Banking on Public Cloud

Reimagining Business Agility

Infosys® Finacle

Contents

Introduction 4

1. Cloud Design and Architecture to Support the Many Flavors of Cloud Computing 5

1.1 Cloud Infrastructure: 6

1.2 Security 6

1.3 Integration 7

1.4 Compliance 7

1.5 Cloud Ecosystem 8

2. Cloud Migration Strategy for Banks 8

3. Cloud Governance and Operating Model 10

4. Building a Business Case for Public Cloud 12

Conclusion 13

About Banking Visionaries Council (BVC) 14

Introduction

From an enabler of efficiencies to an enabler of business – the banking industry is looking at cloud in a clear new light. Two developments have been crucial in changing the industry's mindset towards cloud computing. The first is that the cloud service ecosystem of providers, brokers, system integrators etc. has improved both its understanding of banking requirements and its own ability to service the same. The second is that banking regulators, who once restrained the industry's march towards the cloud, are now encouraging them in that direction.

Banks are increasingly migrating non-core and core applications to the cloud, and having gained confidence through private cloud deployments, are now moving towards the public cloud. Some leading and progressive banks are clearly ahead in this journey, while some are still trying to find their path. Different banks are proceeding in different directions, and over the next few years, most will juggle on-premise applications with private, hybrid and public cloud deployments.

This paper, put together by the Banking Visionaries' Council (BVC) instituted by Infosys Finacle, is a practitioner's guide for a successful cloud strategy covering design and architectural considerations, migration of banking activities to the public cloud, cloud governance, and more. To see the view from the other side, we also invited major cloud services provider, AWS, to share their perspective of cloud adoption in financial services. They observe that media and entertainment companies or Internet firms – businesses that are lightly regulated compared to banks – are leading cloud adoption. In financial services, it is digital native and platform-based companies that are taking to the cloud. Incumbents are more circumspect, still concerned about the cloud's reliability and security; AWS says these concerns are misplaced and cites the example of statutory / highly regulated bodies such as FINRA and NASDAQ that are leveraging the cloud, as evidence of the cloud's suitability.

1. Cloud Design and Architecture to support the many flavors of cloud computing

Different banks are at different stages of their cloud journey. The industry's cloud landscape has two principal elements, namely, IT infrastructure and banking applications, both evolving at their own pace.

In theory, a bank's infrastructure – hardware and IT systems – can reside entirely in-house or at the other extreme, entirely on a public cloud. In practice however, it lies somewhere in between, with some applications hosted within the bank's premises, some hosted on a private cloud, and others on hybrid and public clouds.

A typical journey towards public cloud starts from a bank with a purely on-premise model, a bank that manages its entire infrastructure and IT applications deployed on that infrastructure, in-house. As it progresses to a private cloud model, it allows third party vendors to host and maintain (some of) its IT infrastructure, and pays a fee for the services. The bank continues to own its IT applications.

As the bank progresses towards the stage of public cloud adoption, it transitions through a state of hybrid cloud deployment, where it uses a combination of on-premise, private and public cloud facilities.

In its final stage of cloud journey, the bank uses the public cloud and SaaS (software as a service) for its IT needs – for example, it gets its infrastructure from AWS and email from applications such as Outlook 365 or tools such as JIRA, Quip etc.

Like infrastructure, banking applications are also in different stages of evolution. On one end of the spectrum, there are traditional applications, such as mainframes, built on monolithic architecture and proprietary technology, and tightly coupled to their databases and operating systems. At the other end, there are modern, cloud-native applications, which are built on open-source technology and are highly agile, flexible and DevOps ready. They are typically based on micro services architecture and deployed in containers. Once again, most banking applications lie somewhere in between these two end points.

Accordingly, a bank must design its cloud architecture to be flexible enough to support both its infrastructure and banking applications at different stages of evolution.

A recent research study from RightScale "State of the Cloud 2018" throws up an interesting finding that enterprises are moving from hybrid clouds to multi-clouds – multiple public clouds – for serving their infrastructure needs. We interpret this as a sign of maturity in enterprises, which are going beyond experimentation to adopt cloud technology in their production environments.

Coming to banking, we have seen a similar trend of multi-cloud usage in the past 2 to 3 years in the industry as banks try to avoid vendor lock-in and reap the benefits of competition among cloud providers. This means that banks must not only plan their cloud architecture to support the evolution of IT infrastructure and banking applications, but should also ensure that the architecture is able to deal with a landscape of multiple public clouds.

Cloud architecture has 5 building blocks, namely, infrastructure, security, integration, compliance and ecosystem.

Investment in public cloud infrastructure is growing rapidly across geographies. Google, Microsoft and Oracle have joined Amazon in the race to rapidly increase the footprint of public cloud infrastructure. These public cloud providers are making their infrastructure and services compliant with local laws. This means that banks can straight away build or port applications to the cloud, without worrying about compliance.

Security is an important consideration in a bank especially in a cloud scenario. The good news is that a number of security standards and tools have emerged to help them undertake the cloud journey safely and confidently.

Another key consideration is integration. Banks need to integrate applications deployed in different environments – in-house, on multiple public clouds etc. – so that they can work together as required by the business.

Like security, compliance is a huge priority for the banking industry. Until some time ago, cloud regulation and compliance was a grey area. This hampered cloud adoption among banks. Of late, a number of guidelines have emerged in countries around the world to guide and support banks in their journey towards public cloud adoption.

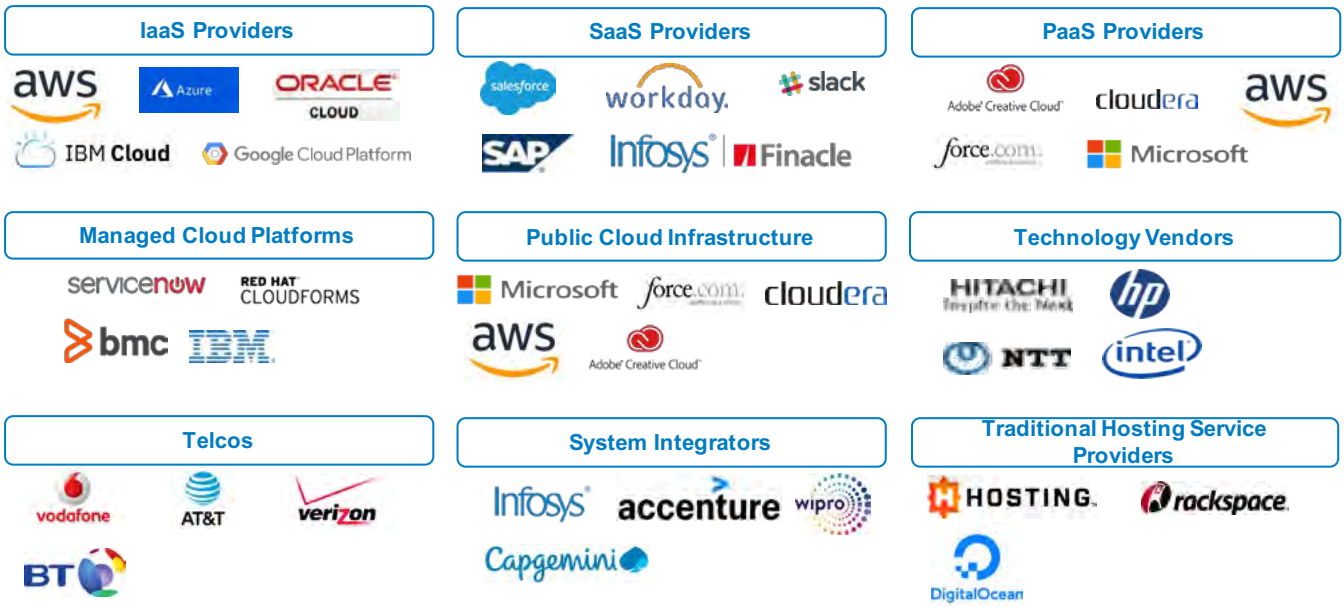
Another development paving the path to adoption is the rise

of a rich cloud ecosystem of ready-to-use third party platforms and applications that banks can tap and scale on demand. This means they do not have to start their cloud journey from scratch, or embark on it alone. A corollary is that banks also share responsibility for their public cloud assets with the ecosystem/ partners.

Fig. 2, for securing workloads on public cloud. It lists seven design considerations for securing applications and workloads on public cloud.

Among the important design considerations is identity and access management based on technologies such as Federation and OAuth 2.0, to enable both bank employees and customers

Fig. 1: **Cloud Ecosystem –Representative Offerings**



Let us examine each of the cloud architecture building blocks in some more detail.

1.1 Cloud Infrastructure:

There is a need to clearly define end to end responsibilities for public cloud deployments between cloud providers and consumers. Based on multiple iterations, a governance mechanism for 'shared responsibility' has been adopted by public cloud providers. Responsibility for managing the cloud itself – basically, physical security and the data center – vests with the cloud provider; and the responsibility for managing what happens in the cloud lies with the banks, who must implement the controls associated with the workloads that are up on the cloud.

1.2 Security

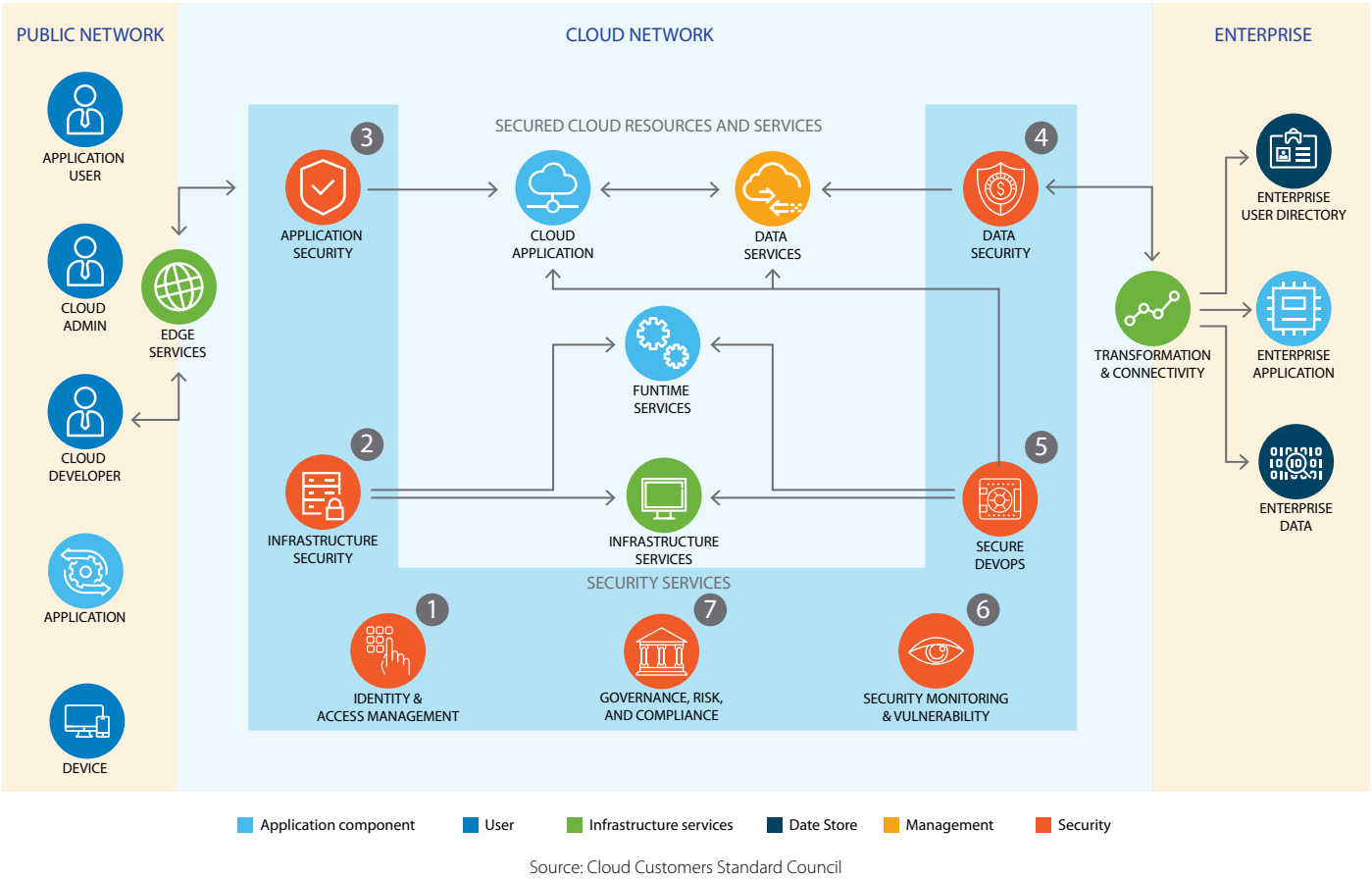
Public cloud vendors are making huge investments to develop in-built security in their cloud platforms. Nowadays, public clouds are becoming recognized for being secure. An end user advocacy group body called Cloud Customer Standards Council[3] has come up with a reference architecture, depicted

to use applications seamlessly regardless of their location. The goal is to ensure users don't have to worry about where the application is deployed – on-premise or public cloud. This melts away all erstwhile concerns such as what needs to be done by way of password management or user training when an application is relocated. From the bank's perspective, it allows free movement of applications from the enterprise premises to the cloud, without any disruption.

Data classification is another important aspect. Regulations such as GDPR stipulate organizations to have strict control over their data's location and who can access it, and adhere to strict guidelines on data encryption, classification, storage and deletion.

The secure DevOps process prevalent as a part of public cloud infrastructure, offers a mechanism to continuously scan both hardware and software for vulnerabilities and send out alerts, making it very hard for hackers to attack. Automated security testing can also be enabled as part of DevOps to ensure every version is tested for security use cases before release.

Fig. 2: **Reference Architecture for Applications**



Source: Cloud Customers Standard Council

AWS suggests that companies porting workloads to the cloud should follow certain security design principles to make sure their assets are well protected.

It is crucial to establish a secure identity foundation that provides a clear identity for every user, be it a developer, IT support staff, or an end user. There should be full traceability and automated auditing of cloud operations. The organization should apply security at all layers: besides securing its applications (which is outside the ambit of the cloud), it should leverage the considerable security capabilities of the cloud itself. Also, from the organization's point of view, automating security best practices is great preparation for facing untoward events.

Enterprises may also find the concept of a "golden image" useful. All the security configurations and codes can be embedded within a so called "golden image" that serves as a template for any future work on the enterprises' applications. Most cloud service providers (CSPs) offer tools for this purpose. Last but not least, enterprises should incorporate features such as logging and auditing into different processes. Following these principles will enable enterprises to standardize security across the organization.

1.3 Integration

Integration is another key facet of cloud architecture, which must find a way to bring together all the bank's data scattered across on-premise and cloud infrastructure, as well as integrate banking processes from end to end while making sure they meet SLAs.

A Hybrid Cloud Integration architecture is necessary to provide a seamless platform for applications regardless of application platform and deployment models.

Hybrid and Multi-Cloud deployments also need robust governance mechanisms to monitor and measure SLAs, uptime and business continuity, to mitigate disruption to business operations across the platform.

1.4 Compliance

A decade ago, there were no separate compliance guidelines for cloud computing; enterprises simply took outsourcing guidelines and adapted it for the cloud. Banks, being highly regulated, were understandably wary of leveraging public cloud in the absence of clear guidelines. Today, standards are emerging to help enterprises self-manage and self-audit their

applications and data running in the cloud. A gist of standards for public cloud is provided below:

Standards	Guidelines for
ISO/IEC 27017	Security for public cloud services
ISO/IEC 27018	Personal data protection for public cloud services
ISO/IEC 19086	Security and privacy components of cloud service level agreements
ISO/IEC 27036-4	Information security risks associated with the use of cloud services and managing those risks
FIPS 140-2, SAML 2.0	Technology standards on Encryption, Tokens
Cloud Security Alliance	Best practices for providing security assurance on Cloud

1.5 Cloud Ecosystem

Today, a diverse cloud ecosystem makes it much easier for banks to undertake their cloud journey. The ecosystem features partners in the form of managed cloud platforms, platforms as a service, technology providers, public cloud infrastructure, and application providers that banks can work with to get a jumpstart on building their cloud landscape.

Fig. 3: **Cloud Providers on the Market**

2. Cloud Migration Strategy for Banks

No two banks are alike, so it stands to reason that the cloud migration strategy of each bank will depend on its unique circumstances – for instance its existing systems landscape, resources, and desired objectives of migration.

While some of these, such as the current landscape and resource base, are a given, the bank may need to determine other aspects before plotting its migration strategy, the foremost being goals and priorities. These could be any of the following:

- **Rapid time to market** – enabling banks to respond quickly to changing market demands with new products, services and experiences.
- **Scalability or delivery of new capability cost effectively** – allowing banks on a high growth trajectory to fulfill their large IT needs on demand, thereby eliminating the need for large capital investments.
- **Avoidance of operating expenses, and preservation of capital** – this goal is related to the above and is especially relevant to small institutions or those with limited budgets.
- **Operational efficiencies** – banks can derive significant operational efficiencies by automating the development life cycle, provisioning etc. on the cloud.
- **Freeing up data center space** – large banks with expensive data centers can significantly cut those costs by migrating to the cloud. A good example is Capital One[2], which is scaling its 8 data centers down to 3, by moving workloads to AWS.
- **Leveraging existing investments** – many projects are stalled or abandoned midway for lack of financial resources.

Banks can leverage such investments and save them from going to waste by porting their activities to the cloud, and switching to an affordable subscription model.

AWS observes that the greatest need in banking is to port both systems of engagement and systems of record to the cloud. Most banks are turning to cloud computing to shorten time to market as well as adopt data technologies including analytics, machine learning and artificial intelligence to improve customer insight.

Providing access to all consumers and devices; integrating with other web and cloud applications – by migrating to the cloud, banks gain native cloud advantages such as access to a host of other applications and to API gateways connecting them to a wide ecosystem of partners and customers.

After identifying the pressing priorities and dependencies driving their cloud migration strategy, banks need to validate the architectural context to determine their readiness for migration. At this point the banks need to have a roadmap, as well as clarity on decisions such as moving to open source technologies and assembling the right talent to build tools that they can leverage on the cloud.

Banks must also validate their current landscape with a blueprint that shows the current state of applications, and the treatment required by each. For instance, they would need to identify what applications to rewrite, what to replace, and what to directly source from the cloud as a service (SaaS). Size plays a role in these decisions: large banks typically have their own manpower for IT development and would likely wish to control and manage their cloud; these banks will simply buy up some space. Other banks may choose to take applications and services, and entrust the Cloud Service Provider to take care of everything else.

Broadly, banks must introspect the following aspects of their architectural context:

- **Cloud adoption strategy** – the organization's goals and approach towards cloud computing.
- **Application portfolio management** – the cost and worth of different applications.
- **Legacy modernization** – replacing strategic applications versus the risk of leaving them as they are.
- **Application platform strategy** – the target application platform.
- **Build, buy, borrow or rent** – the delivery strategy for overhauling the application.

Generally, a bank would need to use some or all of the following strategies when moving applications to the cloud[4]:

- **Rehost** – this strategy applies to applications, which, although not natively built for the cloud, can be deployed (or rehosted) there with minor changes.
- **Replatform** – on-premise applications that need to be certified on a different database or platform before they can work on the cloud must be replatformed. The application

per se is not changed, but its underlying stack, server or third party component is adapted for the cloud.

- **Repurchase** – when a bank does not have a certain type of application that it needs, or has one that is obsolete, it would have to purchase/ repurchase the same. For example, if a bank does not have an API mechanism or gateway in its on-premise set up, it can simply subscribe to it as a service, since such things are now embedded in most clouds. Had the bank not decided to migrate to the cloud, it would have had to purchase the gateway from a third party source and installed it in-house. When it comes to an obsolete application, say an old version of Outlook, the bank can simply replace it by taking an alternative mail management system such as Microsoft 365 directly from the cloud.

- **Refactor** – a critical application that is not ready for cloud deployment, yet must be migrated to the cloud, would have to be refactored, that is, redesigned completely to make it suitable. It would have to undergo application code development, followed by a software development life cycle and integration.

With many vendors now offering native cloud applications, and the option to develop applications on the cloud itself, there will be less need for migrating applications in the future. Instead, banks will use platforms that are by default in the cloud ecosystem and come with built-in advantages such as scalability, database independence and portability (between clouds).

- **Retain** – the bank may decide to retain an application on-premise when migration is not practical, owing to reasons of size, complexity, sluggishness, or memory requirements etc.

- **Retire** – applications that are outdated or unnecessary may simply be retired.

After deciding its migration goals and strategies, architectural position and application migration approaches, a bank would need to select the partners for its journey to the cloud. This decision depends a lot on how the bank plans to migrate its applications: if it mainly plans to rehost, then it can work with providers such as Rackspace or Joyent to manage the infrastructure. But when the need is to refactor applications, then the choice could be a vendor such as Longjump or Force.com. For those primarily going the SaaS way of replacement, providers such as Salesforce CRM, Netsuite or Workday would make up the consideration set.

Capital One

Capital One is one of the largest banks in the United States and offers credit cards, checking and savings accounts, auto loans, rewards, and online banking services for consumers and businesses. The bank followed a four-stage adoption process to transform towards public cloud.

In the project stage, Capital One involved a small group of motivated and experienced individuals. The idea was to test security tools and different processes for a small technology footprint of the bank. The ban worked with AWS team early on. Based on this, the team came up with recommendations for the public cloud journey.

In the foundation stage, the bank added the development and test environment on AWS. This was a period of investment as the bank used services like Direct Connect to extend their virtual network into AWS datacenters. The bank wanted to make the environment between on-premise and AWS seamless and hence access management tools were integrated. As there would be higher demand for resources experienced with the cloud technology, the bank also formed the Cloud Center of Excellence.

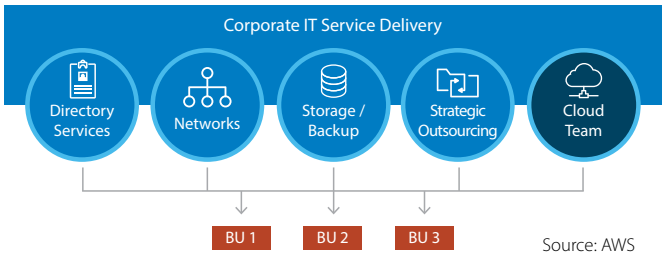
In the migration stage, the bank set itself a target that was announced publicly. The team wanted to reduce the number of datacenters from eight in 2014 to three in 2018. Nurturing the expertise with the bank's center of excellence was important for achieving this target. The bank worked closely with the AWS team to for their application migration, by re-hosting when the changes required was minimum, and re-platforming / re-architecting when they were significant.

Finally, as most of the bank's applications are on cloud, the team is now looking to optimize costs wherever possible and improving speed by automating recurring deployment activities.

3. Cloud Governance and Operating Model

Many organizations today are grappling with the actual transformation from a non-cloud to a cloud mature state. This is a big journey that is accomplished over time. Highly complex organizations such as financial institutions must weigh their options carefully before proceeding to adopt the cloud across the enterprise. Today, there are many tried and tested models of transformation that enable organizations to consume cloud computing effectively.

Fig. 4: **Cloud Adoption Approach**



Source: AWS

One of them is the following approach suggested by AWS:

Start by assessing the current state of inputs, such as ITS organization structure and ITS operating model. Next, devise a new operating model for functioning in the cloud. The AWS Cloud Adoption Framework, for example, assesses the enterprise's various perspectives – business, platform, process, people, maturity, operations and security – to arrive at a suitable cloud operating model that is in harmony with them all.

This is followed by recommendations and next steps leading to a Concept Cloud Operating Model that includes the capabilities in hand, functions to be performed, tools and technologies to build or buy, governance measures, and path to operationalization.

In general, a cloud operating model for an organization has four important tenets – it is customer focused and agile, automates as much as possible, thinks of infrastructure as code and employs lean teams for better communication.

In this model, corporate IT service delivery is responsible for services such as directory services, networking, storage and outsourcing; the cloud team exists as another entity within the overall IT service delivery team, and is responsible for the following:

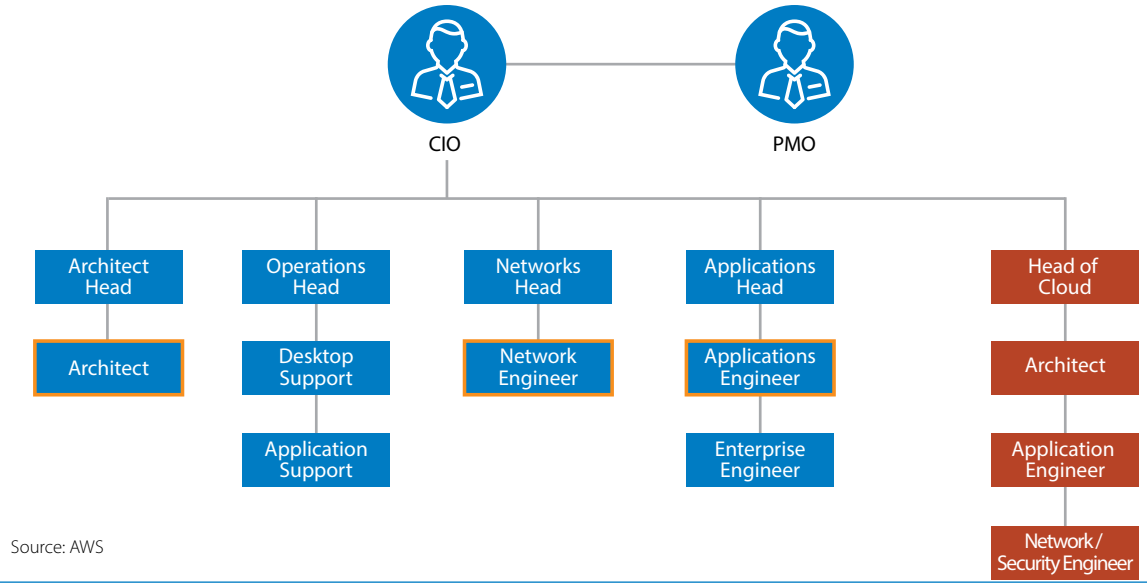
- **Cloud security** – making sure everything that happens on the cloud is secure is the team's foremost responsibility.
- **Cloud performance** – the team must maximize application performance while optimizing cost.
- **Cloud resiliency** – the cloud team must offer design patterns and templates which are continuously available.
- **Cloud consumability** – ensuring applications, platforms and infrastructure on the cloud are easily consumed by users is the key to agility.

Last but not least, the cloud team should evangelize the cloud within the organization.

A possible organizational structure for the cloud team and its reporting relationship to the CIO is depicted below:

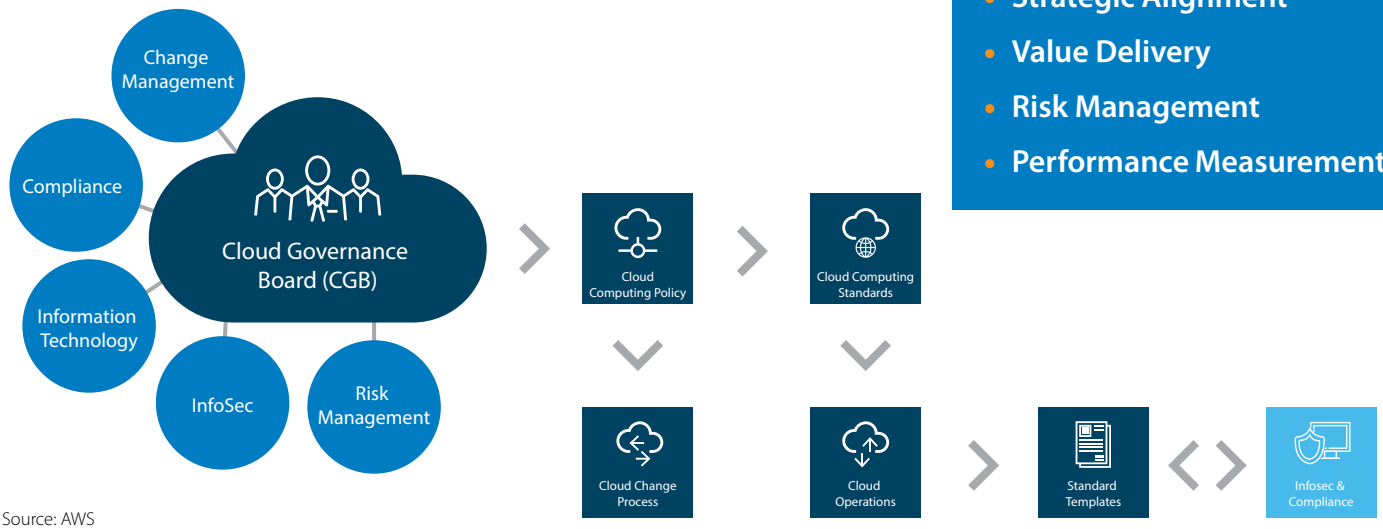
One of the biggest success factors in cloud adoption is governance. Even when a cloud model is running smoothly, the organization needs to be vigilant that nothing is slipping through the cracks. There are a number of cloud assessment

Fig. 5: **Sample Organization Structure**



Source: AWS

Fig. 6: **Cloud Governance Model**



Source: AWS

and auditing frameworks, such as the AWS Managed Service Provider Program, which help enterprises evaluate and monitor their cloud governance practices and technical capabilities. Using these frameworks, financial service organizations can identify and cultivate best practices for cloud adoption.

At the heart of this model is a cloud governance board whose charter is to lay the foundation for a balanced approach to compliance, control and acceptance of cloud computing. The board is made responsible for defining a cloud computing policy concerning all important issues, such as information security, risk management, change management and compliance. The policy should guide the establishment of standards that the cloud operations team can apply throughout the enterprise with the help of templates and tools. The board's functioning should result in clear outputs such as strategic alignment of the organization, value delivery, management of risk by adopting standards, and clear performance measurement.

4. Building a Business Case for Public Cloud

"What does the end-state look like and is it worth it?"

This is the crux of what any board or management seeks to know from a business case for a proposed investment. And the answer more often than not lies in two key metrics - the estimated return on investment (ROI) and the return on assets (ROA). A business case for migration to cloud often takes into account the reduction in total cost of ownership (TCO) of infrastructure and the decrease in operating cost to arrive at these figures to justify the investment in cloud. The benefits of speed and agility, although indisputable are often an afterthought.

Several surveys, studies and researches have continually sought to find the key reasons why IT managers and executives move to the cloud. While cost saving clearly emerged as the key driver in the beginning of the last decade, IT managers didn't take too long to appreciate the agility, the flexibility and the ability to innovate in the cloud as some of the primary reasons for cloud adoption. With digitization, cloud thinking has become more strategic. In a recent Gartner survey nearly 22% banking executives globally, cited IT modernization as the key driver for migrating to cloud. 15.5% stated agility as the primary reason, 15% innovation, 22% cost efficiency, 7% application development and 9% standardization.

IT executives and managers looking to migrate to the cloud need more than the benefits of scalability and agility to put quantifiable business benefits on paper for business buy-in. Here we look at some definite cost considerations and gains for a business case for moving to the cloud:

Capital expense reduction for infrastructure

One of the direct benefits of cloud infrastructure is reduced server, storage and network infrastructure cost. Enterprises can greatly reduce the infrastructure cost of say a data center facility, and move to subscription-based pricing with IaaS. On-demand payment as opposed to reserved infrastructure cost directly translates into reduction in capex.

Operating expense reduction

Although a part of the capital expenditure gets converted into operating expense with subscription cost replacing the cost of the facility and data center, this is offset by the reduction in cost elements such as number of FTEs and other maintenance cost heads.

Banks can save several kilowatts of power by moving data centers to cloud. In addition to power and cooling cost, there is a linear reduction in operating cost as the number of FTEs required to provision, patch, update, diagnose and troubleshoot the infrastructure drastically comes down.

Data center consolidation

Enterprises with multiple data centers often embark on a data center consolidation exercise to rationalize costs. They stand to benefit directly with gains from lower cost of facilities. However, banks must factor in the transition costs associated with implementing the capability in a new SaaS environment or cloud environment. Banks must also figure out a plan for the infrastructure assets retired as a result of consolidation.

SaaS gains and costs

One of the key reasons enterprises move to the cloud is because it makes the infrastructure available on demand. Cloud can help circumvent the whole rigmarole and long cycles associated with procurement and installation before an asset can be used. There is minimal to no lead time with the Instant provisioning of resources in the cloud. Not only this, faster processes result in faster implementation, upgrade, integration, and customization, directly reducing the associated costs.

Application development and delivery improvement

The benefits of on-demand infrastructure, faster provisioning and installation - essentially making a resource ready for use much faster than in a traditional cycle - cascades down to developer productivity. Cloud not only makes it easier to buy new tools for software application development, but also improves how these capabilities are used to develop software faster, thus increasing developer productivity. With shorter release cycles and a constant feedback loop, functionalities can be modified and fixes made before going into testing and quality. This translates into a direct benefit for business with a significantly reduced time to market.

Business agility

With a faster time to market, banks can compete more effectively resulting in direct potential market gains of increased customer acquisition, and potential business benefit of a healthier top line.

Innovation ecosystem

Digitization has heralded a shift towards the platform business model in banking, which hinges on the ability of banks to cultivate, curate or be a part of diverse ecosystems. Forward thinking regulations such as open banking, PSD2 and others have further compelled banks to move towards open APIs. Cloud is the underlying enabler for communication and information exchange through APIs, allowing banks to innovate with partners, FinTechs and extended developer ecosystems. By ensuring compatibility and handshake between the bank and FinTech clouds, banks can benefit from ease-of-integration with the expanded ecosystem and take joint innovations to market faster.

Peak capacity management

Discounts in their digital avatar have become particularly popular. Boxing Day online sales surpassed £1 Billion for the first time in December 2017. Sales skyrocketed equally during Black Friday. Flipkart's billion-dollar-sale in India is a much sought after event that has buyers flocking to the ecommerce giant's website. These transactions reach banks for the same set of authentications, and the infrastructure at banks is not designed for such high volumes. With techniques such as cloud bursting, banks can handle these unusual peaks by moving load beyond a certain threshold to the public cloud. They need not invest in infrastructure for such high volumes since this is not typically the required peak capacity, but only a one off requirement.

Risk management and compliance

According to Gartner's CIO survey result, only 14% banks had public cloud deployments in 2014. But with public cloud vendors setting up localized data centers the trend is slowly changing. Leading and progressive banks such as Capital One, DBS[1] and more, have given a thumbs-up to public cloud by progressively moving their workloads and reducing their data center footprint. Concerns around security have always been a key impediment to public cloud adoption. But now banks are beginning to trust the public cloud, given the enhanced encryption practices and security controls of vendors such as AWS that are far superior to banks' own infrastructure and data

center security. What's more, AWS also provides the necessary tools to assess and meet regulatory compliance. The vendor is also working with regulators in various countries to advance the case for public cloud adoption.

A common myth is that the public cloud is invariably cheaper than traditional IT. But the perceived cost benefits may be difficult to achieve if factors such as appropriate sizing and hidden costs of investment in quality assurance are overlooked. For a business case to actually deliver on the cost gains it promises, it must assess the following parameters:

Workload pattern

The more variable the demand, the better the cloud is for business. An enterprise or bank may choose to own the infrastructure if the demand is consistent. But if there are frequent highs and lows, it's prudent to invest for average peak load, and manage unusual capacity with cloud bursting.

Data workloads

Cloud design architecture must ensure proximity of data servers and compute resources to avoid latency and delay that can hamper not only operations and maintenance or developer productivity, but also the end-user experience.

Uniqueness vs. commonality

Security in the public cloud is a shared responsibility. Thus retaining the unique functionalities, products or processes in the private cloud may bode well for banks.

Compliance

As stated earlier, different countries may have different regulations for data residency and data sensitivity. For e.g. data such as customer confidential information might be prohibited from leaving a country. To contain regulatory costs, the cloud architecture must be built around these considerations.

Conclusion

The move towards open banking in many parts of the world is accelerating adoption since the cloud offers a good foundation for open banking, and also for the creation of purely digital businesses.

That being said, even in the case of traditional banks (that are not digital natives), cloud computing is fast becoming the new normal for running core systems as these institutions increasingly migrate their core platforms to the cloud to improve customer experience and service, launch new market-facing applications, and automate and operationalize manual back-office processes.

References:

1. DBS Press Release 'DBS collaborates with cloud leader Amazon Web Services to deepen cloud engineering talent pool': https://www.dbs.com/newsroom/DBS_collaborates_with_cloud_leader_Amazon_Web_Services_to_deepen_cloud_engineering_talent_pool

2. Capital One's Cloud Journey
https://medium.com/aws-enterprise-collection/capital-ones-cloud-journey-through-the-stages-of-adoption-bb0895d7772c

3. Cloud Standards Customer Council
http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-Hybrid-Integration.pdf

4. AWS Enterprise Collection – 6 strategies for migrating applications to the cloud
https://medium.com/aws-enterprise-collection/6-strategies-for-migrating-applications-to-the-cloud-eb4e85c412b4

About Banking Visionaries Council (BVC)

Banking Visionaries Council has been instituted by Infosys Finacle to collaborate with senior business and technology leaders from the banking community to develop actionable points-of-view around contemporary themes within the industry. The purpose of this council is to solve the most pertinent problems with research and collective thought leadership efforts. Currently, the council consists of a twenty-member-strong board with representation from eleven countries across six continents.

This point of view paper is an abridged version of the collaborative research work done by the council and the contributing partner Amazon Web Services (AWS). For more information on the council, please reach out to finacle@edgeverve.com.

- Share key market development and trends observed in respective geos with rest of the group
- Collaborate to develop actionable point-of-view on how banks can leverage emerging trends
- Openly discuss learning from innovation initiatives taken by respective banks

Contributing Partner:

aws

About Infosys Finacle

Finacle is the industry-leading digital banking solution suite from EdgeVerve Systems, a wholly owned product subsidiary of Infosys. Finacle helps traditional and emerging financial institutions drive truly digital transformation to achieve frictionless customer experiences, larger ecosystem play, insights–driven interactions and ubiquitous automation. Today, banks in over 100 countries rely on Finacle to service more than a billion consumers and 1.3 billion accounts.

Finacle solutions address the core banking, omnichannel banking, payments, treasury, origination, liquidity management, Islamic banking, wealth management, analytics, artificial intelligence, and blockchain requirements of financial institutions to drive business excellence. An assessment of the top 1250 banks in the world reveals that institutions powered by the Finacle Core Banking Solution, on average, enjoy 7.2% points lower costs-to-income ratio than others.

For more information, contact finacle@edgeverve.com

www.finacle.com