White Paper

Banking on Cloud

Essential tips for implementing a cloud strategy.

iCreate | BANKING INTELLISENSE

WE PUT THE BANKING INTO BUSINESS INTELLIGENCE

www.icreate.in

Banking on Cloud

Essential Tips for Implementing a Cloud Strategy

The Banking sector is renowned for the volume and velocity of Data it generates, transmits and stores. Given the recent financial crises and the subsequent regulatory pressures, the cost of IT has grown exponentially for not just the banking organisation on the whole but even at a divisional level.

Banks are now faced with drastically cutting IT costs, but not at the cost of compromising data security and integrity, which could lead to reputational, legal, monetary damages. The need therefore to explore unconventional and innovative options which shrink IT costs while safeguarding data integrity. However, with limited resources and even limited budgets, a conventional IT implementation methodology is neither an efficient nor an advisable solution.

Cloud as a technology option for Data and business processes has gained a credible foothold in recent times across several industry sectors including financial services. This article details the 'must knows' for implementing an efficient and secure information management framework in a Cloud environment. Let's first take a quick look at the various Cloud delivery and deployment models available for a bank.

Cloud Delivery Models

Software as a Service: A SaaS service provider hosts the application software and related Data. A user is provided minimal access to administrative control while the complete application can be accessed through web services.

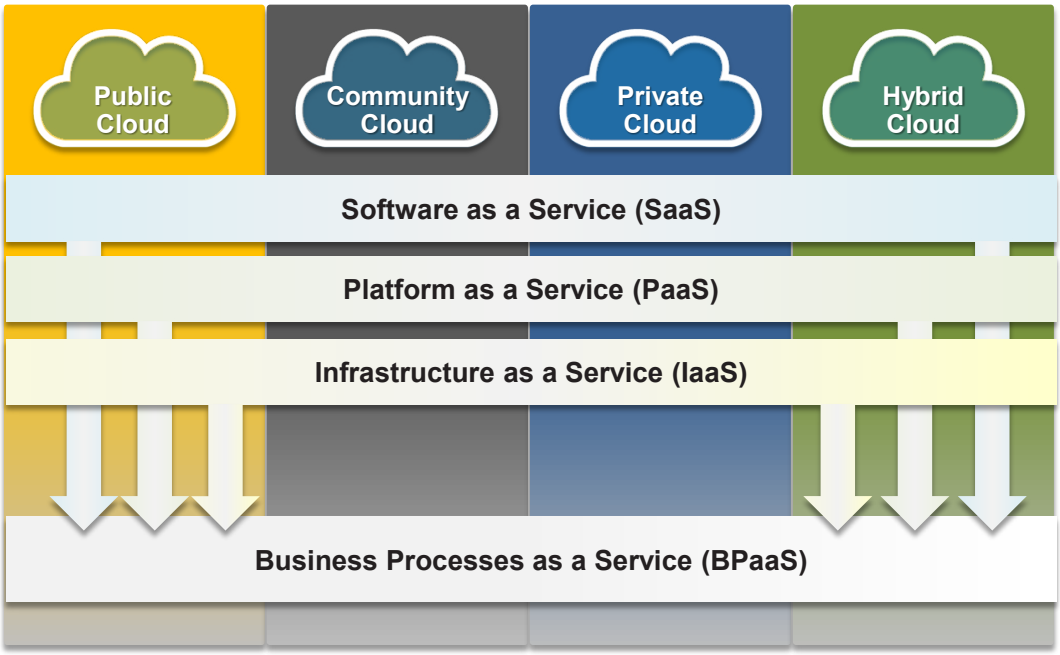
Platform as a Service: A PaaS service provider hosts a pre-deployed and pre-configured environment for development, maintenance and testing of custom applications. A user is spared of enormous IT overheads (arising from hardware and software), during various stages of application development.

Infrastructure as a Service: An IaaS service provider hosts only the infrastructure required to build/maintain an application. Various infrastructural components could be servers, network connectivity and other non-configured resources. Users can create various levels of controls in a Cloud environment or rather create their own platform for custom application development

Business Process as a Service: Business processes are activities performed in the process of delivery of services to end customers or stakeholders. One of the well know technology research firm defines BPaaS as "...delivery of business process outsourcing (BPO) services that are sourced from the Cloud and constructed for multitenancy. Services are often automated, and where human process actors are required, there is no overtly dedicated labour pool per client. The pricing models are consumption-based or subscription-based commercial terms. As a Cloud service, the BPaaS model is accessed via Internet-based technologies."

BPaaS is delivered on a Cloud model using either one or a combination of the foundational delivery models as illustrated below.

Cloud model options for Banking



Cloud Deployment Models

Public Cloud: A public Cloud infrastructure is owned by a third party vendor who is responsible for creating, maintaining and upgrading the environment.

Community Cloud: In recent times, community Cloud has evolved as a separate deployment model, although being similar in characteristics to a public Cloud. The only differentiating characteristic of a community Cloud is that it is owned by or maintained for a specific set of users. The access is restricted to the community members only.

Private Cloud: The infrastructure for a private Cloud is hosted only for a single organization. It can either be managed by the organization itself or can be outsourced to a third party vendor.

Hybrid Cloud: A hybrid Cloud consists of two or more different deployment models, which though distinct, are linked to provide services to end consumers.

Financial Data Classification

Although Data classification processes are quite difficult to implement within the context of a financial institution, the methodology and parameters are clearly defined. The major objectives of determining output of Data classification are **Confidentiality** (loss of confidentiality is the unauthorized disclosure of information; **Integrity** (loss of integrity is the unauthorized modification or destruction of information; and **Availability** (loss of availability is the disruption of access to or use of information).

Based on the potential impact levels of breach of security for information, Data can be classified as -

- **No impact:** No adverse effect
- **Low impact:** Limited adverse effect
- **Moderate impact:** Serious adverse effect
- **High impact:** Severe or catastrophic adverse effect

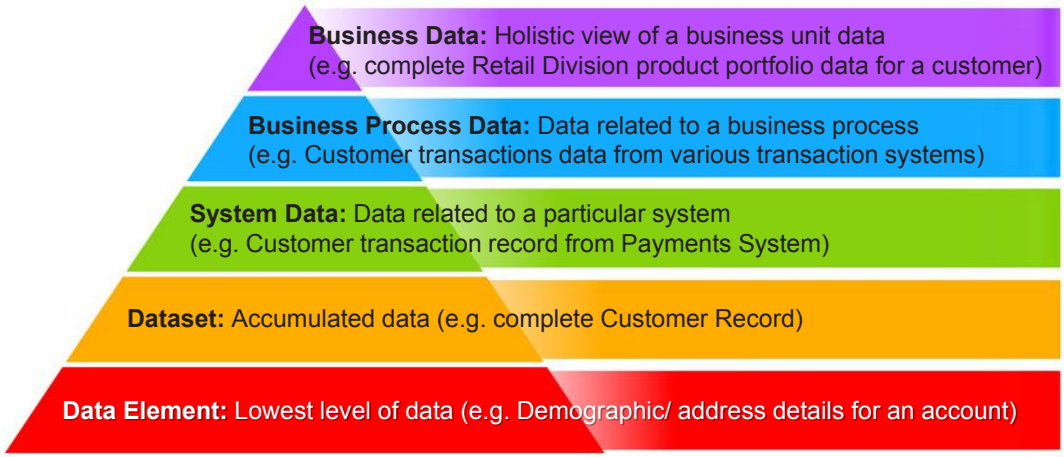
Data at every level of information hierarchy (as shown in Information Hierarchy based on levels of abstraction illustration below) has to be classified within the above categories and the process of classification involves the following steps:

- Business owners work with the Information system owners to map the Data (from various systems that a specific business owns), under the above categories.

- Representatives from each business unit, then work together to ensure that the definition of levels for similar elements across business units remain consistent. This has to be done in the presence of the Data Governance team members and Information system owners.
- The Data category is officially recorded for each type of Data processed or stored by the systems

Since, it would be a cumbersome process to categorize each Data element into the above buckets; it is advisable to categorize higher levels of the information hierarchy. However, one should be cognizant of the fact that the higher level would take precedence over the lower level in all aspects of Data security. So, all components within business process Data (i.e. system Data, Dataset and Data element) would be classified as "High Impact", if the "Business Process Data" is classified as "High Impact", irrespective of whether any lower levels are "Low Impact"

Information Hierarchy based on levels of abstraction

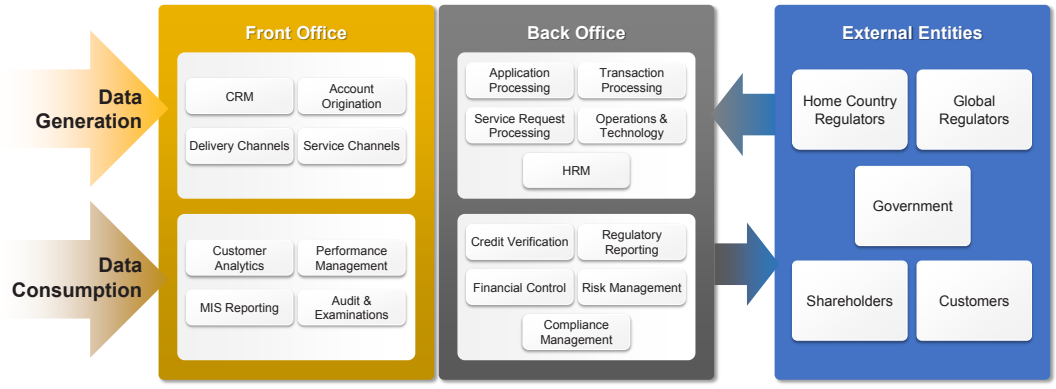


Classifying Information within a Banking System

The processes in a bank can be viewed from various perspectives. A sample set of processes from a functional perspective could be from Corporate Banking, Retail Banking, Trade, Treasury, Investment Banking, Brokerage, Corporate Functions, Risk & Compliance Management and Customer Service. To deep-dive into the Data requirements, we have classified the processes in a bank from the Data lineage perspective (as shown in the Process Classification by Data lineage illustration below). The Data can be either generated or consumed by the front office or a back office (which includes mid-office operations as well).

Front office implies functions that have direct client or shareholder contact, while back office supports the front office activities. All processes that create Data in any form (for example - CRM/Account Origination process creates lead Data or new customer records with all personal information) are classified as Data Generation Process. All processes that consume the Data and create an output to be provided to stakeholders/regulators (external entities) are categorized as Data Consumption Process. A sample set of processes in each category is shown below.

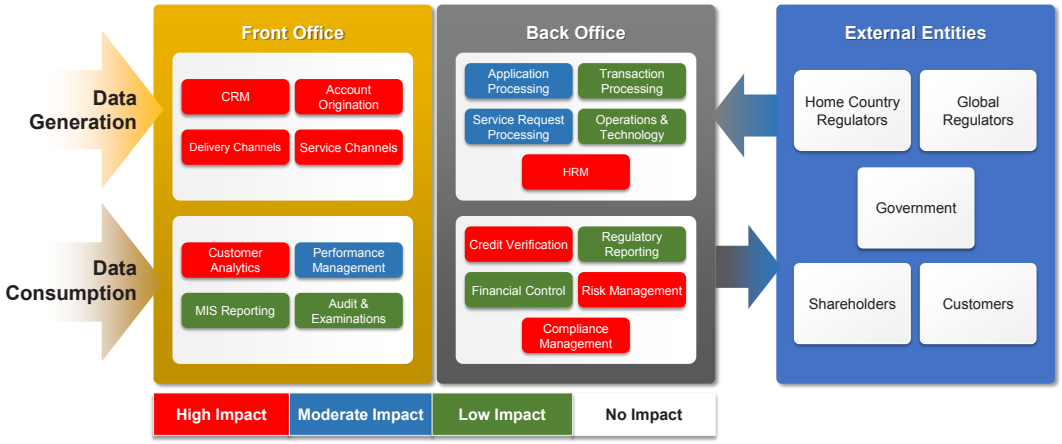
Process classification by Data lineage



Once the classification is completed, each process (4th level in Information Hierarchy) is analysed for the Data type involved in either generation or consumption and finally infer the impact of Data security breach. Each process can be categorized from “No Impact” to “High Impact”, based on the lowest level of Data involved in the process. Let’s analyse two processes to illustrate this point -

- **Account Origination:** The lowest level of Data accessed in the account origination process is customer personal information. The recent spate of system breaches that have compromised customer information have not only proven the increasing number of attacks on such Data but also underscored the importance of security layers for the same. Compromises typically result in reputational, legal and monetary damages. Hence this category of process has been market as “High Impact”.
- **Regulatory Reporting:** The lowest level of Data required for regulatory reporting is either General Ledger or product financial details. Most of the Data is at an aggregated level resulting in minimal customer information to create regulatory reports. Hence, the instances of Data breaches in such a process and the impact of such a breach is minimal. A regulatory report therefore has been categorized as “Low Impact”.

Process categorization based on potential Data impact levels



A Framework for Information Security

The processes defined by the bank also needs to be able to address issues pertaining to information security including -

1. Risk Assessment and Mitigation Plan: To identify and assess threats, vulnerabilities and their probabilities and outcomes. The plan should also have a mitigation plan for these threats covering technology tools, procedures and training.
2. Implementation Plan: The acquisition and operation of technology and delegation of duties and responsibilities to managers and staff. It also includes the understanding of responsibilities by everyone involved in the process.
3. Monitoring and Updating: The use of audits and various other tools to gain assurance that the risks are being assessed and mitigated and processes are in place and performing as intended. Also, to continuously gather and update information on new threats and vulnerabilities and update 1 & 2 above on a continuous basis.

US Laws governing Data Privacy

Protection of Non-Public Personal Information

Gramm-Leach-Bliley Act, 15 USC 6801

Title 15, Chapter 94, Subchapter I, Sec. 6801. Us Code Collection - Sec. 6801.

(a) Privacy obligation policy.
It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ non-public personal information.

(b) Financial institutions safeguards.
In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards -

(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records;
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any Customer

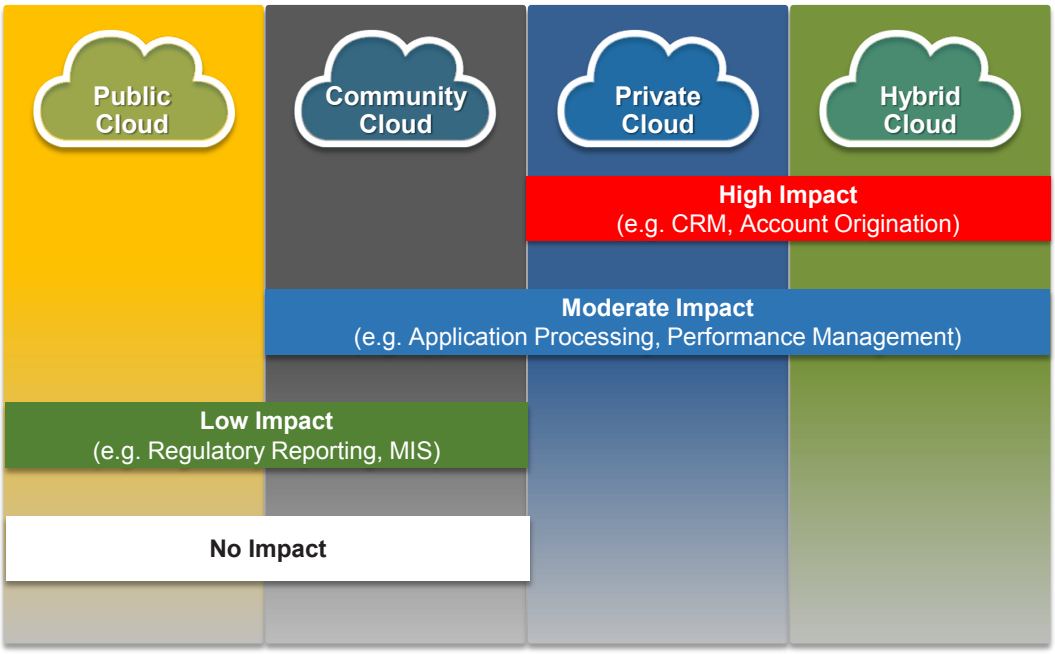
The steps recommended by regulators on the basis of the information related laws (refer right box for Gramm-Leach-Bliley Act on information security in US) for implementing the above are

- Setting up of a Governance team
- Defining an Internal Information Privacy policy
- Mapping Information security levels and their implications
- Defining a Cloud strategy
- Identifying multiple deployment options
- Identifying Technology and partners
- Implementation and Governance cycle
- Periodic Reviews and improvements

Banks need to ensure that the steps above evolve into an on-going and continuously improving process within the organization rather than a one-off activity.

Suitability of Cloud

Suitability of Cloud based on impact level of breach for a Data element



In terms of security levels, a Private Cloud is the most secure option and should be used for “High Impact” Data. A Hybrid Cloud which contains a Private Cloud component, wherever the Data warrants that level of security could also be suitable for high impact Data. “Moderate Impact” Data can be securely accommodated either in Hybrid or Community Clouds with a reasonable amount of confidence, as access is well controlled in these modes and the probability of breach is comparatively low.

“Low Impact” Data and “No Impact” Data (where there is minimal personally identifiable information) are viable cases for moving into a Public/ Community Cloud setup. Security levels in Public Clouds have increased tremendously in recent times, with various providers incorporating multiple levels of encryption not only while storage, but also during transmission. This can help banks shrink their technology costs exponentially, while ensuring that their Data is secure. Although, most banks continue to be sceptical about moving any form of information to a public Cloud, it is only a matter of time when public Cloud becomes the usual norm given its scalability and cost-efficiency.

The Way Forward

A well-devised Information security policy with clearly evinced sponsorship from the board and senior management is fundamental to the Cloud strategy. Also, concerns around storage, transmission and usage of Data (driven by various factors including risk and regulatory factors), vis-à-vis Cloud are not any different from those in the areas of Business Processes Outsourcing or Technology Outsourcing; both of which have been successful and cost-optimized IT options which Banks have been successfully leveraging.

However, a Data classification/ hierarchy definition followed by a detailed mapping exercise to determine the ideal Cloud option would be an essential first step. Furthermore, having a strong Data Governance framework and a continuous audit process would help as 'gatekeepers' to the bank's overall Cloud strategy ■

(This paper was published as an article in International Banker, Spring 2014 issue.)

About the Authors:

Ramakrishnan Natarajan is a Managing Consultant at iCreate and comes with seven years of experience in IT Consulting, Product Management and Implementation Management of Technology solutions in the Banking and Capital Markets Domain. A Marketing and Strategy graduate from the Indian School of business, his current interests are in the areas of Compliance and Decision sciences for banks.

Sourav Sekhar is a Lead Consultant at iCreate and comes with six years of experience spread across Investment Banking and IT Consulting for the BFSI Domain. A Finance graduate from the Indian School of Business and a Mechanical Engineer from the National Institute of Technology - Warangal, Sourav's interests span Risk, Compliance and Banking Decision Sciences.