Deloitte.

Secure and Private Computing for Banks on a Cloud Platform

Team 37
Timothy O'Connor, Gaurav Shukla, Brian Dempsey, Katherine Stammer, Bradley Martin Mroz
Coach: Ranjit Bawa, Myke Miller
May 29, 2015

Table of Contents

Abstract

Banks are increasingly leveraging the scalability, flexibility and affordability offered by cloud computing over myriad applications. Market forces requiring additional flexibility and customer demands for lower costs are driving them towards incorporating cloud computing into more areas of the business.

Over the past few years, we have witnessed security breaches that have resulted in the loss of hundreds of millions of customers' personal, financial and medical information being compromised and billions of dollars in economic damages. Given these high profile breaches and energized regulatory oversight specific to the financial services industry, maintaining the security of confidential data and customer privacy is a reputational, legal and economic imperative.

The introduction of cloud technology introduces security enhancements above legacy infrastructures by automating tasks like provisioning and access management. However the usage of a physically shared infrastructure also introduces new potential vulnerabilities unless the system is tightly monitored and controlled.

We argue that an effective cloud security and privacy solution requires both the inclusion of key security features in the technology as well as a properly designed governance organization and processes.

This paper will provide an overview of the technology features, organization structures and processes needed to achieve comprehensive and sustained security for cloud computing in banking.

What is at stake?

Cloud computing means entrusting data to information systems that are managed by internal or external parties on remote servers, “in the cloud.” Cloud-based storage, on-line documents (such as Google docs), and customer-relationship management systems are familiar examples.

Cloud computing raises privacy and confidentiality concerns because the very features that make the cloud an attractive platform economically – the shared infrastructure, data replication and redundancy by design, dynamic provisioning, etc – create unique difficulties complying with customer data privacy and security requirements within banking.

As summarized in the table below, there are 4 key reasons why compliance with data regulations for a multi-national bank creates difficulties when leveraging a cloud platform:

Despite these complications, economic factors and trends within Banking are driving large banks to still migrate to a cloud environment.

Challenge 1: Extraterritorial Regulatory Reach
Constrained data transmissions: While data laws have significant local effects, many of these laws restrict data transmissions abroad to regulate noncompliance offshore, and are therefore extent inherently cross-border. This limitation restricts the degree to which shared infrastructure can be leveraged by a multi-national bank. Large domiciles, such as the United States, can manage to gain the benefits of scale locally despite even their patch-work of regulations. Smaller domiciles, such as countries in Europe and the Middle East, create far more limiting constraints on the physical placement of data.
Challenge 2: Data Accessibility and Retention
Maintaining data usage integrity: In the US, entities that store consumer information on the cloud face the threat of FTC enforcement if their representations to consumers about where and how information is stored and secured do not match their actual practices. In addition, the EU and Australia impose strict requirements on retention and the scenarios under which data must be purged.
Challenge 3: Data Usage Restrictions
Data application considerations: In certain localities, individuals have the right not to be subject to measures which may have legal effects or which significantly affect them where such measures are solely based on profiling As an example, the draft EU regulation restricts the possibility of taking automated individual decisions regarding natural persons. Natural persons have the right not to be subject to measures which may have legal effects or which significantly affect them where such measures are solely based on profiling. These restrictions will need to be enforced in a multi-tenant, dynamically provisioned environment
Challenge 4: Significant Penalties
Threat of potential fines: Cloud computing means entrusting data to information systems that are managed by internal or external parties on remote servers. Cloud computing raises privacy and confidentiality concerns because the very features that make the cloud an attractive platform economically - the shared infrastructure, data replication and redundancy by design, dynamic provisioning, etc – create unique difficulties complying with customer data privacy and security requirements within banking

We present Deloitte's approach to enabling global banks' technology needs while remaining compliant with relevant data regulations

Technology Trends in Banking

In addition to the regulatory pressures, the banking industry is experiencing other external pressures including:

1. ***Capital inadequacy*** that depresses profit margins, placing pressure on banks to reduce costs
2. ***Enhanced customer expectations*** for new services and offerings
3. ***Fierce competition*** for customers resulting in industry consolidation and the entrance of nontraditional firms

We are seeing a confluence of customer expectations and market trends that are converging towards banks increasingly adopting cloud platforms As banks adapt to higher regulatory scrutiny, a renewed focus on streamlined costs as well as the flexibility that their customers desire. We see this trend only accelerating.

Cloud computing is revolutionizing ecosystems in multiple industries, and banking is no exception. Cloud technology offers secure deployment options that can help banks develop new customer experiences, enable effective collaboration and improve speed to market—all while increasing IT efficiency. Cloud adoption is growing rapidly because it can be made secure for business. In fact, according to the IBM 2010 CIO Study, "Sixty percent of CIOs plan to use Cloud—up from thirty-three percent two years ago." If we summarize our core drivers we see that there is an overwhelming need to leverage cloud infrastructure in banking to retain a competitive edge:

Balancing this need to expand usage of the cloud platform while also remaining compliant with the disparate regulations is the key to realizing the full benefits of cloud adoption.

Unsurprisingly, as shown in ***Figure 1***, the financial services industry represents the most lucrative sector for cloud computing vendors as FSI firms will likely be the highest spenders on cloud versus

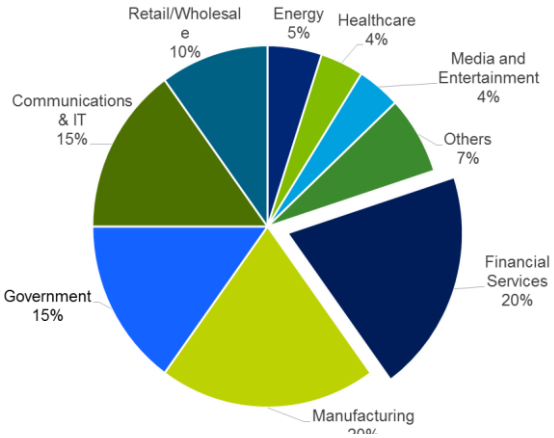

Figure 1: Cloud Computing Spend Share

companies in other market verticals.

More importantly, as seen in Figure 2, even as FSI is the dominant industry for business oriented cloud spend, cloud computing as a proportion of overall IT

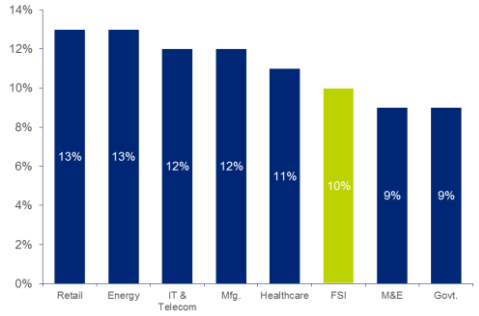

Figure 2: Cloud Spend as a Proportion of IT Spend

spending within FSI is relatively low. This indicates that there is still plenty of room to grow.

The net result is that we can anticipate banking firms will continue to invest heavily within cloud computing.

Key Banking Regulations

Given that banks will respond to economic needs to remain competitive, we can examine our security and data constraints further. Generally, most countries require that we maintain:

Customer Privacy

Collecting personal financial information from customers is required for day-to-day banking operations. Recognizing the potential damages from privacy loss, key policies and laws have been established to regulate how banks are able to collect and share customer data. In most regions, customers have the right to be informed what their data will be used for through privacy policy communications. Governments may require banks to provide customer information to support efforts to prevent money laundering and terrorism.

Data Security

Data security measures seek to protect customer data from loss and unauthorized users. Some of the key methods of data security are encryption, backups, data masking, and user authorization. Increased outsourcing to third-party service providers also produces a heightened need for data security. Many countries have limitations on the storage and access of customer data in other countries, an issue that continues to grow as banks outsource IT and other functions to offshore locations.

Key Country Guidelines

Globally, the means by which these two goals are maintained vary both in the degree to which the objectives are defined and the execution methods and penalties.

United States

In the United States, customers are protected under the Right to Financial Privacy Act passed in 1978, which regulates government and third party access to customer financial data and requires banks to have an initial and annual privacy policy notice. Additionally, consumers must have the option to opt-out from sharing personal information with nonaffiliated third parties. Other laws, however, have established U.S. government access to financial data. The Bank Secrecy Act of 1970 requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Under this act, financial institutions are required to record cash purchases of negotiable instruments, report cash transactions exceeding $10,000, and report suspicious activity. Additional regulations have amended the Bank Secrecy Act, such as the USA Patriot Act of 2001. This act required banks to report information to the U.S. government that would assist in preventing international money laundering and financing of terrorism.

European Union

The European Data Protection Directive serves as the comprehensive data protection standard across the European Union. It establishes that data should not be processed unless it is transparent, for a legitimate purpose, and appropriately collected and handled. Individuals have a right to know when their data is being processed and for what purpose, and data may not be processed without receiving consent. Data should not be collected and used unless it is for a legitimate purpose. Data should only be collected when essential, and should not be stored longer than needed.
An additional General Data Protection Regulation is currently being drafted that proposes a 2 year period to transition the EU to a more rigorous data protection framework. Key changes to the current data protection framework include:

1. A single set of rules on data protection , directly applicable in all EU Member States
2. Increased responsibility and accountability for those processing personal data, for example, companies and organizations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours)

3. Organizations will only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the EU

4. Wherever consent is required for data to be processed, consent must be given explicitly, rather than assumed

China

Globally, the banking regulatory atmosphere for customer privacy varies significantly. In China, the legal system gives the government extensive access to personal data from banks and other businesses. The SN-NPC Decision in 2012 prohibits selling personal data to others, but there is not a significant banking regulatory movement to protect customer financial data.

At the end of 2014, the China Banking Regulatory Commission (CBRC) and Ministry of Industry and Information Technology (MIIT) issued the Guide to Banking Data Privacy and Security Regulation

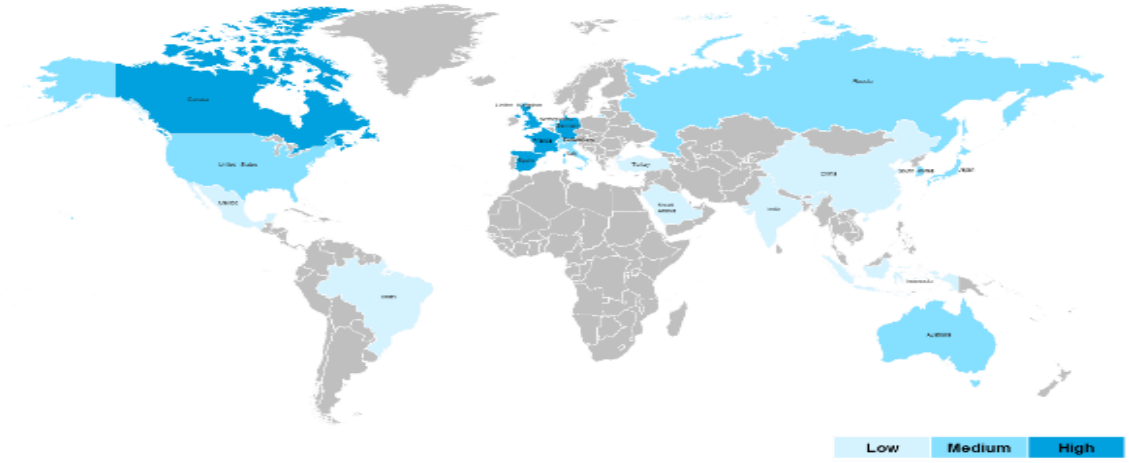

Figure 3: Global Information Regulations

Promoting Banking Application of Secure and Controllable Information Technology. The Guide requires banks to ensure that at least 70 percent of their IT products are "secure and controllable" according to Chinese law. It would also highly regulate banking technology in a way that would favor domestic producers, making it controversial with international players who feared being required to provide encryption keys and hardware "back doors." Although this law has been delayed for further review, banks may still be required to provide authorities with encryption keys and store data domestically in China under a new law that is being drafted to counter terrorism.

Japan

Japanese banks are prohibited from providing personal data to third parties without consent from the subject. However, they are required to report suspicious transactions to the Financial Service Agency in compliance with the Act on Prevention of Transfer of Criminal Proceeds.

Germany

The primary legal source of data protection in Germany is the Federal Data Protection Act which implements the European data protection directive 95/46/EC. This directive serves as the comprehensive data protection standard across the European Union.

Implications and Key Technology Considerations

The diverse criteria imposed across the key global financial centers impose critical issues that cloud service consumers must consider as they consider whether and how to leverage the technology platform most effectively. Typical considerations that we have observed within banking include, but are not limited to the following:

Considerations Across the Data Lifecycle	
I. Data Segregation & Protection	▪ Do Service Providers Segregate Customer Data into Logical Zones – Isolate & Contain Zones to Prevent Data or User Activity Leakage? ▪ Is a Comprehensive Data Segregation Policy in Place to Protect Users in a Multi-Tenant Environment? ▪ Are Zones Configured Individually via the Compute Resource Manager for Distinct Levels of Trust & Confidentiality ▪ Is Zone Segregation Monitored for Visibility and Enforcement via the Compute Resource Manager? ▪ Are there Controls for Supporting Cross-Border Data Views Given Diverse Geographies and Regulatory Environments?
II. Data Integrity & Deletion	▪ Is an End to End Data Management Process from Conception to Deletion Established? ▪ Is Data Completely and Effectively Destroyed Prior to Repurposing Resources for New Users? ▪ A Data Loss Prevention Program to Monitor, Prevent, and Assess Loss of Data in Use, Data in Motion, and Data at Rest is in Place. ▪ Data Access, Uploads, Changes, Encryption, and Deletion are Monitored via the Compute Resource Manager by Service Provider System Admins. ▪ Policy for Data Management/Deletion in the Case of Server Seizure of Multi-Tenant Physical Servers is in Place.
III. Data Classification & Privacy	▪ Comprehensive Data Classification Policies and Application Encryption Standards are Clearly Defined and Closely Followed. ▪ Compliance Boundaries and Responsibilities Owned by the Business and Service Providers are Clearly Understood. ▪ Defined Data Classifications Enable Compliance with Industry Privacy and Security Standards such as the Cloud Security Alliance and NIST. ▪ Clear Data Protection SLAs are Established and Real-Time Continuous Monitoring of Privacy and Protection Standards is Incorporated. ▪ Rights & Obligations for Data Assets Based on the Physical Location of the Data Owner, Custodian, and User are Clearly Established.

Recent Security Breaches and Impacts

If the outlined considerations are not accounted for, there can be severe consequences. We have observed several high profile breaches in the past few years within the financial services industry. Each case has resulted in significant immediate costs to the company reputationally, financially and legally

Company	Issue / Background	Penalty
Anthem (1/15)	**80m SSNs exposed** Reports indicate that hackers gained access to Anthem's by stealing network credentials from at least 5 employees with high-level IT access. Possible means include phishing emails or getting the target to unwittingly download software code that gave the hacker long-term access. Information accessed included names, dates of birth, health care ID numbers, home addresses, email addresses, employment information and income data. No credit card or banking information was compromised. **(Reference)**	- Provided identity protection services to all affected individuals for 2 years through AllClear - Announced breach on 1/29/15. Stock price initially dipped in the following week but has since risen 12% on earnings YTD
JP Morgan	**76m households and 7m small businesses** Hackers had access to a list of applications and program that ran on JPM's infrastructure and began cross checking these programs and web applications for known vulnerabilities. Names, addresses, phone numbers, and emails of account holders were stolen. **(Reference)**	- Bank was forced to respond to numerous regulatory and legal inquiries. Bank also provided credit monitoring to affected customers through a similar program as other high profile breaches. - JPM said it plans to spend $250m on digital security annually but has been losing many of its security staff to other banks over the last year.
HSBC (4/15)	**Mortgage customer data accessible via the internet** Personal information including customers' names, account numbers, SSNs, old account information, and possibly phone numbers we inadvertently made accessible via the internet. Initial assessment of the attack points to lack of encryption as the main issue for data accessibility. (American Banker)	- TBD;
HSBC (11/14)	**HSBC Turkey lost 2.7m customers' bank data** Data theft on cards and related bank accounts for Turkish customers. Information compromised in the breach includes debit and credit cardholder names, account numbers and expiration dates. The bank says that, so far, it has not seen any evidence of fraud or other suspicious activity arising from the incident. **(Reference)**	- Historically, Turkey has not enforced a requirement for institutions to disclose data breaches to individuals, unlike those in place in more than 40 US states. - Not sure if credit monitoring was even provided based on articles read **(HSBC Response)**
Heartland Payment System (1/09)	**100m+ credit card customers card information impacted** A piece of malicious software planted on the company's payment processing network recorded payment card data as it was being sent for processing. The data stolen included the digital information encoded onto the magnetic stripe built into the backs of credit and debit cards. At the time, this was the largest data breach ever. In May 2010, Heartland launched an end-to-end encryption technology designed to prevent magnetic card information from the moment of card swipe and through the Heartland network. (**Sources**)	- Millions of dollars in fines, legal and compliance fees - Damaged share price in early 2009 following the breach

Our Approach

Banks have struggled for years to keep pace with the ever-changing and increasing number of new business and regulatory requirements. Security in the cloud ultimately represents an ongoing technology concern for banks and should be a shared responsibility between banks and third-party cloud providers given that many banks fail to put in the extra controls, processes, or reporting needed to manage risks associated with cloud computing.

Cloud Security Technology Blueprint for Banking

Cloud Delivery Models

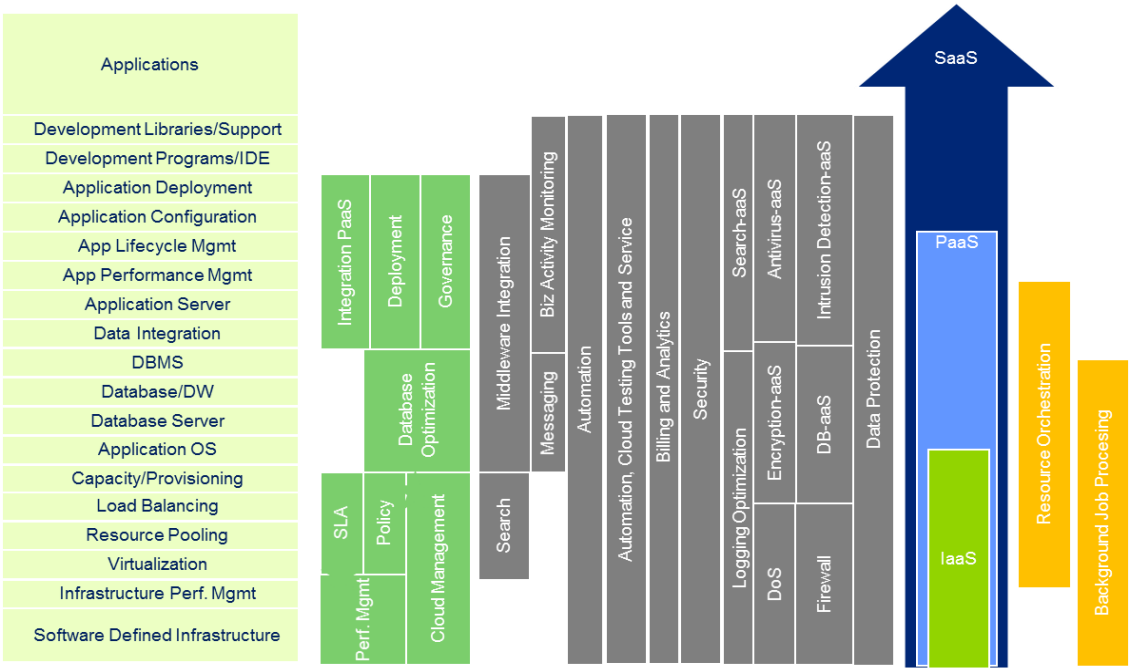

Figure 4 Cloud Computing Delivery Options

Cloud computing can be delivered in a variety of models as highlighted in **Figure**

4. Based on a bank's needs, an escalating portion of the technology stack can be put in a cloud model (whether internally managed or not).

However, regardless of the delivery model used, there are key security features that need to be established.

Access Management and Data Usage Controls

Due to escalating security and privacy concerns over data breaches, the need to centrally control access to data and applications is becoming increasingly vital to banks today. Recently, attackers have been using increasingly sophisticated and complex techniques to target organizations and specific individuals, often looking to obtain people's access credentials.

For preventive controls, banks should restrict access credentials to only directories / databases that are required for a given employee. For this, systems should be used to provide cloud-based bridges to directories. Also, single sign-on capabilities are suggested as having too

many passwords tends to lead to insecure password management practices.

For reactive controls, bank's second lines of defense (compliance and risk) should monitor all application access and authorization via comprehensive audit and reporting capabilities, provided at a granular lev el, so that all activities can be attributed to specific individuals.

Privacy Controls

Regarding privacy controls, at a high level there are three primary cloud implementation models available to banks today: public, hybrid, and private. The first, public, provides services and data centers that are shared among multiple companies, with varying and somewhat limited data privacy controls. With the privacy concerns in the industry today, larger banks are unlikely to implement this option. The second is the hybrid option where some services are managed by a cloud computing provider and others (i.e. an in house, single country data center) are managed internally. This option is likely for banks dealing in countries with some cross border data flow requirements. Lastly, the private cloud option is a cloud network built, managed, and used exclusively by the owning bank. This option is most attractive for universal banks dealing with highly restrictive privacy and data flow requirements and who have customers / branches scattered across the globe.

As part of the above implementation models, one solution to combat the intense data privacy and business secrecy associated with Knowing Your Customer (KYC) in multi-tenant public and hybrid cloud environments is to have the third party cloud provider create virtualized separate application instances and separate master data management systems for each bank or company. At this point the controls can be dialed up or down to control access management and data privacy.

Data Demise Requirements

U.S. regulatory requirements today require banks to keep customer data for an additional seven years after accounts are closed. This obligation should be a shared responsibility of both the third party cloud provider and the specific bank. Given that, it is important for banks to establish a comprehensive data retention policy which is agreed upon between all parties.

At time of disposal there are a variety of ways to ensure clean data in the cloud. Options include crypto shredding (deletion of the encryption key), overwriting of storage media with new or dummy data, degaussing, (removal or reduction of the magnetic field of a storage device), or physical destruction of the storage device (e.g. picture Office Space like destruction…baseball bat to device). The method for destruction should be defined within the data retention policy and defined by each classification of data.

Cyber Threat Defense

Securing monitoring of data will be paramount within any cloud solution approach. Data Loss Prevention processes and auditing will be keys to successful use. Several key challenges must be considered for cyber threat defense. Incident detection and response can be a difficult to create, maintain and test/validate effectiveness prior to a situation. Data movement protection can be difficult as well as protection at rest with acceptable use /access. Patch and Vulnerability Management can be an issue with a focus on aligned methodologies, adherence to agreed process and timeliness of implementation.

The following components are essential for cyber threat defense:

- Strong firewall and proxy server
- Anti-virus software

- Timely and frequent network vulnerability scanning

Banks should perform an internal/external risk assessment including Penetration-Testing, Vulnerability Scanning, Social Engineering and business process analysis related to data security.

They should also develop a cloud computing roadmap based on business risk exposure (low-high), Cost of Ownership (CoO) and opportunity of Return on Investment towards moving to the cloud. These two components should combine to create an overall cloud computing approach

Cloud Security Governance and Processes

The Deloitte Risk Intelligence Roadmap for banking details major security and privacy risks for providing cloud services, framing a security and privacy approach

As seen in **Figure 5**, within banking, we can see that there are typical areas that are

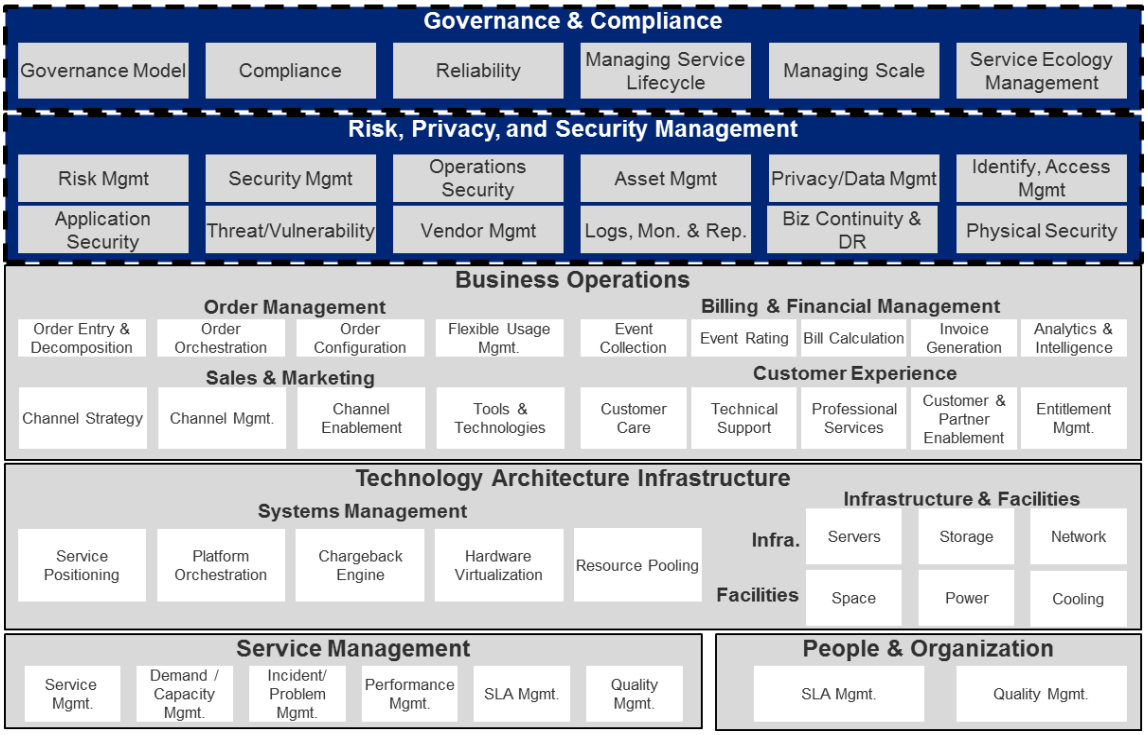

Figure 5: Key Security Capabilities for Cloud Computing

impacted disproportionately due to the heavy regulation:

Security Operations

Security Operations Center (SOC): Subscribers need to ensure that all cloud service providers have an operational SOC with five basic capabilities: event correlation, collection, notification, analysis and second tier reaction/resolution to /incidents and/or outages.

Sensitive Applications & Data: Transfer Subscribers need to align with service providers and use secure transfer processes for exchanging of application and data in transit and at-rest.
Real-Time Risk Monitoring: Subscribers should carefully evaluate service providers to ensure adequate monitoring of security systems such as Intrusion Detection Systems, Security Information and Event Management, and Compliance Policy Management takes place.

Challenges

- SOC alignment between CSP and user community difficult to align based on maturity matrix, acceptability and function focus. Some CSP do not have formal SOC process in place.
- Establishing process or systems to monitor transfer of protected data. Additionally installing reporting systems to capture, correlate and

produce valuable and actionable data (False/Positives)

- Staff acceptance and understanding of CSP service as well as understanding shared security responsibilities between the CSP and the user organization. Additionally boundaries of responsibility based on incident discovery/notification.

Key Steps

- Security review and assessment to validate readiness to adopt a shared security responsibility within a subscription-based relationship.
- Create a strategy to validate compliance, operational risks and interconnected security management expectations.
- Develop an operational privacy readiness assessment for evaluating data movement between the business and the cloud service provider.

Cyber Threat Defense

Interconnected Security Framework (ISF): Security in the cloud is a partnership providers and subscribers; defined secure boundaries need to be established within explicit security agreements.

Data Security in the Cloud: Securing monitoring of data will be paramount within any cloud solution approach. Data Loss Prevention (DLP) processes and auditing will be keys successful use.

Real-Time Risk Management: Establishment of a "Continuous Monitoring" program to document and monitor explicit security practices between the business and service providers related to Access, Vulnerability, Data and System security management.

Challenges

- Incident detection and response process can be a difficult to create, maintain and test/validate effectiveness prior to a situation.
- Data security in transit, at-rest and acceptable use within the cloud. Data movement protection can be difficult as well as protection at rest within provider environments along with acceptable use /access by the service provider.
- Patch and Vulnerability Management (PVM) between businesses and providers can be an issue with a focus on aligned methodologies, adherence to agreed process and timeliness of implementation.

Key Steps

- Perform internal/external risk assessment to include Pen-Testing, Vulnerability Scanning, Social Engineering and business process analysis related to data security.
- Develop integrated tools sets that are enabled through Cloud friendly architecture, practices and processes and provide equal focus on internal and external threats.
- Application security assessment to ascertain current levels of guard against an evolving attack vectors.

Data Management & Regulatory Compliance

Data Classification: Subscribers as well as service providers need comprehensive data classification policies, standards and user education, which are key factors to moving data to the cloud.

Single Source of Truth (SSOT):
Consumers should establish an SSOT practice of structuring information/data into elements to be stored only once prior to moving to a cloud service provider.
Data Lifecycle Management: Both subscribers and service providers should establish an end to end data management process from conception to destruction.

Challenges

- Operationalizing data classification processes can be challenging internally. Moving data to the cloud creates new challenges for tracking Data in Motion, Data at Rest and Data in Use. A comprehensive Data Loss Prevention (DLP) process is necessary.
- Defining Single Source of Truth can be difficult and should be driven by business owners of the data. Process includes owners, data classification and data lifecycle.
- Institutionalizing a data lifecycle process can be complex based origination source (internal/external), ownership, regulatory requirements and retention policies or expectations.
- The regulatory environment for Cloud Computing is unknown and rapidly evolving, making compliance difficult to plan for over the long term.

Key Steps

- Review existing data classification and data lifecycle policies, standards and processes as well as source of record repositories
- Identify what data elements to move to a cloud solution based on assessments of regulatory requirements for data in the cloud
- Create a strategy to sanitize sensitive, duplicate & protect data
- Establish and/or update Data Loss Prevention (DLP) program to monitor, prevent and assess DiU, DiM and DaR. Additionally define protection/encryption expectations with all cloud service providers to which the business subscribes

Identity and Access Management

Industry wide IAM Standards: SAML, XACML, SPML, Oauth, and OpenID are emerging as key IAM standards to manage identities in the Cloud.
Identity "to" the Cloud: IAM software vendors, such as Oracle and IBM are adding the functionality to provision to cloud-based applications such as Salesforce.com and Google Apps.
Identity "in" the Cloud: New vendors are providing cloud-based Single Sign On (SSO), federation and identity solutions.
Responsibility Tiering: Responsibilities should be delegated to tiers of system administrators and business users aware of applicable data access, use, and disclosure constraints.

Challenges

- Mature identity & access management policies to support cloud transition. Additionally, if using an IAM solution how to leverage, integrate and/or move to the Cloud within the existing solutions?
- Evaluating levels of service, security and capabilities to meet current business and maintain security, privacy and regulatory compliance as it relates to IAM.

Key Steps

- Assess compatibility and readiness of policies, standards and processes to support migration to a cloud solution.

- Evaluate existing security architecture for managing digital identities currently and possible changes for cloud adoption.

- Define and assess governance, policies and standards for creating and managing Identity's workflows and define the changes necessary for migration to the cloud.

Privacy Protection

Privacy: Organizations need to understand their privacy requirements, cloud capabilities and establish how they protect certain data.
Regulatory Framework: Compliance boundaries MUST be established. “Rules of Behavior” and explicit compliance roles and responsibilities should be maintained between the business and service providers.
Privacy Laws: The location independent nature of cloud data can conflict with various state and international country privacy laws. As data moves around the cloud, privacy directives and other agreements may be needed to manage compliance.

Challenges

- Data geography, asset management and privacy responsibility within cloud environments can be extremely difficult to define, control and maintain.

- Incident response, privacy breach notification, business associate agreements and reporting responsibilities workflows can be complex based on cloud models (Private, Hybrid or Public) and regulatory frameworks and standards.

- Information protection – Data in Use (DiU), Data in Motion (DiM) and Data at Rest (DaR). Areas of focus - Access Controls, Identity Management, Encryption and Data Loss Protections (DLP).

Key Steps

- Comprehensive review of internal policies and operational processes with focus on data management and privacy responsibility based on cloud model (Private, Hybrid or Public).

- Assess current regulatory responsibilities and map/outline control responsibilities between cloud provider and subscribers. (e.g. Provider/Customer - Common, Hybrid or Inherited controls).

- Review/establish contract management practices specific regarding Service Level Agreements (SLA), Interconnected Security Agreements (ISA) & Business Associated Agreements.

- Application security assessment to ascertain current levels of guard against an evolving attack vectors.

Conclusion

Adoption of cloud computing has passed a tipping point and is increasingly a fact of life for many banks, and IT will not succeed in undoing that trend. However this change in technology does not allow IT organizations to ignore their responsibilities to their customers. Cloud computing needs to meet the growth in usage while also complying with privacy laws and data restrictions

Deloitte recommends an approach that manages the entire landscape to protect customers proactively as banks evolve their infrastructure. We advise that:

Security is a Core Consideration During Profiling and Technology Design: We must ensure that proper data management, privacy and security considerations are taken into account when initiating a migration effort. Failure to do so has resulted in severe financial, reputational and legal consequences in the past

Governance and Process Changes are Critical: A properly architected system will not enable a secure environment on its own. An ongoing oversight mechanism needs to be incorporated to manage ongoing changes, monitoring and reporting.

Using Lessons Learned and Available Toolsets Will Expedite a Transition: Several banks have undertaken this technology change. Leveraging their experiences can bypass common pitfalls and accelerate the time to delivery

By adopting a balanced approach towards not only implementing cloud technology, but also implementing the appropriate security, governance and process controls, banks can create an environment that can fully leverage the cloud platform. Deloitte, with our deep experience in both the industry and the technology, is ideally positioned as a partner to guide clients through migration.

Contacts

Timothy O’Connor	Senior Manager	**tioconnor@deloitte.com**
Gaurav Shukla	Manager	**gashukla@deloitte.com**
Brian Dempsey	Manager	**bdempsey@deloitte.com**
Katherine Stammer	Consultant	**kstammer@deloitte.com**
Bradley Martin Mroz	Consultant	**bmroz@deloitte.com**