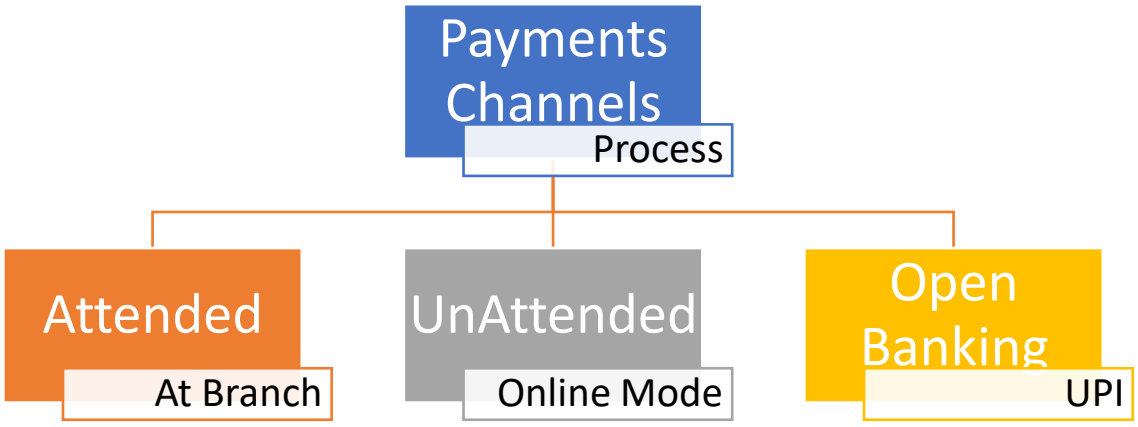
Cloud And Security

Team Members

RAJSHEKAR (Lead)

1. **Manoj**
2. **Priyadarshika**
3. **Arun Balaji**

Payments Methods



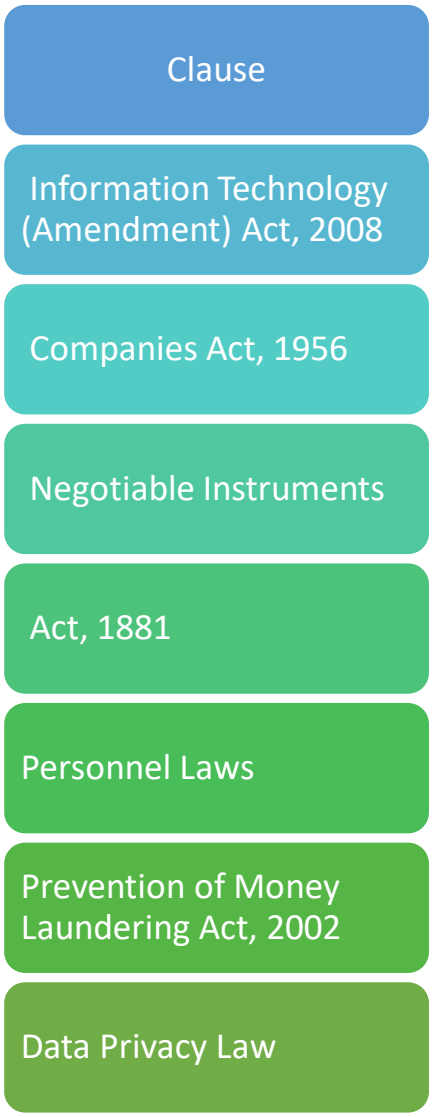
Legal Issues

Data and processes in Cloud Computing should comply with both Indian and international laws when the organization (Bank)availing the Cloud service has an international presence. Legal compliance is to be ensured in availing Cloud service as both Cloud service provider and the organizations availing the Cloud service are bound to comply with the laws of the land where they operate

Key Pints to check Adherence to Laws, Service Level Agreement, Data Security, Access to Data for Purposes of Discovery, Location of Data, Unauthorized or Inappropriate Use, Emergency Security Issues, Ownership of Data, Disclaimer of Warranty, Indemnification by Customer, Indemnification by Vendor, Governing Law and Jurisdiction, Confidentiality, Audit, Compensation for Data Loss/Misuse, Service Levels,

Compliance and Audit

Compliance can be defined as the awareness and adherence to obligations including the assessment and prioritization of corrective actions deemed necessary and appropriate. It is necessary that strict compliance should be observed with various banking related laws, regulations and guidelines issued by the regulating authority as well as other laws applicable in India. As Cloud computing is a relatively new and evolving technology, there are a number of grey areas which are not adequately covered by existing laws and regulations. It is necessary to be extra cautious on the positive side while interpreting and complying with these laws and regulations. A broad list of requirements, acts and laws have been specified for compliance as under.



Roles and Responsibilities

Roles and responsibilities are part of a Cloud environment, in which people and processes, along with technology, are integrated to sustain tenant security on a consistent basis. Security roles and responsibilities of employees, contractors and third party users should bedefinedanddocumentedinaccordancewiththeCloudprovidersandCloudconsumers

information security policy. Based on the conceptual reference model of NIST, the following parties are involved in a Cloud environment.

- Cloud Consumer: This could be a bank or any other consumer that would avail of the services on the Cloud.
- Cloud Provider: This would be a system integrator who would integrate offerings from multiple parties to provide a solution and sign contracts with Cloud consumers. These parties would be data center and hardware provider, infrastructure providers, virtualization software providers, application providers, and network provider.
- Cloud Carrier: This would be the provider of network infrastructure to connect various bank branches to the data center.
- Cloud Auditor: This could be a reputed audit firm who can conduct an independent security, data privacy and performance audit of operational processes and deployment infrastructure. The scope of the audit could include banking aspects depending on the charter, which could be specified. It could also provide for inspection by the regulator.
- Cloud Broker: These parties would provide value added services using aggregation or arbitration on the top of Business services provided by Cloud service providers.

In each of the above parties, roles of the employees and their responsibilities should be defined and documented.

Data and Information Security

DATA and information security provides services that protect unstructured and structured data from unauthorized

access and data loss, according to the nature and business value of information. It also provides usage and access monitoring and audit services.

1. Data Discovery
2. Data Classification
3. Data Migration
4. Data Privacy
5. Data Assurance

6. Data Redaction
7. Data Retention
8. Data Disposal

Application and Process Security

Various service models to access applications on the Cloud.

1. Infrastructure as a Service(IaaS)
2. Platform as a Service(PaaS)
3. Software as a Service(SaaS)

IT Infrastructure Security

- **NetworkSecurity:**Network security consists of security services those restricts or allocate access and those distribute, monitor, log, and protect the under lying resources services.
- **Virtual Environment Security**
- **VM Monitoring**