5 METRICS FOR FINANCIAL SERVICE SUCCESS IN THE CLOUD

JANUARY 2019

TABLE OF CONTENTS

Opportunities Realized

by Creating a Compliant,

Performant and Cost

Efficient Cloud Ecosystem

INTRODUCTION

Traditionally Financial Service Organizations (FSOs) have been digital pioneers driving technology further faster. From the ATM to mobile banking, banks have led the charge to a more connected, technology driven world. Ironically it is this early adoption of IT that has resulted in a modern reliance on outdated mainframes and inherited legacy technology that has acted as a speed bump, slowing financial firms adoption of cloud.

Due to the sanctity and value of financial services customer's data and the amount of cyber criminals eager to get the data, a measured approach has been prudent. After all, cloud technology is relatively new. AWS launched in March of 2006. Google cloud launched in April of 2008. Microsoft's Azure launched in February of 2010. In regards to "the Cloud" financial regulators and policy makers did not have a framework for analysis. Infrastructure has to be purchased and maintained based on usage spikes. Until recently inhouse, collocated, capital intensive "private clouds" reamined status quo.

Perhaps it is the use of "cloud" as a metaphor that is partly responsible for a lack of confidence with storing mission critical data in the "cloud." A 2012 survey of 1,000 random people noted that 51% believed that weather impacted cloud computing, and 29% believed that cloud computing was actually in the clouds.[1] With banks, whose survival and growth depend on the reality and perceptions of the level of security they practice, the marketing department would be correct in advocating louder than anyone for an inhouse approach to data storage and production workloads.

With the proven, secure, performant and cost effective cloud of today, old perceptions are permanently in the past. 74% of companies are already running workloads on the public cloud or utilizing hybrid architecture.[2] The financial services sector is one of the fastest growing verticals in the public cloud ecosystem and producing truly remarkable innova-

tion leaps as a result.[3] Cloud can be delivered with 99.999% uptime Service Level Agreement guarantees and provide highly available, geographically diverse, elastic architecture which can transform the IT department from a sunk cost to a springboard for innovation, disrupting the market and giving customers what they demand before they know they needed it.

While the risks of the cloud may have been too high for the finserve CTO and CIO five years ago, the benefits of NOT moving to the cloud today are too risky to ignore.

While the risks of the cloud may have been too high for the finserve CTO and CIO five years ago, the benefits of not moving to the cloud today are too risky to ignore. In the ever evolving world of mobile and online services customer needs and expectations are driving innovation towards a more connected, responsive and intuitive future thanks to the cloud.

This whitepaper will explore the opportunities that financial service companies can realize by migrating to the cloud. We will bring into clearer focus these benefits, through the lens of security, architecture, performance, software development and cost savings.

1 Citrix Survey 2012
2 https://grist.org/business-technology/126628/
3 Forbes, 2017 State of Cloud Adoption

CLOUD SECURITY AND COMPLIANCE

In the public cloud of 2019, the regulators have caught up with cloud technology, and cloud providers have kept pace with the changing regulatory landscape. Whether your organization needs compliance such as PCI, SOC 1, SOC 2, FISMA, or FFIEC the cloud is now the fastest path to compliance. With documentation, change control, encryption and geographic diversity the cloud offers exciting elasticity and scalability that give peace of mind to FSOs, customers and regulators simultaneously.

Change Management

Traditionally, the most trusted method of ensuring security and availability of customer data was to implement tightly controlled and documented change control processes. This ensured that nothing could slip into production without severe scrutiny. Within a traditional IT environment, this processes could often slow innovation to a halt. Even the smallest change could take weeks and often months to get approval. Unaddressed this practice can act as a speedbump and eliminate any advantage to moving to cloud infrastructure.

In order to eliminate this bottleneck to innovation in the cloud, change control must be transformed without compromising regulatory compliance. In order to accomplish this, change control must be re-imagined with cloud infrastructure in mind. One of the main benefits of change control is to ensure changes are known, documented, and auditable.

With cloud infrastructure, all configurations, from the physical network up through the servers, operating systems, and application deployments can be automated with configuration management code. By building infrastructure deployment pipelines and limiting

cloud access to those pipelines, configuration management can be more accurate than the most strict change control processes, without sacrificing agility.

Holistic security testing must be central to deployment pipelines. The job of the pipeline is to ensure confidence in the software release or infrastructure change. Confidence in your security is not negotiable. The cloud has robust tools to facilitate and automate testing outside of production, and with on demand infrastructure resources.

Data Sovereignty

Compliance with certain countries may dictate that data cannot leave the boarders. Azure, Google Cloud, and AWS have tools to establish residency of your data, meaning the encrypted data never leaves the borders of that specific country or group of countries.

While 100% of the infrastructure and the physical security layer are within the responsibility of the cloud provider, 100% of the responsibility of compliance of the system as a whole remain the responsibility of the financial institution. Regulators expect financial services institutions to build safeguards and protections in the architecture. Just as with on premise data centers, data in the cloud must be protected with firewalls and encryption to keep data from hackers grasp.

PCI COMPLIANCE CHECKLIST

	RESPONSIBILITY	
	FSO	CLOUD PROVIDER
Safeguard cardholder data by implementing and maintaining a firewall.	✓	
Create custom passwords and unique security measures rather than default setting from vendor-supplied systems.	✓	
Safeguard stored cardholder data.	✓	
Encrypt cardholder data that is transmitted across open, public networks.	✓	
Anti-virus software implemented and actively updated.	✓	
Create and sustain secure systems and applications.	✓	
Keep cardholder access limited by need-to-know.	✓	
Users with digital access to cardholder data need unique identifiers.	✓	
Network resources and cardholder data access needs to be logged and reported.	✓	
Physical access to cardholder data needs to be restricted.		✓
Run frequent security systems and processes tests.	✓	✓
Address information security throughout your business by creating a policy.	✓	✓

CLOUD ARCHITECTURE

Many Financial Services Organizations often begin their cloud journey with marketing, HR, and payroll SaaS (Software as a Service) running in the cloud. With inevitable and growing comfort with these cloud based offerings many FSOs embark upon a hybrid cloud/ data center design. Today with all the risk out of cloud technologies and their own experience validating cloud FSO is increasingly moving all in with the cloud.

Single Cloud vs. Multi-cloud
Like organizations in other highly regulated industries, Financial Service Organizations can benefit from investing in multi-cloud capabilities. Many organizations strategically decide to go all in with a single cloud provider, citing the benefits of leveraging cloud native services, and developing to a single API vs. the benefits of workload portability, which allows vendor independence but at the cost of being limited to leveraging "lowest common denominator" services. Although there can be benefits to a single cloud strategy, this logic assumes that the main benefit to a multi-cloud capability is workload portability from one cloud to another.

The reality is that each cloud provider is developing cloud native services to differentiate itself from the other vendors. Each is building their proprietary services based on their strengths. For example, Amazon's NoSQL and Mass Storage expertise has been integral in their development of S3 and DynamoDB. Google's expertise in big data analytics has led to BigQuery. Microsoft's deep expertise with their own product stack has led to deep integration of cloud services with Active Directory. The real benefit of a multi-cloud strategy is not the ability to move a single

workload to any cloud; the real benefit is the ability to select the cloud that is most suitable to each workload. In order to launch and manage workloads in several clouds, organizations need to build the capabilities to do so. This includes network integration, ensuring connectivity to the datacenter and corporate network, authentication and authorization, workload monitoring, and automated provisioning capabilities, among other foundational service capabilities.

Part of building these capabilities includes considering multi-cloud when selecting tools, and when training staff. Cloud agnostic tools can help organizations provision and manage workloads across multiple clouds, even if each workload is leveraging a proprietary cloud service, restricting that workload to a single cloud. Docker has developed a workload agnostic containerized system that seamlessly integrates multiple clouds and operating systems. Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications, that is growing in popularity.

Additionally, this capability increases leverage with cloud vendors. Even if each workload can run in only a single cloud, new workload architecture and cloud selection may be subject to new pricing requests. This is especially important for companies like Financial Services Organizations, or others in highly regulated industries, as one vendor may meet specific compliance requirements for their cloud native services sooner than other vendors. Having the capability to leverage that vendor can create a huge competitive advantage from a product or service differentiation perspective.

CLOUD PERFORMANCE

65% of cloud customers cited scalability as a key driver for moving to the cloud. [4] These IAAS (Infrastructure as a Service) customers appreciate the elasticity and flexibility that the cloud provides. Bankinter, a Spanish Bank and the European leader in online transactions turned to AWS for its risk analysis application. To determine the financial health of their clients, Bankinter's algorithm computes over 5,000,000 simulations. Using Amazon Elastic Compute Cloud (Amazon EC2) they decreased the average time-to-solution from 23 hours to 20 minutes resulting in substantial cost savings. [5]

Amazon.com's Prime Day and Cyber Monday produces record setting sales spikes year after year. AWS was built to handle these, and when they offered their infrastructure to other enterprises this selling point resonated soundly with financial firms who themselves have seasonal and even daily spikes in usage. This elasticity offers cost and performance benefits where limitless traffic can be processed without any throttling or loss of performance. And customers only pay for the capacity when they need it.

With geographically dispersed infrastructure the cloud of 2019 can use code instead of hardware to automate previously manual processes, decreasing cost, human errors while

having performance enhanced. With tablets, mobile phones, watches, laptops, desktops the end user can have peace of mind that all of their data can be accessed without further manipulation. These services are available and on demand 24x7.

In order to take full advantage of performance advantages of cloud infrastructure, workloads need to be architected with cloud infrastructure in mind. Prior to migrating workloads to the cloud, loosely coupled systems that can independently scale out, not up should be taken into consideration. Managing state becomes critical when servers become ephemeral, or when serverless architectures are employed.

Moving core banking functions to the cloud in a measured, secure and proven way eases the transition. By taking into account application and data dependencies, architectural alignment and the competitive advantages of the cloud FSOs can realize scale, security and high availability. A phased approach will take into account short and long term goals while always striving for business and cloud platform alignment. AWS, GCP and Azure all offer 99.99% availability Service Level Agreements (SLA).

4 Cloud Industry Forum, 2018, Cloud: Driving Business Transformation.
5 Tamebay, 2019, BigCommerce Google Cloud Platform migration sees faster load times.

SOFTWARE DEVELOPMENT

For Financial Service companies today, a growing cloud means a shrinking data center footprint. It means the silos between development and operations are being demolished and agile software development is producing game changing innovations with record time to market. By adopting and supporting a DevOps framework innovations can get to market in weeks instead of years and incumbent Financial Services Organizations can become digital and agile once again creating experiences that delight customers and attract new ones. Cloud computing makes new products and services easier to develop and launch, which is particularly important for a financial services industry that has traditionally been slow to respond to evolving customer requirements due to legacy infrastructure investments.

With over seventy million accounts, Capital One is the world's largest digital bank. By adopting a cloud first strategy they have shrunk their data center footprint from 8 to just 3 in just the past 5 years. They wanted to get out of the infrastructure business and focus on human centric developments that dazzle their customers, attract new customers and zoom them in front of the competition. With over 1,000 engineers on staff they create software instead of managing software and infrastructure.

> **"AWS enables us to operate more securely in the public cloud, than we could in our own data centers."**
>
> **Rob Alexander,**
> **Capital One CIO**

For Capital One and other financial service organizations being agile in the cloud allows for rapid development and integration of emerging technologies, such as big data, blockchain, AI, robotics and IOT. As the cloud continues to intuitively integrate our digital and physical lives the cloud and robust networks become the enabler for this symbiosis. With mobile usage already outpacing desktop usage 2 to 1, this revolution will continue in the streets, in the car, on our bikes and on the bus.

6 AWS re:Invent 2015 Keynote | Rob Alexander, CIO, Capital One

FINANCIAL BENEFITS

Utilizing economies of scale, AWS, Google, and Microsoft have built production and storage ecosystems that cannot be replicated by a single user. These are compute powerhouses with hundreds of thousands of engineers developing solutions to make the ecosystem work securely, efficiently and effectively. With the right architecture, design, cost controls and monitoring these ecosystems can deliver profound performance enhancements and cost savings.

Cloud infrastructure got its start as an easy to use tool for developers, and as a low cost of entry infrastructure option for startups. As companies saw the benefits cloud infrastructure offered, they pushed companies like Amazon to offer services for mission critical infrastructure. The market responded. FSOs can scale with cloud vendors knowing they have levels of certification, regulatory compliance, and operational excellence that no single company could afford to recreate.

By partnering with cloud vendors to use services like AWS, Google cloud Platform and Microsoft Azure, Financial Services institutions can gain the agility that comes with cloud infrastructure without compromising security, durability, or availability. With huge seasonal usage spikes, the financial services vertical is an ideal partner with the public cloud. This paradigm shift in modern IT, takes away the costly upfront CapEx (Capital Expenditure) and replaces it with a right sized, elastic OpEx (Operating Expenditure.)

With expensive hardware, power, cooling, security, annual license fees the cost of doing business in banking, insurance, mortgages and payment technologies was prohibitive just 10 years ago. With cloud technologies start-ups need not make an investment in infrastructure and can instead focus their solutions on software design and building applications that harness the enterprise level compute and storage the cloud securely offers. By only paying for what they use the nimble start-up is upending a previously monopolistic high street, and forcing the market to innovate or go the way of Kodak.

Getting out of the costly infrastructure business can make companies much more efficient and reactive to market conditions. Embracing cloud means embracing all of the attributes that come with cloud infrastructure. Financial Services firms can benefit greatly, but there is a level of commitment, and a level of effort involved in transforming applications, systems, and infrastructure architecture. Operational models must be transformed in order to get the true benefit from the cloud. This can only happen with executive leadership's public commitment to cloud, as well as tolerance for growing pains and investments in rebuilding capabilities in new areas. A cloud transformation can only happen from the top down.

By getting out of the space, power, cooling and physical layer of data storage and production, costly and idle reactive servers and facility engineers can be replaced by proactive software engineers creating new products and services that add to the bottom line. A pay-as-you-go model, and subscription based approach, right sizes infrastructure at scale. Data can be manipulated with fine grained controls and processed securely at record compute speeds. Actionable intelligence can inform software design to help deliver financial products that delight the modern consumer. Financial services firms can and are banking on cloud, and consumers can bank on a secure, performant future full of digital innovation thanks to cloud technologies.

Review Your Financial Services Cloud Project with a FOGHORN Cloud Expert.

SCHEDULE A CALL

Foghorn Consulting was founded in 2008 with a mission to ensure that cloud computing initiatives deliver maximum value for its customers. Based in the Silicon Valley, Foghorn provides domain expertise in strategy, planning, execution and managed cloud services to high-growth and enterprise companies seeking a cloud partner. Our team of DevOps engineers, SRE's and certified cloud architects bring over 20 years of domain expertise to ensure your cloud initiatives are a success.

FOGHORN

330 Townsend St, Suite 202

San Francisco, CA 94107

foghornconsulting.com

info@foghornconsulting.com

650-963-0980