem partners with experience can also assist with considerations listed under security, like proper controls for data or proper monitoring.

Finally, it's worth noting that the public cloud is only the delivery mechanism for institutions deploying banking services. The true value of public cloud will be how an institution approaches building services for its customers based on cloud components provided within an ecosystem. Public cloud ecosystems are key enablers for success but require the proper strategy and approach to create significant value.

KEY CONSIDERATION #4: CUSTOMER EXPERIENCE

When migrating to a public cloud environment, Celent finds the conversation about its benefits usually starts with commodity infrastructure; that is, moving commodity hardware and software from internal capital expenditures ("CapEx") to variable cost operating expenses ("OpEx"). However, cloud maturity quickly leads to a broader conversation about public cloud in terms of customer experience. In fact, when Celent asked banks in a December 2019 FI study to rate the biggest drivers for migration to a public cloud, customer experience was ranked third out of ten drivers. It's worth noting that customer experience in this context means the end-user as well as the developer team.

There are some key technical considerations for customer experience in the cloud:

- **Agile or waterfall IT development for enhancements**: Institutions should evaluate the application development process and whether it makes sense to leverage agile methodologies. Agile development won't be right for every application, especially older, stable, mission-critical platforms which remain on premise. However, modern customer-facing applications will likely do best with modern development practices which attain much higher build velocity. There's a learning curve here, and banks may want to seek advice from a trusted partner.
- **Separation of cloud vendor and financial institution responsibilities**: Sometimes it makes sense for operating models to separate responsibility across instances. For example, a bank can decide to separate its own instance of a cloud provider from the vendor's instance. With a separate instance, the vendor has its own service level agreement (SLA) when it needs to scale up and manage the infrastructure. The FI can then manage other higher-value tasks without a vendor, and ensure that its customer experience standards are met.
- **Outage recovery time**: Some financial institutions are considering the public cloud for its response time to outages and other system downtime. Faster recovery time can make disruptions almost unnoticeable to the customer, which for certain applications may be significant. Vendors with multiple zones and data center regions hold an advantage here.
- **Current modernization efforts**: Traditional applications are difficult to modernize; depending on how critical they are to the business, they are often left in place and worked around rather than transformed. Short of full transformation, however, there is a middle way: API-enabled integration of containers and microservices allows specific pieces of functionality to modernize separately, faster, and with less risk than retaining a monolithic solution. This approach improves the customer experience while respecting the FI's other technology priorities.
- **Bridging new ways of working**: Traditional development organizations often lack the skills needed to fully leverage cloud-native tools and ways of working. To bridge this gap, institutions need to consider how a move to the cloud should be managed in order to maximize the positive effects on the customer experience.
- **Availability of tools**: Similarly, a large number of cloud-native tools exist which can amplify the user experience on the front end. AI services, for example, that a bank can not readily build themselves may be accessible through a public cloud provider's ecosystem.

Customer experience is arguably the most impactful competitive battleground in the industry today. Financial institutions need to think about where it makes sense for applications to run in the public cloud and how the public cloud can improve the customer experience.

KEY CONSIDERATION #5: COST MANAGEMENT FLEXIBILITY

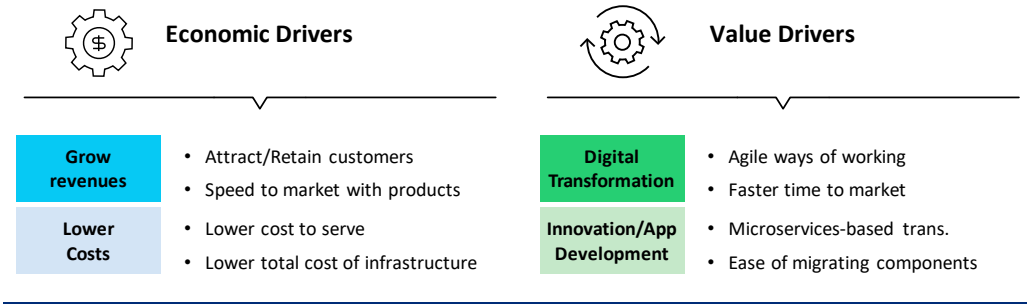
Cost is a major consideration for any institution looking to move to the cloud, but financial institutions' rationale for using the public cloud has shifted from a large reduction in costs to some cost reduction and a shift to variable costs. The CapEx to OpEx strategy is still valid but there is less focus on significant cost takeout.

While cost efficiency is always important, managing hybrid cloud (combined public cloud/on-premise infrastructure) usually adds costs. In addition, the cloud's seemingly infinite scalability can be both a blessing and a curse. Variable costs may spike depending on transaction volume and the speed at which batch workloads are processed. This may be by design; but institutions need to consider the process by which these levers are pulled.

Figure 6 looks at how many institutions have reconsidered the cost/value equation for cloud migration. Rather than cost reduction, banks should consider the economic drivers

behind public cloud; that is, how cost is *optimized* rather than simply reduced. Conversely, value drivers influence ROI and may justify a more neutral position toward the cost of public cloud migration. Celent has found that institutions are no longer considering public cloud as a significant driver of cost reduction, but rather as a longer-term technology flexibility and optimization strategy that will pay additional dividends over time through access to ecosystems, scalability, and resiliency.

Figure 6: Cost Management Now Focused on Economic Value, Not Maximizing Cost Reduction



Source: Celent

Because the goals for cloud migration can often straddle the line between economic drivers and value drivers, a financial institution will need to rank its priorities. Banks often have to balance different parameters in a cloud deployment and decide between premium services or a more basic migration. For example, there are cloud migration services or auto-scaling to run batch processes in a matter of minutes. In this scenario cloud won't provide a cost reduction benefit but will be more of a value driver.

Alternatively, when done right, outsourcing large portions of on-premise hardware and optimizing/streamlining for cloud can come with some significant resource efficiency gains. The key here is driving cost transparency and accountability to the business through proper governance, expense management, and cost reduction. Ultimately, key stakeholders will need to consider what the application and migration strategy will be as well as how it factors into the cost equation.

KEY CONSIDERATION #6: AGILITY TO INNOVATE FASTER

Improved flexibility to update cloud-based systems more quickly is perhaps the biggest benefit from moving on-premise workloads to the public cloud. Optimizing deployment enables financial institutions to respond to market changes and competition more quickly and introduce new products and services more rapidly.

Cloud environments are architected differently than older on-premise hardware and software, and transform the way software is built, maintained, and enhanced. For example, cloud-native development includes these main tenets:

- Development operations (DevOps) enable software development and IT operations to collaborate and automate software delivery and infrastructure changes.
- Containers dynamically divide a server (and application) into one or more separate containers for faster and more efficient processing.
- Microservices build applications as independent component services that run on their own; the applications communicate over HTTP APIs.
- Continuous delivery accelerates and lowers the cost of new software releases, enables rapid release cycles, and is more responsive to client and market needs.

Financial institution stakeholders should consider *how* they want to create public cloud solutions. They can deploy cloud native solutions or cloud-enabled solutions. Cloud-

native software is designed to be deployed in the cloud using a componentized, microservices-based architecture. System scalability is performed automatically, system maintenance and updates can be applied automatically without interrupting service, and system capacity is always available.

Financial institutions can also put existing legacy software applications in containers, which "enables" them for automated cloud operations. Cloud-enabled solutions were originally designed to be locally hosted. They may be limited to server capacity, must be customized to the installation environment, or require specific configuration to scale in the cloud. Although cloud-enabled solutions cannot leverage all the benefits that native cloud computing can, they are still more efficient than solutions deployed on premise.

Public cloud deployments can also increase the number of technology partners that a financial institution can integrate with its core banking, lending, and payments systems. This expanded access to new technology providers also reduces vendor lock-in to existing providers because partner replacement costs are lower. This flexibility and agility also extends to the cloud provider itself, since platforms are easier to port from one cloud provider to another. FIs may also want to host solutions on multiple public clouds so that they're not locked into one provider.

KEY CONSIDERATION #7: OPERATIONAL EFFICIENCY

Outsourcing technology hardware and software to the public cloud improves the overall operational efficiency of the solutions outsourced. It helps the IT division optimize its internal people resources, project priorities, and workloads. IT can take on new discretionary digital transformation projects, while investing time to reskill and train staff.

An IT division is often overloaded with a huge inventory of systems to maintain, enhance, and/or replace over time. Outsourcing technology applications to the public cloud also reduces technical debt, which is the implied cost of additional rework caused by choosing an easier (limited) solution or IT architecture now instead of using a better approach that would take longer.

However, banks need to consider DevOps in the context of cloud migration. Without a DevOps strategy which takes advantage of many of the tools and operational advantages in cloud, many of the benefits of enhanced scalability, time to market, and agility will not be realized.

Transitioning IT to the public cloud takes time, but it reduces costs and creates operational efficiencies that more than make up for the transition costs. With a smaller portfolio of IT to manage closely on a regular basis, IT department resources are freed up to address backlogs of line of business requests designed to increase revenue and client satisfaction. Other stakeholder interests are also better served as IT roadmaps become more dynamic and filled with more discretionary projects.

CONCLUSION

The path to cloud has many routes, with some banks slowly dipping in with specific non-critical applications, while others enact sweeping cloud migrations strategies across the entire application ecosystem. No matter the path, there are considerations that will affect the success of the journey. The business case is clear, and banks should use this report as a starting point to address questions that will ultimately maximize the success of migration efforts to the public cloud.

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

For more information please contact info@celent.com or:

Stephen Greer sgreer@celent.com
Craig Focardi cfocardi@celent.com

AMERICAS

USA

99 High Street, 32nd Floor
Boston, MA 02110-2320

Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 10036

Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, CA 94111

Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Brazil

Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B –
26° Andar
São Paulo SP 04711-904

Tel.: +55 11 3878 2000

EUROPE

France

1 Rue Euler
Paris
75008

Tel.: +33.1.45.02.30.00
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW

Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Italy

Galleria San Babila 4B
Milan 20122

Tel.: +39.02.305.771
Fax: +39.02.303.040.44

Switzerland

Tessinerplatz 5
Zurich 8027

Tel.: +41.44.5533.333

ASIA

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

Tel: +81.3.3500.3023
Fax: +81.3.3500.3059

Hong Kong

Unit 04, 9th Floor
Central Plaza
19 Harbour Road, Wanchai

Tel.: +852 2301 7500