Cloud Security Framework
for Indian Banking Sector
Cloud Security Framework for Indian Banking Sector

FOREWORD

The rapid emergence of cloud computing is transforming the way organizations think about their IT resources. Cloud computing, which offers vast cost-effective computing resource as a service on a pay-per-use basis in different models, is proven to directly translate to less upfront capital expense and reduced IT overheads.

Cloud computing is increasingly becoming an integral component of any organisation's computing strategy. Organisations including banks now understand that cloud computing offers the possibility of being able to seamlessly change IT without expending the time and resources in setting up, configuring, and deploying new systems. This technology offers a more efficient use of resources such as storage, memory, processing, applications and bandwidth ensuring high availability, security and quality.

The advantages of Cloud computing are many. However, there are a few concerns in cloud computing related to security and privacy which are to be addressed before taking it forward. The Reserve Bank has been echoing these concerns for some time now.

The Cloud Security Framework for Indian Banking Sector prepared by IDRBT is an excellent document that covers all the aspects relating to the security of Cloud computing which are to be necessarily examined by banks intending to use Cloud solutions.

I appreciate the hard work that has been put in by IDRBT and I am sure this material would go a long way in serving as reference material for banks attempting to deploy Cloud Technologies.

Anand Sinha
Deputy Governor,
Reserve Bank of India,
Chairman, IDRBT.
MESSAGE FROM IBA

Banks business levers will concentrate on enhancing the distribution model, specifically around two axes: customer centricity and the potential of new and emerging devices to deliver true multichannel experiences. Banks will have to transform their product offerings, channels and customer services to reflect the demands of the changing consumer who is connected, impatient, empowered, and demanding of services that meet their individual and social needs by reshaping and reinvention of their core banking operations to enable a more competitive, customer-centric, efficient and sustainable business model. All of the above will be shaped around trends like cloud computing, service-centric architecture, IT security and data privacy, user experience, social platforms or data accessibility and analytics.

As banks adapt to the changes in their competitive and technology environments, cloud computing will play a major role. Cloud-based offerings will leverage social and mobile media to transform the banking experience and relationships for customers. Cloud’s combination of low cost and high scalability, effectively unlimited processing power and storage, unprecedented agility and speed to market, and variable pay-per-use cost structures all support the qualities that banks will need to compete and win in the future. However, banks' adoption of cloud will be highly selective and targeted, focusing on matching the characteristics of each specific process with the different variants of cloud computing.

There are a number of security issues/concerns associated with Cloud Computing such as privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support, long-term viability, virtualization, identity and access control management, legal issues, isolation of roles, encryption and key management, browser vulnerabilities, etc. Many consortia, organizations and associations like National Institute of Standards and Technology (NIST), Cloud Security Alliance (CSA), Distributed Management Task Force (DMTF), Storage Networking Industry Association (SNIA), Open Grid Forum (OGF), Association for Retail Technology Standards (ARTS), Cloud Standards Customer Council and Organization for the Advancement of Structured Information Standards (OASIS) have taken initiatives to develop security standards and guidelines for the various facets of cloud computing.
IDRBT has developed a set of guidelines and best practices describing IDRBT Cloud Security Framework as a practical, simple and easy to use guidebook for the Indian Banking Industry that will help banks to understand and explore security concerns in the Cloud environment. IDRBT’s Cloud Security Framework consists of security levels that are categorized into horizontal layers and vertical layers. These layers are physical and logical security, IT infrastructure security, application and process security, data and information security and cloud security management.

The guidelines provided in the document are not static and the security concerns of each level in the framework are still evolving. IDRBT proposes to review and update this document periodically by concerning forthcoming security issues in cloud computing. IDRBT’s attempt to provide generic security guidelines and best practices for cloud providers and consumers to get the benefit from the cloud computing is commendable.

I hope IDRBT Cloud Security Framework will meet the requirement gap of the Indian Banking Industry for cloud security best practices and guidelines. I thank and congratulate the Members of the IDRBT Cloud Security Framework Working Group and Institute for Development and Research in Banking Technology (IDRBT) for doing an excellent job in preparing and timely release of this report.

K. Ramakrishnan
Chief Executive,
Indian Banks' Association
PREFACE

There are many definitions of cloud. It is difficult to confine to one. But there are key common characteristics of cloud computing that emerge out of these definitions like dynamic provisioning and de-provisioning, location independent resources pooling, multi-tenancy, rapid elasticity, broad network access, on demand self-service, etc.

The evolution of CLOUD COMPUTING is influenced by some important developments in architectural and technological space. Grid/Utility computing, horizontal scaling, virtualization, high scalability architecture, consolidation, web, etc., have huge influence on cloud architecture. Cloud emerges out of the convergence of these architectural and technology developments.

The concept of cloud computing evokes intense and diverse emotions. Many potential and prospective users in financial sector are deterred by Fear, Uncertainty and Doubt. But the cloud providers and their supporters are going to town touting benefits like agility, flexibility, cost-effectiveness, the benefits of switching over from capex to opex model, on demand self-service, almost infinitely scalable, pay per use and many more goodies. They say you can whistle your way at provision and de-provision. To put it simply, cloud computing is nirvana from all the ills and pains of the present IT infrastructure. But it looks as though it is a divided house between providers and potential users.

Issues of privacy and security are the two most important barriers and rightly so for adoption of cloud by banks. These issues cannot be underplayed. How can one be trusted to keep massive and sensitive customer database on cloud? But one need not throw the baby with the bath water, as is often said. Let us have a quick look at the IT infrastructure and its management. One often hears about complaints that IT infrastructure is monolithic, less agile, less flexible, unable to keep pace with the fast changes and long cycle times to implement new solutions and even execute change requests.

Over the last two decades, banks have accumulated huge and diverse solutions. Most of the time and resources are spent to keep the lights on and fire fighting low-level activities with little time for strategies, leave alone innovation. Not that there are no larger issues. There is an urgent need to consolidate the infrastructure and secondly empower business. One needs to ask a fundamental strategic question. Do banks want to own IT assets or operate business and focus on what they are good at, i.e. banking? IT-business alignment is a neglected area in this milieu quite often. IT governance is yet to mature.
Adoption of cloud does not mean mere replacement of data centers. It is wholly a new IT delivery model and lot of business and operating processes both within IT and Business needs revamp.

Notwithstanding the potential benefits of cloud computing, privacy and security are uppermost on the IDRBT’s agenda for cloud initiatives. CI 4A (CONFIDENTIALITY, INTEGRITY, AVAILABILITY, AUTHENTICATION, AUTHORISATION, AUDIT) is a useful framework to evaluate cloud computing.

Jeff Vance has the following FAQ for vendors. Banks need to find satisfactory answers to at least the following 10 questions before embracing the cloud:

1. Were your service developed using a secure development lifecycle?
2. Can you prove it and provide, say, penetration testing overviews?
3. What data protection policies do you have in place?
4. What are your data privacy policies?
5. How do you enforce those various policies?
6. Is security covered in your SLAs? If not, why not?
7. How do you back up and recover data?
8. How do you encrypt data, both in motion and at rest?
9. How do you segregate my data from others?
10. What kind of visibility will I have into your logs?

This is a fertile ground for institutions like IDRBT with focus on applied research with a practical bias. Not wanting to watch from the sidelines, it took baby steps to test the waters. It has set up a lab to experiment community cloud with open source tools and has roped in technical experts.

To start with, IDRBT is working with a few select banks by migrating non-critical and non-customer facing applications to the community cloud. There is a palpable excitement. Cautious optimism is the watch word. Think big and act small is the guiding principle. This pilot project would offer a lot of practical lessons and help build robust operating guidelines.

Security shall not be after thought. As privacy and security is priority for IDRBT and Banks, this framework is now published for use by banks.

I compliment Dr. G. R. Gangadharan, Dr. Shakti Mishra, Mr. Lalit Mohan and the entire team for bringing out the IDRBT Cloud Security Framework and I am sure that this would provide immense insights to banks.

B. Sambamurthy
Director, IDRBT
Chapter 1

Introduction to Cloud

Cloud computing is a way of delivering IT enabled capabilities to users in the form of ‘services’ with elasticity and scalability, where users can make use of resources, platform, or software without having to possess and manage the underlying complexity of the technology. According to the National Institute of Standards and Technology (NIST), Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

![Figure 1.1 NIST Architecture for Cloud Computing](image)

**Essential Characteristics of Cloud Computing**

- Broad network access from a variety of devices or platforms such as mobiles, desktops, laptops, workstations, etc., through standard mechanisms.
- Rapid elasticity and scalability that allows functionalities and resources to be rapidly and automatically scaled out or in, as demand rises or drops.
- Measured provision to automatically control and optimize resource allocation and to provide a metering capability to determine the usage for billing purpose, allowing easy monitoring, controlling and reporting.
- On demand self-service that enables users to consume computing capabilities (e.g. applications, server time, and network storage) as and when required.
- Multi-tenancy and resource pooling that allows combining heterogeneous computing resources (e.g. hardware, software, processing, servers, network bandwidth) to serve multiple consumers – such resources being dynamically assigned.
Service Models

**Infrastructure as a Service (IaaS)** refers to the capability of provision of raw computer infrastructure, such as servers and storage, by a provider to a buyer. The functions required to provide the infrastructure are abstracted. Users are not required to manage the infrastructure as they do not possess the ownership of the underlying Cloud infrastructure.

**Platform as a Service (PaaS)** refers to the provision of the capability in which development platforms and middleware systems hosted by a vendor are offered to application developers, allowing developers to simply code and deploy without directly interacting with the underlying infrastructure.

**Software as a Service (SaaS)** refers to the capability provided to the user to run and use applications on a Cloud infrastructure of the provider. Buyers are freed from the possession and maintenance issues of software and hardware. The capability can be accessed by users from various client devices.

Deployment Types

**Private Clouds** are proprietary networks, often data centers, residing within the organization for the exclusive use of the organization. These are shared and multitenant environments built on highly efficient, automated and virtualized infrastructures. In case of a private Cloud environment, the organization is in charge of setting up and maintaining the Cloud resources and, thus, the organization can take better control of security and regulatory compliance issues. The added advantage is in terms of better control of security (including security of sensitive data), more effective regulatory compliance and improved quality of services.

**Public Clouds** are Cloud services provided by third parties but hosted and managed by the service providers. The Cloud providers take on the responsibility of installation, management, provisioning and maintenance. The customers access and use the services and physical resources. Consumers are charged only for the resources and services they use.

**Hybrid Clouds** are a combination of private and public Clouds. They combine on-demand external capacity with on-premises resources and in-house compliance. In this case, the management responsibilities are often split between the organization and the public Cloud providers, which can often become an issue of concern.

**Community Cloud** is a semi-private Cloud that is used by a defined group of tenants with similar backgrounds and requirements.

Security and Related Concerns in Cloud

There are a number of security issues/concerns associated with Cloud computing. Gartner report specifies the following seven security issues in Cloud computing.

- **Privileged User Access**: Cloud computing allows the processing of the confidential data of user by personnel outside the organization, so non-employees could possibly have full access to it. Consumer should ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.
- **Regulatory Compliance**: Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications.
- **Data Location**: When a customer uses the Cloud, customer probably would not know exactly where his data is
hosted. It is required to ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

- **Data Segregation**: Data in the Cloud is typically in a shared environment alongside data from other customers. Encryption is effective but is not a cure-all. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability.

- **Recovery**: Even if the consumer does not know where his data is, a Cloud provider should tell to his consumer what will happen to data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure.

- **Investigative Support**: Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.

- **Long-term Viability**: Ideally, Cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But the consumer must ensure that his data will remain available even after such an event. It is essential to know from providers how he would get his data back and if it would be in a format that could import into a replacement application.

Other related Concerns in Cloud are as follows.

- **Virtualization**: One potential new risk has to do with the potential to compromise a virtual machine (VM) hypervisor. If the hypervisor is vulnerable to exploit, it will become a primary target.

- **Identity and Access Control Management**: Cloud providers either integrate the customer’s identity management system into their own infrastructure, using federation or SSO technology, or provide an identity management solution of their own.

- **Legal Issues**: Providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

- **Isolation of Roles**: Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the Cloud providers and Cloud consumers information security policy.

- **Encryption and Key Management**: Organizations’ confidential or sensitive data must be appropriately protected while at rest and in transmit. Keys used for appropriate encryption adopted by organizations should be managed securely throughout its life cycle.

- **Browser Vulnerabilities**: Consumers access their applications or services offered by providers using secure communication through a web browser. Web browsers are a common target for malware and attacks. If the consumer’s browser becomes infected, the access to the services can be compromised as well.

### Cloud Security Standards

Following are some of the security standards/initiatives being developed by several consortia/organizations.

- **National Institute of Standards and Technology (NIST)**: NIST discusses the threats, technology risks, and safeguards surrounding public Cloud environments, and their suitable defense mechanisms. (NIST SP 800-57, and 144)

- **Cloud Security Alliance (CSA)**: The CSA alliance covers key issues and provides advice for both Cloud computing customers and providers within various strategic domains. (CSA guide version 3.0)

- **Distributed Management Task Force (DMTF)**: For security issues in Cloud computing, DMTF has established a
partnership with CSA to promote standards for Cloud security as part of DMTF Open Cloud Standard Incubator. The Open Cloud Standard Incubator group has designed a series of management protocols, packaging formats and security tools to foster interoperability between Cloud, followed by specifications that will foster Cloud service portability and cross-Cloud management consistency.

- **Storage Networking Industry Association (SNIA):** The Cloud Storage Technical Work Group under SNIA describes system implementation of Cloud storage technology.

- **Open Grid Forum (OGF):** The security group of OGF is concerned with technical and operational security issues in the grid and Cloud environments, including authentication, authorization, privacy, confidentiality, auditing, firewalls, trust establishment, policy establishment, and dynamics, scalability and management aspects of these issues.

- **Association for Retail Technology Standards (ARTS):** ARTS identifies the characteristics of Cloud computing that makes it compelling for retailers, and attempts to highlight areas in which a Cloud-based solution offers strong benefits to retailers. It also discusses the key obstacles to adopting Cloud-based solutions, including reliability, availability, and security.

- **Cloud Standards Customer Council (CSCC):** CSCC is an end user advocacy group dedicated to accelerating Cloud’s successful adoption, and drilling down into the standards, security and interoperability issues surrounding the transition to the Cloud. The council provides Cloud users with the opportunity to drive client requirements into standards development organizations and deliver materials such as best practices and use cases to assist other enterprises.

- **Organization for the Advancement of Structured Information Standards (OASIS):** OASIS sees Cloud computing as a natural extension of SOA and network management models. The OASIS Cloud Application Management for Platforms (CAMP) Technical committee advances an interoperable protocol that Cloud implementers can use to package and deploy their applications. CAMP defines interfaces for self-service provisioning, monitoring, and control. The OASIS Identity in the Cloud (IDCloud) technical committee works to address the serious security challenges posed by identity management in Cloud computing. Cloud Authorization (CloudAuth) technical committee will develop specifications and protocols to enable contextual attributes and entitlements to be delivered to policy enforcement points in real time.
Cloud Security Framework

There are several Cloud security standards and guidelines which describe the various aspects of security in the Cloud environment. While reviewing those security standards and guidelines, to the best of our knowledge there are no Cloud security best practices, and guidelines that meet the complete needs of Indian Banking and Financial Institutions. We have developed a set of guidelines and best practices describing IDRBT Cloud Security Framework as a practical, simple and easy to use guidebook that will help banks to understand and explore security concerns in the Cloud environment.

IDRBT Cloud Security Framework consists of security levels that are categorized into horizontal layers and vertical layers. These layers are described as follows.
Physical and Logical Security

Physical security provides awareness and protection of people security, and physical resources. Logical security techniques are used along with physical security to provide complete security to distributed business critical data and systems.

IT Infrastructure Security

IT Infrastructure security provides data protection concerns in networks, and virtual environments, and it also describes encryption and monitoring related issues.

Application and Process Security

Application and Processes security has become major concern while accessing an application from the Cloud. In a multi-tenant Cloud environment, this provides security to applications, and processes and to their patches and upgrades.

Data and Information Security

Data and Information security provides protection to unstructured and structured data from data privacy, data loss, data disposal, and unauthorized access according to the nature and business value of information.

Cloud Security Management

Organizational security describes governance, risk and control, legal issues, compliance, audit controls, roles and responsibilities that are needed prior to the Cloud deployment. Operational security describes awareness and training, identity and access control management, SLA and vendor management, business continuity and disaster recovery issues that are needed after the Cloud deployment to protect their assets, and to ensure security across the organization.

The guidelines provided in this document are not static and the security concerns of each level in the framework are still evolving. There is a need to review and update this document periodically by concerning forthcoming security issues in Cloud computing.

We have made an attempt to provide generic security guidelines, and best practices for Cloud providers and consumers to derive the benefit from Cloud computing. This work is expected to serve as a useful guide to Cloud security practitioners in the Banking and Financial Services Sector.
Chapter 3

Cloud Security Management

Governance, Risk and Control

Governance is the set of processes, technologies, policies and laws affecting the way an enterprise is directed, administered or controlled. Good governance is based on the acceptances of rights of shareholders, as the true owners of the bank, and the role of senior management as trustees. A criterion to select applications that can be deployed to Cloud provider must be in place. The criterion must bucket applications in at least one of the following categories.

- Low Risk
- High Information Risk (Sensitive Customer Information, Intellectual Property, Data Leakage can result in financial loss)
- High Regulatory Compliance Risk
- High Business Continuity Risk (Application Unavailability, Disaster Recovery Failure, Inflexibility to Future Needs)

The following four main factors must be considered in Cloud adoption decisions.

- Technical adequacy for porting the application to the Cloud – Assess the application profile to ensure it is a right fit to be ported to the Cloud.
- Cost Efficiency
- Risk including availability requirements, regulatory, compliance and statutory requirements, data sensitivity
- Control over intrusion decisions, vulnerability monitoring, denial of service attacks.

It is important that adequate procedures and SLAs are agreed between the provider and the service consumer. All necessary security metrics must be reported back to the service consumer by the Cloud service provider. Stakeholders should carefully consider the monitoring mechanism that is appropriate and necessary for the company's consistent performance and growth.

Enterprise risk management is rooted in the commitment by every organization to provide value for its stakeholders. Information risk management is the process of identifying and understanding exposure to risk and capability of managing it, aligned with the risk appetite and tolerance of the data owner. Hence, it is the primary means of decision support for IT resources dedicated to delivering the confidentiality, integrity, and availability of information assets.

- Each bank has to weigh these variables to decide whether the Cloud is an appropriate solution.
- Customers must assess the provider's supply chain to the extent possible which must also include third party management.
- Assessment of third party services provider should specifically target the provider's incident management, business continuity and disaster recovery policies, and processes and procedures and should include reviews of collocation and back-up facilities.
- Incident information can be specified in contracts, SLAs or other joint agreements. The level of attention and scrutiny should be connected to the value at risk.
Following are the Best Practices for Cloud Governance, Risk and Control.

- Reinvest the cost saving obtained by Cloud computing services into increased scrutiny of the security capabilities of the provider, application of security controls, and ongoing detailed assessments and audits to ensure requirements are continuously met.
- User organizations should include review of specific information security governance structure and processes, as well as specific security controls, as part of their due diligence for prospective organizations.
- Collaborative governance structure and processes between customer and provider should be identified as necessary, both as part of the design and development of service delivery, and as service risk assessment and risk management protocols, and then incorporated into service agreements.
- Security department should be engaged during the establishment of Service level agreements (SLAs) and contractual obligations to ensure that security requirements are contractually enforceable.
- Metrics and standards for measuring performance and effectiveness of information security management should be established prior to moving into the cloud. At a minimum, organizations should understand and document their current metrics and how they will change when operations are moved into the Cloud and where a provider may use different metrics.
- Due to the on-demand provisioning and multi-tenant aspects of Cloud computing, traditional forms of audit and assessment may not be available or may be modified.
- If the services provided in the Cloud are essential to corporate operations, a risk management approach should include identification and valuation of assets, identification and analysis of threats and vulnerabilities and their potential impact on assets, analysis of the likelihood of events, approved risk acceptance levels and criteria, and the development of risk treatment plans with multiple options.
- Risk assessment approaches between provider and user should be consistent within impact analysis criteria and definition of likelihood.
- Due to the evolving nature of Cloud and its providers, care should be taken to include vendor risk.
- Asset inventories should account for assets supporting Cloud services and under the control of the provider. Asset classification and valuation schemes should be consistent between user and provider.
- The service, and not just the vendor, should be the subject of risk assessment. The user of Cloud services and the particular service and deployment models to be utilized should be consistent with the risk management objectives of the organization, as well as with its business objectives.
- Cloud service customer and provider should develop robust information security governance, regardless of the service or deployment model. Governance should include periodic review, and the service model may adjust the defined roles and responsibilities in collaborative information security governance and risk management, while the deployment model may define accountability and expectations.
- Customers of Cloud services should ask whether their own management has defined risk tolerances with respect to Cloud services and accepted any residual risk of utilizing Cloud services.
- Where a provider cannot demonstrate comprehensive and effective risk management processes in association with its services, customer should carefully evaluate use of the vendor as well as the user’s own abilities to compensate for the potential risk management gaps.
- The organization should define risk metrics for engaging providers based on business and technical exposures.
## 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.

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Controls</th>
</tr>
</thead>
</table>
| **Adherence to Laws** | - The CSP (Cloud service provider) has to comply with the law of the country where his Cloud is hosted and the customers / participating organizations are bound by the law of the country wherein they operate.  
- There is no law with regard to Cloud service providers, but the various laws like Information Technology Act, Data Privacy Act, Data Retention Directive, E-Privacy Directive, E-Commerce Directive, The Computer Fraud and Abuse Act 1984, Digital Millennium Copyright Act 1988 will be applicable to Cloud service providers and also the customers of the Cloud service. |
| **Service Level Agreement** | - It is always preferable to use the CSP who has datacenter within the country where the customer conducts business. Here both the service provider and customers will be bound by the same set of laws.  
- As there is no specific law governing the CSP, the contractual agreement should incorporate all the legal requirements for data protection.  
- There is no general legal requirement for a vendor to provide customers with the data export facilities. This shall be covered in the contractual agreement.  
- Many CSP in their contracts limit liability of hosting provider to a level that is not in line with potential risk. This point has to be borne in mind while availing Cloud service.  
- In many Jurisdictions, CSP can be held liable for the illegal data they may be hosting. |
| **Data Security** | - Contracts are likely to promise to provide only “reasonable” security for customer data, or perhaps to adhere to “industry standard” security practices. While such promises sound good in the abstract, they are open to considerable interpretation and argument.  
- It is preferable to specify an actual, specific, independent security standard and require that it be updated, and perhaps audited, regularly. In addition, for certain kinds of data, there may be specific security requirements that must be included in any CSP contracts. Ideally, the contract should also provide for regular SAS 70, Type II audits, with customer access to the results. |
<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>The contract should require the CSP to give the customer, notice of any security/data breaches, and, to the extent that user notification is legally required, such notice should preferably be in advance of user notification (which should be the vendor’s responsibility).</td>
<td></td>
</tr>
<tr>
<td>The contract should clearly state that all data are owned by the customer and contain a provision that, at the termination of the contract, the provider should agree to deliver a copy of client data and permanently destroy all copies of the data in its possession.</td>
<td></td>
</tr>
</tbody>
</table>

**Access to Data for Purposes of Discovery**

- Although the contract probably will not (and probably need not) expressly address the issue, it is important to understand—ahead of time—the architecture of the CSP’s system, how and in what format it keeps customer data, and what tools are available to customer to access his data so that customers will be ready for any e-discovery needs that may arise.

**Location of Data**

- Some vendor form contracts expressly reserve the right to store customer data in any country in which they do business. Others may not address the issue, but the CSP may follow similar practices nevertheless, on the (generally legitimate) theory that what is not expressly prohibited is thereby permitted. While dispersed geographical storage is beneficial from a data protection and backup perspective, it can raise export control (EAR/ITAR) issues in the context of research data. If that is important to the user organization, it should include language prohibiting “extra-territorial” storage.

**Unauthorized or Inappropriate Use**

- Contracts may attempt to make the customer responsible for affirmatively preventing any “unauthorized” or “inappropriate” use of the vendor’s service by others, or perhaps to use “best efforts” or “commercially reasonable efforts” to do so. Given that these services are “in the Cloud” and therefore largely outside customer control, it is preferable to provide only that customer will not “authorize” or “knowingly allow” such uses.
- Some contracts also may require customer to notify the vendor of “all” unauthorized or inappropriate uses of which he become aware. Particularly with respect to vendors with broadly stated AUPs (Acceptable Use Policy) or terms of service, such expansive obligations seem burdensome and unnecessary. It is preferable to replace “all” with “material” or some similar, higher threshold.

**Emergency Security Issues**

- CSP understandably may wish to have the right to “immediately” suspend an “offending use,” and possibly the service altogether, in the event of an “emergency” issue. However, the standard for what constitutes an emergency should be clearly defined, should not give the vendor much if any discretion or flexibility in its application, and, preferably, should incorporate a “materiality” or similar threshold.
<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ownership of Data</strong></td>
<td>✦ The contract should expressly make clear that all data belongs to the customer/organization (and/or its users) and that the vendor acquires no rights or licenses, including without limitation intellectual property rights or licenses, to use the data for its own purposes by virtue of the transaction. It also may be useful to provide that the vendor does not acquire and may not claim any security interest in customer data.</td>
</tr>
<tr>
<td><strong>Disclaimer of Warranty</strong></td>
<td>✦ Contracts typically disclaim essentially all warranties, including any warranty that the CSP’s service does not infringe third-party intellectual property rights.</td>
</tr>
<tr>
<td><strong>Indemnification by Customer</strong></td>
<td>✦ Some CSP contracts require the customer to indemnify the vendor not only for his own actions (which is not necessarily unreasonable), but also those of his end users. Nevertheless, it is preferable not to voluntarily accept that liability, which is also no different than the vendor’s liability for any other, non-institutional end users.</td>
</tr>
<tr>
<td><strong>Indemnification by Vendor</strong></td>
<td>✦ Contracts rarely include any form of indemnification benefitting Customers, but such protection is critical in at least two areas: infringement of third-party intellectual property rights and inappropriate disclosure or data breach, both of which are largely, if not entirely, in the vendor’s sole control, and both of which can be extremely costly to defend and remedy. Ideally, the vendor would indemnify the customer for all of its acts and omissions.</td>
</tr>
<tr>
<td><strong>Governing Law and Jurisdiction</strong></td>
<td>✦ A CSP’s contract will specify that it is governed by the law of the vendor’s home state and grant the courts of that state exclusive jurisdiction over any disputes arising out of the contract. It is preferable to either (a) specify the law and jurisdiction of Customer state (large vendors likely operate in and are subject to all such jurisdictions, so it is no significant inconvenience for them), (b) provide that disputes must be brought in the defendant’s jurisdiction (which is even-handed and tends to encourage informal resolution, as the plaintiff won’t have the “home court” advantage), or (c) simply delete the provision and leave the question open for later argument and resolution if and when needed.</td>
</tr>
</tbody>
</table>
| **Confidentiality** | In cases where the CSP is obtaining access to particularly sensitive information, the level of protection will need to be significantly stronger. The organization should consider in an agreement:  
  ✦ The replication of any obligations placed upon the organization by contract or law.  
  ✦ For non-sensitive data, requirements to ensure the CSP are aware of the level of confidentiality required and commits to protecting that data appropriately.  
  ✦ For sensitive data, more detailed confidentiality obligations are required. In some cases where an extra layer of protection is necessary, it may be appropriate to |
Organizations going for Cloud should consider including the following rights in any agreement:

- Restricting the locations/countries in which organization data may be held (with movement to new locations permitted with advance approval in writing from the organization).
- Rights to audit the CSP’s compliance with the agreement including rights of access to the provider's premises where relevant records and organization data is being held.
- Audit rights for the organization (or its nominee)
- A right for the organization to appoint a commercial auditor as its nominee (as this allows the organization to appoint an auditor in the same location as the CSP’s data center to save costs and ensure compliance with relevant jurisdictional laws).
- Where technically available, the right for the agency to remotely monitor access to its data and where this is not possible, a requirement that the provider maintain an audit log of access to the agency's data and provide that log to the agency on request.

Service levels are an important way of ensuring that a provider meets the level of service expected by the Organization. This is particularly important where the Cloud computing service is critical either to the functioning of an organization or to the organization’s clients.

Compliance and Audit

Compliance

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.

<table>
<thead>
<tr>
<th>Clause</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT (Amendment) Act 2008</td>
<td>IT (Amendment) Act 2008 has specified “reasonable security practices and procedures” to protect “sensitive personal data or information” (SPDI). It is mandatory to identify the SPDI processed or stored by the CSP and ensure all the processes are compliant with IT (Amendment) Act 2008.</td>
</tr>
<tr>
<td>Companies Act, 1956</td>
<td>Most, if not all, banks are companies under the Companies Act. This act requires various disclosures, filing and record keeping obligations to be fulfilled. When the data and reports that are needed for complying with such obligations are on the “Cloud” extra care has to be taken to ensure compliance as regards availability, verifiability, authenticity, amenability to inspect, audit and review.</td>
</tr>
<tr>
<td>Personnel Laws</td>
<td>Various personnel laws like the Payment of Wages Act, the ESI Act, Provident Funds Act etc. require various disclosures, filing and record keeping obligations to be fulfilled.</td>
</tr>
<tr>
<td>Negotiable Instruments Act, 1881</td>
<td>Banks deal with cheques, promissory notes and bills of exchange. These are now not covered under the IT Act. But it is worth examining whether the use of the “Cloud” will have any implications relating to these Acts.</td>
</tr>
<tr>
<td>Prevention of Money Laundering Act, 2002</td>
<td>Illicit money dealings and money laundering often depend on the Internet. Electronic transfers, storage and record of financial transactions have added velocity, volume and complexity to the tasks of ensuring compliance and reviewing compliance. This is aggravated by the use of the “Cloud”. Hence, extra care has to be taken to ensure compliance as regards availability, verifiability, authenticity, amenability to inspect, audit and review</td>
</tr>
<tr>
<td>Limitation Act, 1963</td>
<td>Bank recovery cases are subject to the Limitation Act (or perhaps to special laws of Debt Recovery). The use of Cloud for storage of data may have some implications in this respect since retrieval of key data needed for recovery proceedings may need exceptions to typical data retention policies.</td>
</tr>
<tr>
<td>Data Privacy Law</td>
<td>A full-fledged Indian data privacy law is expected any time. It will be mandatory to protect the data privacy as per this law.</td>
</tr>
</tbody>
</table>
Audit and Assurance

Assurance is defined as an objective examination of evidence for the purpose of providing an assessment of risk management control or governance processes for the organization. The Cloud computing audit/assurance review will:

- Provide stakeholders with an assessment of the effectiveness of the Cloud computing service provider’s internal controls and security
- Identify internal control deficiencies within the customer organization and its interface with the service provider
- Provider audit stakeholders with an assessment of the quality of and their ability to rely on the service provider's attestations regarding internal controls

<table>
<thead>
<tr>
<th>Clause</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| **Provide Assurance against the selected Common Certification Assurance Framework** | ➤ A common certification assurance framework for IT governance and security controls (e.g. ISO 27001 or COBIT 5) should be agreed by CSP and the client.  
➤ Periodic audit should be performed by an approved external auditor against the selected framework as per the agreed scope document.  
➤ The Cloud consumer should be allowed to participate in the external audit |
| **Process Assessment** | If COBIT 5 is the agreed framework, it is desirable that the CSP achieves at least Level 3 of process capability levels under the COBIT 5 Process Assessment Model based on ISO 15504-2 for managing service agreements, risk, security, continuity and compliance. |

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 be defined and documented in accordance with the Cloud providers and Cloud consumers 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.
Figure 3.1 shows how control is typically shared between a provider and a consumer across different service models.

![Figure 3.1 Level of Control/Responsibility for consumer and provider across different service models](image)

The following roles and responsibilities must be formally defined in an organization's information security policy framework and approved by senior management:

- Segregation of duties requires at least two persons with separate job responsibilities to complete a transaction or process end-to-end. It is suggested to separate the Cloud software development team from Cloud software operational or maintenance team.
- Avoidance of conflict of interest is essential to the protection of Cloud consumers.
- Ensure that different personnel manage different critical infrastructure components.

**Business Continuity and Disaster Recovery**

**Business continuity**

Business continuity deals with the continuity component of information security confidentiality, integrity and availability.

Following are the best practices for business continuity:

- Banks should review the contract of third party to maintain the business continuity. Appropriate regulatory controls must be taken especially when there is sensitive data handled over the Cloud. Even these requirements must be applied during third party data processing.
- Banks should review the third party for certification. On-site assessment must be conducted to confirm and verify the asserted controls used to maintain the continuity of the services.
- The banks should ensure for the confirmation of any business continuity/disaster recovery test undertaken by a CSP. Banks must stress the importance of getting formal verification of business continuity/disaster recovery tests.
Disaster Recovery

A fully virtualized storage infrastructure, a scalable file system and a compelling self-service disaster recovery application that responds to the customers’ urgent business requirements are the foundational fundamentals to build Cloud disaster recovery solutions.

Following are the best practices for disaster recovery.

- IaaS providers should have contractual agreements with multiple platform providers and have the tools in place for rapid restore system in the event of loss.
- Disaster recovery drills should be conducted regularly.
- Hypervisor must have different continuity/disaster recovery.
- Data validation should be an automated or user intended validation protocol.
- Full site, system, disk and file recovery should be accessible.
- The CSP should provide the fast SLA-based data recovery.
- The SLA should be negotiated up front, and the customer should pay for the SLA required to ensure that there is no conflict of interest.
- WAN optimization between the customer and the physical site should be in place so that the Cloud enables full data mobility at a reduced bandwidth, storage utilization and cost.

SLA and Vendor Management

It is essential to ensure clear definition, monitoring and governance of service level objectives, between Cloud Service Providers and the consumers (i.e. Banks). Cloud Service Providers should deliver a guaranteed level of service that are essential for smooth functioning of the business (based on references 17 & 18).

<table>
<thead>
<tr>
<th>SLA Terms</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Data Level Policies** | ✦ Policies and procedures related to data retention, preservation, location, security and privacy needs to be framed.  
✦ Many of the standards / recommendations for data classification and data privacy and retention would need to be included in the data level SLA policies.  
✦ Policies should also include other legal and regulatory requirements.  
✦ Policies should be defined considering the service model and deployment model.  
✦ Policies should include compliance with security standards and regulations. |
| **Guarantees** | ✦ SLA policies must be comprehensive, objective and measurable, along with penalty matrix and the escalation in the event of non-delivery of the agreed guarantees.  
✦ SLA metrics should include performance metrics like network performance, application uptime, application response time, etc. |
| **Service Usage** | ✦ Policies should cover details of services that are covered / not covered and the conditions therein. This would include the acceptable usage policy expected from the Cloud provider point of view. |
Cloud Security Framework for Indian Banking Sector

Penalty and Payment Modes
In the event of breach of service delivery by the Cloud provider or excess usage by service consumer, modes and conditions of payment must be formed.

SLA Lifecycle Management
Policies around governance and versioning of SLA terms should be framed.

Support and Maintenance Policies
Policies for support and planned maintenance should be framed.

Licensed Software
Policies around procurement and maintenance of software license should be planned. This would include version update / patch update.

Certification and Audit
Policies should cover bodies designated for certification and audit of SLA.
Policies should include necessary certification and compliance framework.

Identity and Access Management
Validating the state of identity and access management is fundamental to the protection of data and availability. Two types of identity and access management need to be covered.

- **CSP Identities**: These tie back to administrators and CSP staff and resources that have access to the system, VM, and infrastructure components.
- **Consumer Identities**: These are user accounts associated with the application that the SaaS is hosting for their various tenants.

Identity and Access Management for CSP
The following are the different levels of access management for different Cloud service delivery models.

<table>
<thead>
<tr>
<th>SLA Terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Activation</td>
<td>Policies around the time for service activation / policy enforcement are needed</td>
</tr>
<tr>
<td>Penalty and Payment Modes</td>
<td>In the event of breach of service delivery by the Cloud provider or excess usage by service consumer, modes and conditions of payment must be formed</td>
</tr>
<tr>
<td>SLA Lifecycle Management</td>
<td>Policies around governance and versioning of SLA terms should be framed</td>
</tr>
<tr>
<td>Support and Maintenance Policies</td>
<td>Policies for support and planned maintenance should be framed</td>
</tr>
<tr>
<td>Licensed Software</td>
<td>Policies around procurement and maintenance of software license should be planned. This would include version update / patch update</td>
</tr>
<tr>
<td>Certification and Audit</td>
<td>Policies should cover bodies designated for certification and audit of SLA. Policies should include necessary certification and compliance framework.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SLA Terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity and Access Management</strong></td>
<td>Validating the state of identity and access management is fundamental to the protection of data and availability. Two types of identity and access management need to be covered.</td>
</tr>
<tr>
<td><strong>CSP Identities</strong></td>
<td>These tie back to administrators and CSP staff and resources that have access to the system, VM, and infrastructure components.</td>
</tr>
<tr>
<td><strong>Consumer Identities</strong></td>
<td>These are user accounts associated with the application that the SaaS is hosting for their various tenants.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to physical data center</td>
<td>Access to physical data center</td>
<td>Access to physical data center</td>
</tr>
<tr>
<td>Access to data center operations suite of tools</td>
<td>Access to data center operations suite of tools</td>
<td>Access to data center operations suite of tools</td>
</tr>
<tr>
<td>Console access to servers, SAN, security tools, and network devices</td>
<td>Console access to servers, SAN, security tools, and network devices</td>
<td>Console access to servers, SAN, security tools, and network devices</td>
</tr>
<tr>
<td>Administration access to the virtualization and orchestration technologies</td>
<td>Administration access to the virtualization and orchestration technologies</td>
<td>Administration access to the virtualization and orchestration technologies</td>
</tr>
<tr>
<td>Access to development platform, including code repository</td>
<td>Access to development platform, including code repository</td>
<td>Access to development platform, including code repository</td>
</tr>
<tr>
<td>Administrative access to presentation layer</td>
<td>Administrative access to presentation layer</td>
<td>Administrative access to presentation layer</td>
</tr>
<tr>
<td>Administrative access to middleware</td>
<td>Administrative access to middleware</td>
<td>Administrative access to middleware</td>
</tr>
<tr>
<td>Administrative access to database layer</td>
<td>Administrative access to database layer</td>
<td>Administrative access to database layer</td>
</tr>
<tr>
<td>Administrative access to application layer</td>
<td>Administrative access to application layer</td>
<td>Administrative access to application layer</td>
</tr>
</tbody>
</table>
Consumer need to ask how the CSP provisions contractors, consultants, outsourcers, offshore resources, auditors, business partners, and essentially anyone that could obtain access to its network, system, database, and application. To add to that complexity, consumer may also have to address the issues of authentication and authorization for inter application connections and Cloud services.

**Identity and Access Management for Consumer**

Identity management for consumer can be loosely categorized into two general areas:

- **Task Workers**: Users in an organization that consume the services, whether application, platform, or computer services.
- **Administrative Access**: Users in an organization that are given an administrative console to assign right and manage users, procure or discontinue Cloud services, monitor usage and operational metrics, etc.

Adoption models for identity management for Cloud services can be done in three modes:

- **Local User Repository**: Account is hosted and stored on directory services and are typically managed by consumer via a consumer administrative console provided by the CSP.
- **Integration with Consumer Enterprise User Repository**: The Cloud provider has the ability to integrate back into consumer enterprise directory to facilitate single sign-on.
- **Federated Identity through Cloud Identity Brokers**: Cloud identity brokers build integration tools to act as the channel between various Cloud providers and consumer enterprise directory.

**Awareness**

All stakeholders (employees, contract staff, third party service providers, vendors) should be aware of organizational information security policies, procedures, guidelines, threats, their roles, responsibilities, knowledge, skill and liabilities and be ready to support and abide by them to reduce the risk of human error.

- The organization shall ensure that all personnel who are assigned responsibilities defined in the information security management system are competent to perform the required tasks by:
  - Determining the necessary competencies for personnel performing work affecting the information security management system (ISMS).
  - Providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs.
  - Evaluating the effectiveness of the actions taken and
  - Maintaining records of education, training, skills, experience and qualifications.

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS and Cloud security objectives.
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.

**Data Discovery**

Data Discovery is the process of identifying all the data repositories in an organization and analyzing the schema, data values and data patterns identify relationships between the database elements.

- Data Discovery looks at data relationships across repositories, understands how they relate to each other, and understands how the structured relationships are organized to represent business objects.
- Data Discovery detects transformations and conditional logic that has been applied to data as it has been moved among repositories.

**Data Classification**

Data classification and the management of data according to its classification will vary from organization to organization. A defined data-classification system can help organizations identify data that is sensitive or confidential, and data with specific security needs. This allows organizations to assign appropriate protection mechanisms based on the security needs of different data types, and helps to prevent sensitive data from being inadvertently mishandled or treated as non-sensitive.

- Organizations should ensure that their particular data security needs can be met by the Cloud service before migrating that data into the Cloud environment.
- Considerations should include how storing data types with different levels of sensitivity in the same virtual environment may impact the protection levels required for each data type.

**Data Migration**

Adequate controls shall be implemented to ensure data integrity and confidentiality during/after data migration and its completeness shall be verified. Data shall be protected and its integrity shall be maintained while it is being migrated.

- Access controls shall be implemented to ensure that data is not altered manually or electronically by a person or program.
- The file/record in the new application shall be consistent with that of the original application.
- The new application shall continue with newer records as an addition and help in ensuring seamless business continuity.
- The last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform shall be maintained separately for any future reference.
- The error logs pertaining to the pre-migration, migration and post migration period shall be available.
- The complete transaction data and audit trails from the old system to the new system shall be migrated.

**Data Privacy**

Data privacy shall be maintained for all the business critical data while at rest as well as during transit. Adequate controls shall be implemented to ensure data privacy.

- There shall be proper access control to view and download the data by authorized users.
There shall be a mechanism to ensure that only data items relevant to the business requirement be viewed and accessed.

There shall be a mechanism to ensure that critical data is tokenized / encrypted to protect it even from authorized users.

Bank’s employees shall sign an undertaking regarding data secrecy and privacy.

The data shall be anonymised before it is made available for use in the test or development environment.

There shall be an enterprise wide “Data privacy policy” addressing privacy in the data collection, use, processing etc.

**Data Assurance**

Data assurance refers to methods and activities to make sure that data is cleansed and standardized to a defined model before it is used.

- Data assurance also tracks the origin of the data when it is received through logging and auditing capabilities.
- Data assurance processes also provide a governance checkpoint for aggregation, redaction, and obfuscation requirements to ensure confidentiality and privacy.

**Data Redaction**

Data redaction refers to a set of methods for eliminating sensitive or confidential data from a data set based on policy rules before it is given to a receiver.

- Data can be partially aggregated in ways that make it impossible to determine individual data records. In certain techniques, errors can be deliberately introduced into data in ways that preserve confidentiality while preserving the ability to perform statistically valid operations on the data.
- Data Redaction techniques enforce access control security policies while enabling the release of related and relevant data.

**Data Retention**

Data retention capabilities cover both backup and archive mechanisms and processes. Backup refers to the mechanisms/process and activities needed to restore service to a well-known point in the event of system or media failure. Archiving refers to tools and processes to remove transactions from an active system that is no longer needed, but that might need to be preserved for legal requirements.

Data Retention tools and techniques are part of a records management system that decides about what must be kept and in certain cases what must be deleted according to policy.

**Data Disposal**

Data disposal refers to the tools and processes to delete data from a system that is no longer needed and required by law or policy to be retained. Disposing of data that is no longer needed reduces data management costs.

- Data Disposal processes can create a security risk if they inadvertently leave a way for the disposed data to be retrieved.
- Data Disposal tools and processes have to be designed to prevent likely threats to recovering the data, based on the value and sensitivity of the data and the techniques that an attacker might employ to retrieve the disposed data.
- Data Disposal processes must also preserve sufficient records to show that the disposal processes have been followed.
- The CSP should provide data-disposal mechanisms that provide assurance to the client that all data has been securely removed and deleted from the Cloud environment. Procedures for “termination of service” should be clearly defined and documented.
Best Practices for Cloud Data and Information Security

- Understand how integrity is maintained and compromise of integrity is detected and reported to the concerned. The same recommendation applies to confidentiality when appropriate.

- The Cloud service provider must assure the Bank that they provide full disclosure (aka ‘transparency’) regarding security practices and procedures as stated in their SLAs, if a public Cloud.

- Ensure specific identification of all controls used during the data lifecycle.

- Maintain a fundamental philosophy of knowing where your data is. Ensure your ability to know the geographical location of storage. Stipulate this in your SLAs and contracts. Ensure that appropriate controls regarding country location restrictions are defined and enforced.

- It is the Bank’s responsibility to determine who should access the data, what their rights and privileges are, and under what conditions these access rights are provided. The Bank should maintain a “Default Deny All” policy.

- The Bank’s responsibility is to define and identify the data classification. It is the Cloud service provider’s responsibility to enforce the Bank’s access requirements based on data classification. Such responsibilities should be in the contract and enforced and audited for compliance.

- Encrypt data at rest and encrypt data in transit.

- Identify trust boundaries throughout the IT architecture and abstraction layers. Ensure subsystems only span trust boundaries as needed and with appropriate safeguards to prevent unauthorized disclosure, alteration, or destruction of data.

- Understand what compartmentalization techniques are employed by the Cloud Service provider to isolate its customers from one another.

- Understand the Cloud provider’s data search capabilities and limitations when attempting to view ‘inside’ the dataset for data discovery.

- Understand how encryption is managed on multi-tenant storage.

- Data retention and destruction schedules are the responsibility of the Bank. It is the Cloud service provider’s responsibility to destroy the data upon request, with special emphasis on destroying all data in all locations including slack in data structures and on the media. The Bank should enforce and audit this practice if possible.

- Understand the logical segregation of information and protective controls implemented.

- Understand Cloud provider policies and processes for data retention and destruction and how they compare with internal organizational policy. Be aware that data retention assurance may be easier for the Cloud provider to demonstrate, while data destruction may be very difficult.

- Perform regular backup and recovery tests to assure that logical segregation and controls are effective.

- Ensure that Cloud provider personnel controls are in place to provide a logical segregation of duties.
BEFORE we discuss application and process related security aspects of Cloud, let us look at the following examples of how Cloud consumers could potentially use various service models to access applications on the Cloud.

**Infrastructure as a Service (IaaS):** This will be typically used by banks to augment their processing capacity at a short notice e.g.
- A bank might like to leverage additional machines for development and testing. The bank could simulate a new product or a process in a test environment before rolling it out into production.
- A bank could use additional machines on the Cloud for validation of sizing before ordering machines for production.
- A bank could use additional machines to augment their production capacity e.g. bank could run interest calculation or other CPU intensive algorithms on the Cloud while keeping customer or account data within the bank’s data center itself.

**Platform as a Service (PaaS):** This will be typically used by the consumers for application development e.g.
- The bank may want to develop be-spoke applications while being spared of the overhead of installing and maintaining a complex development environment like application servers, process server, etc.
- The bank may use core banking or other application of similar complexity from an application vendor as a platform to develop surround applications or reports and so on.
- The bank may use a database on the Cloud for their development.

**Software as a Service (SaaS):** Cloud provider may provide ready to use applications on the Cloud taking care of various aspects of application development (or sourcing from external vendor), deployment, maintenance, monitoring and business continuity. This makes sense especially for smaller banks which may find it expensive to maintain a state-of-the-art data center, applications and infrastructure on their own for. Few examples are as follows:
- Cloud provider could provide a comprehensive solution suite including core banking and channels on the Cloud. This would typically be a private or community Cloud setup by the Cloud provider for banks which sign up for such a service. Various branches will be typically connected to the provider’s data center using a dedicated network though Internet could also be an option.
- Cloud provider could provide a channel e.g. Internet or mobile banking which will connect to a bank’s core system typically through the leased line or through the Internet.
- A Cloud provider could provide ATM switch on the Cloud offered to banks which sign up for this service. This could connect to ATM and POS machines, which could belong to the Cloud provider, any of the banks participating in this service or to another organization. The ATM switch itself could be connected to each of the participating bank’s core system again typically through the leased line or through the Internet.

**Application Access Mechanisms**

There are two possible mechanisms in which Cloud provider would offer service to Cloud consumers. In case of public
Cloud, Cloud consumers would be expected to be connected to the Cloud provider using Internet. This scenario is as shown in Fig 5.1.

Cloud consumers could access applications on the Cloud using HTTPS for browser based applications. They could also use machines on the Cloud using SSH based tunneling for services like Telnet or secure file transfer or X forwarding.

We do not expect HTTP or Telnet or FTP ports to be opened from the server side. Alternately VPN can be set up for each consumer, which can allow branches to access the bank’s servers within data center using a variety of protocols.

This mode will be used to access public Clouds and will be the default mechanism provided for various forms of Cloud deployment i.e. Infrastructure as a service, Platform as a service or Software as a service.

As an alternate to using a public network for accessing applications over Cloud, Cloud provider can set up its own private network which can allow connecting various branches to the provider’s data center (see Fig 5.2). Using technologies like MPLS, each bank can effectively have its own private LAN. This arrangement makes sense when the Cloud provider is offering a private (or community) Cloud to banks that enroll for the services provided by the Cloud provider. This would be more relevant when transactional applications accessing customer data are hosted in the Cloud in Software as a Service kind of deployment as described in the previous section.

While it is possible to use a secure tunnel for application access over the Internet as described above, scenario 2 is more secure since it does not pass through a public network.
Multi-Tenancy and Implication on Security

One of the basic principles of Cloud computing is “shared infrastructure”, which is achieved through multi-tenancy. There are several mechanisms to achieve multi-tenancy and these lead to different considerations for data privacy etc. We analyze the two most commonly followed approaches for multi-tenancy.

Multi-tenancy through Virtualization

In this case, banks share large physical servers which are separated into multiple virtual machines (VMs) using one or more virtualization products. Since each bank’s programs and data lie on separate virtual machines, there is already a clear separation of data between various banks. This mechanism also allows for the kind of elasticity that is required for movement of resources from one VM to another based on the increased load.

Few important considerations for virtualization are as follows:

- Application should be explicitly tested and qualified using virtualization product that is deployed within the Cloud. Application vendor needs to provide sizing considering deployment under virtualized environment. Alternatively vendor could provide sizing based on physical servers and state the overhead with specific virtualization product. Application image should be available for the virtualization product used and this image can be used for quick initial deployment of the application for a new bank.

- Each virtual machine needs to be allocated resources (actually a range) commensurate with projected transaction load for the bank. Resource consumption needs to be periodically monitored against actual load so that necessary refinements can be carried out.

- Infrastructure vendor needs to officially support the deployment of their software under virtualized environment that will be used on the Cloud.

- The Cloud provider needs to follow specific guidelines stated by virtualization vendor e.g. many virtualization vendors do not recommend CPU or memory over commit beyond the physical capacity of the server in a production system.

- For mission critical applications, provider needs to create (at least) two sets of virtual machines for all the tiers on separate physical boxes to provide resilience. For illustration purposes, Fig. 5.3 provides a sample scenario 3.

- Putting different tiers of the application onto separate physical boxes can allow passing communication between tiers to go through physical network and facilitate implementation of firewall policies to allow communication only between VMs belonging to the same bank. Also, using different disk partitions to isolate VMs belonging to different banks can provide further isolation.

- Monetary agency in a country could impose regulatory requirements to place customer data in that country. That would necessitate setting up data centers in countries where such restrictions apply. In such cases, we would expect that all tiers of the application for a bank are placed together, considering the latency that could get induced when these tiers are geographically separated.

- A variant of this deployment scenario could be to run multiple database instances on the same machine limiting resource consumption by each instance e.g. instance caging in case of Oracle.

- There can be other variants as well e.g. we could bring up multiple web server instances on different ports, one for each bank, in which case URL for each bank will differ, based on the port number. Similarly, multiple application server instances could be brought up on the same machine to listen on different ports. Web or application server
Multi-tenancy provided by Application

Some applications are capable of providing native multi-tenancy features. This means that the application uses a single database which is essentially partitioned by application itself by having “Bank Id” field within all tables that carry bank specific data. Also, all application processes (or threads) would be able to set context to a specific bank before they commence processing of requests for that bank. The application itself would provide the capability to add a new bank. Since the entire infrastructure is shared between banks, concerns related to data privacy need to be explicitly certified by the application vendor.

- The key to this approach is a high amount of standardization e.g. all banks naturally share the same infrastructure and application software versions. Cloud provider could maintain technical parameters like IP addresses or port numbers and reference information like country codes, currency codes, error messages or market feeds for all banks. On the other hand, Cloud provider could allow individual banks to have their own business processes, chart of accounts, product definitions, user roles, user interfaces based in languages as required by their users, time zones to which their branches belong and so on. The Cloud provider needs to explicitly publish what is standard across all Cloud consumers and what is variable.

- Through the application, no user should be able to view or access data beyond the bank to which that user belongs.

- Bank user may need an access to specific data for reporting, etc. For this purpose, database views or synonyms specific to each bank needs to be created. The user should be able to access only the data specific to the bank to
which she belongs. Using these views, it should be possible to extract data belonging to any specific bank at a short notice.

- File system based business reports or logs belonging to different banks need to be in separate directories. No user should be able to see the data beyond the bank to which that user belongs.

- Since the entire infrastructure is shared by multiple banks, an application needs to have the necessary checks in place to ensure that “runaway” processes are detected and brought down; transactions that take more time than a certain threshold are aborted; time consuming database queries are regularly detected and optimized and so on.

The Cloud provider needs to specifically address these aspects for native multi-tenancy provided by the application. Fig. 5.4 shows multi-tenancy implementation through application.

Figure 5.4 Sample application deployment having J2EE, App and DB tiers

Please note that the above considerations would apply to Software as a Service and specifically to applications which natively support multi-tenancy. These do not apply to Infrastructure as a Service which uses hardware or OS level virtualization for multi-tenancy. These would also not apply to Platform as a Service since that model would use hardware or OS level virtualization or the variants for virtualization that have been described in the previous section.

**Access Rights for Cloud Provider**

Responsibilities of Cloud provider and access rights required to discharge these responsibilities vary based on the deployment model i.e. Infrastructure as a Service, Platform as a Service or Software as a Service. For the purpose of this discussion, we will assume that we are using virtualization to achieve multi-tenancy, though most considerations would apply even otherwise. Given below is a list of representative activities that would be expected to be performed by a Cloud provider for various deployment models. We expect a detailed list to be contractually agreed between Cloud provider and Cloud consumer. Employees of the Cloud provider may also need to sign appropriate legal agreement in case they are given access to virtual machines that belong to the Cloud consumers.

**Software as a Service**

In this case, Cloud provider takes the responsibility of providing ready to use business services to consumers by operating
the hosted application on a day-to-day basis. Hence, Cloud provider may need minimal user and application level access to consumers’ virtual machines to perform various functions. We recommend usage of tools or automated scripts from application and infrastructure vendors for most of the functions listed below.

- Deployment of infrastructure and application components i.e. virtual machine, OS, database, application server and application
- Configuration of infrastructure and application components, where application configuration pertains to setting technical parameters like port numbers, IP addresses, directory paths, debug log level etc.
- Applying OS, database, application server and application patches or performing upgrades
- Starting or stopping the virtual machine, database, application server and application
- Monitoring performance to identify bottlenecks, some of which we have listed below.
  - Expensive database operations
  - Slow use-cases from web server logs
  - Batch processes taking longer than expected
  - Increase in process/heap memory, file or socket handles due to leaks
  - Excessive logging from application
  - Poorly performing network interfaces to external applications
  - Runaway processes consuming high CPU
  - Excessive CPU, memory, disk I/O at virtual machine level
- Troubleshooting at various levels which includes looking at OS, database, application server and application error logs (technical errors)
- Taking remedial actions for trouble shooting or performance bottlenecks like:
  - Temporarily shutting down application or infrastructure components having issues
  - Reconfiguration of application or infrastructure components e.g. reduction of log level
  - Archival and purging of old log files to release disk space
  - Database reorganization
  - Archival and purging of database tables
  - Bringing down runaway processes
  - Taking thread or heap dumps for Java based application servers
  - Temporarily disabling functions (e.g. menu options) with known issues
  - Sending error logs to application or infrastructure vendor for further troubleshooting
- Taking a verified backup of the database and restoration if required (Please note that if the application being hosted involves transactions with customer data, database files and backup should be encrypted and only authorized bank user / application should be able to decrypt the data).
- Performing other application related activities as agreed with the Cloud consumer e.g. running end-of-day or beginning-of-day batch jobs, uploading files for processing, etc. These jobs should not require access to data
pertaining to customers, accounts, transactions, banking products, users and other important business information. These activities would be application specific e.g. in case Cloud provider is hosting an ATM switch, it could mean activities like reconciliation of transactions between ATM switch and bank’s core banking system.

**Platform as a Service**

In this case, Cloud provider takes the responsibility of providing a development platform to consumers rather than business services. Responsibilities in this case are a subset of those mentioned in the above section and would include:

- Deployment of infrastructure and application components i.e. virtual machine, OS, database, application server and application (where the application is used as a development platform)
- Configuration of infrastructure and application components
- Applying OS, database, application server and application patches or performing upgrades
- Starting or stopping the virtual machine, database, application server and application
- Monitoring CPU, memory, disk I/O utilization at the virtual machine level and at a more granular level if there are bottlenecks found within the development platform
- Troubleshooting at various levels within the development platform e.g. OS, database, application server and application error logs
- Taking remedial actions for troubleshooting or performance bottlenecks to provide a stable development platform

**Infrastructure as a Service**

Here we see no reason for Cloud providers to access virtual machines that belong to bank unless specifically agreed between Cloud provider and consumer for specific functions like VM back up. At an overall infrastructure level, there would be a cap on the resources used by any virtual machine.

**Application Related Security Aspects**

Application related security aspects are not unique to Cloud based deployments. We enlist these aspects generically here though it should be understood that different types of applications would have different security requirements. Following are few aspects that need to be looked at by the application vendor before the application is deployed on the Cloud:

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support for Zoning Needs</strong></td>
<td>✦ Ensure that the application meets the requirements for zoning security, and prevents direct access from the user interface layers to the database layers. The application needs to follow a multi-tier deployment model to achieve this.</td>
</tr>
<tr>
<td><strong>Support for OWASP Guideline</strong></td>
<td>✦ Ensure the application conforms to Open Web Application Security project guidelines on web application security, including protection against SQL injection, cross-site scripting, data validation for special characters etc.</td>
</tr>
<tr>
<td><strong>Support for Industry Guidelines</strong></td>
<td>✦ Ensure the application conforms to applicable security guidelines from relevant standards e.g. payment applications need to comply with PA-DSS (PCI-DSS)</td>
</tr>
</tbody>
</table>
| **Prevent Unauthorized Access to Source Code and Executable Files** | ✦ The application executable files and the source code need to be secured from unauthorized access and possible theft  
✦ Obfuscation should be employed as a means of protecting source code theft |
<table>
<thead>
<tr>
<th>Aspect</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Support for Multi-tenancy and Related Security Features** | ✦ If the application is deployed on the Cloud using native multi-tenancy features offered by the application, privacy of data across tenants or entities needs to be ensured through appropriate access control mechanisms  
✦ Application should clearly log business errors and technical errors separately to support separation of duties between business users and data center operator |
| **User Access to Data** | ✦ User access to sensitive data needs to be controlled e.g. a user may be restricted to access only specific products, not allowed to access staff accounts and so on.  
✦ Enforce appropriate password management policies  
✦ Features like session timeouts and restricting logins to office hours can be implemented to enhance security  
✦ The application should clear sensitive data like passwords from memory immediately after it is processed |
| **Role Definitions** | ✦ Ensure application level support for definition of users, roles, and exception management functions |
| **Application Access to Data** | ✦ Ensure well-defined application user interfaces to avoid manual database updates or queries  
✦ For integration with external applications, application needs to have well defined APIs and application needs to ensure that only authorized application can invoke such APIs. |
| **Audits and Maker-Checker** | ✦ The application must have extensive audits to log all transactions and important non-transactional activities. The application needs to implement maker-checker principle for activities like important business parameter updates. |
| **Business Validations** | ✦ Applications should provide relevant and well-documented business validations which need to be periodically carried out e.g. list of accounts not verified before end of day. |
| **Purging Support** | ✦ The application should provide a mechanism to purge old data (after archival if required) while maintaining transactional integrity |
| **Maintainability** | ✦ The application should provide a tool for installation (or OS image usable with virtualization product), for applying patches and keeping track of latest version of the application, including patch release. Manually copying files can lead to security issues. A patch application tool should be able to work on the simultaneous deployment of application patch on multiple virtual machines.  
✦ The application needs to provide a documented mechanism, preferably a tool for application monitoring.  
✦ The application needs to provide a documented mechanism, preferably a tool for reporting important errors and taking automated actions where feasible |

In case of Platform as a Service or Infrastructure as a Service, banks may load test data on the Cloud. If this represents a subset of the live data, it needs to be protected e.g. sensitive elements like customer ID, name, address, phone number, account number, need to be hashed so that the risk of data leakage is minimized. The Cloud provider and Cloud consumer need to agree on the sensitive elements that need to be hashed.
Process for Applying Patches

In case of Software as a Service, Cloud provider often requires to apply OS, application server, database or application patches. These patches would be for fixing functionality, security or performance bugs in the application or infrastructure. This applies to Platform as a Service for all components hosted on Cloud, which form part of development platform e.g. OS, application server and database. It does not apply to Infrastructure as a Service, where this responsibility will be with the Cloud consumer.

The process for application of patches would typically be as follows:

- Need to patch application or infrastructure arises when OS, application server, database or application vendor releases a patch that needs to be applied to production or development environment. Need for a patch could also arise when a consumer reports an incident that requires an application or infrastructure fix.
- Typically maintenance patches are released by infrastructure and application vendors on a regular basis e.g. every three months. In infrequent situations, there could be an emergency patch released due to the identification of a security loophole or a critical defect that could affect production.
- For Software as a Service and preferably for Platform as a Service (in cases where hosted application is used as a development platform), Cloud provider is expected to maintain a test environment which should contain a fully running application with test data. The patch is applied to this environment and sanity tests are done to see if there is any adverse impact. If sanity tests fail, Cloud provider would raise the issue with the application or infrastructure vendor to get a resolution.
- Cloud provider would normally keep the environment up-to-date applying latest patches that are received from infrastructure or application vendors. In cases where the patch requires application of previous unapplied patches, the same is planned.
- Cloud provider plans for application of patch to live environment.
- After sanity testing, patch is qualified for deployment. The Cloud provider informs about availability of the qualified patch to Cloud consumers.
- A committee comprising of representatives of Cloud consumers and Cloud provider takes a decision as to when the patch needs to be applied. This will be typically in off-hours when system load is expected to be low.
- After the above sign-off is received, the Cloud provider informs consumers about when the patch would be applied. Typically patches can be applied node-wise for all the tiers – OS, database, application server. If the patch cannot be applied node-wise, downtime is planned.
- The Cloud provider prepares a fallback plan to revert the system (OS, database, application server and application) to a state prior to patch application. This would generally be supported by infrastructure or application vendor. Worst case scenario would be to take a backup of application directories for a subsequent restoration.
- For this discussion, let us assume that the patch can be applied node-wise and that there are two active nodes processing workload for each Cloud consumer for each tier – web, application and database. One of the active nodes is brought down while other node continues to work. The patch is applied to the node which was shut down while system continues to work with the other active node. If required, the capacity of the remaining node is increased to avoid any negative impact on the overall system.
- Now active node (unpatched) is brought down and patched node is brought up. The system is allowed to run under observation with just the patched node in operation. Periodicity of monitoring is increased to see if the patch has any negative impact on performance.
- Subsequently, the patch is applied to the unmatched node and the same is brought up, after which system is back to normal state.
If an issue is found, fallback plan would be to bring down the patched node, revert the patch and bring it up again.

Important steps within this process are as shown in the Fig 5.5. As specified, the assumption here is that patch can be applied node-wise.

![Figure 5.5 Process for applying patches](image)

**Process for applying upgrades**

Cloud provider may need to plan for OS, application server, database or application upgrades. Upgrades would generally be feature-rich releases and would be much more infrequent compared to patches. Process for upgrade will be similar to that for applying patches with the following variations:

- Application upgrade may entail a database upgrade as well. The Cloud provider needs to evaluate whether database upgrade is backward compatible i.e. whether older version of the application can work unchanged with the upgraded database, which provides a fallback mechanism. Process for fallback will be more complex and could involve a reverse migration database script if database upgrade is not backward compatible. In general, Cloud provider may need to plan for downtime for carrying out database upgrade and inform Cloud consumers accordingly. This step would precede remaining steps which would be similar to those for regular patch application.

- In case of Software as a Service form of deployment, while the upgraded application may need to have downtime for database upgrades, Cloud Provider can look at stand-in functions that could be enabled to minimize the business impact of downtime e.g. few core systems or channels like ATM switches may provide stand-in functionality. It is expected that stand-in server would work in Store and Forward mode i.e. authorizes and store transactions when main server is down and forward the stored transactions to the main server once it comes up.

- Application upgrade could also mean changes to application API signatures. Even if the database and API changes maintain backward compatibility, this would entail doing sanity testing to qualify existing surround applications and reports to work with the upgraded application.

- In some cases, the application server upgrade could also entail application upgrade e.g. J2EE application server upgrade may mandate a new JVM version, which would require recompilation of the application.

Important steps within this process are as shown in the Fig 5.6. The assumption here is that there is a stand-in server available for providing limited functionality in the absence of the main application server.
Process for Testing Business Continuity with Disaster Recovery (DR) Drills

For transactional applications that require an access to customer data, the Cloud provider needs to plan for at suitable DR site. This setup needs to be planned keeping in mind, Recovery Time and Recovery Point Objectives (RTO and RPO). DR could optionally be used for generation of reports. The Cloud provider needs to communicate a detailed DR process to consumers. DR drills need to be planned and all the concerned consumers need to be informed of the same. Shown below is a process assuming a simplistic set up, comprising of only one DR site (near DR might be additionally required in case there is a requirement of zero RPO). Please note that DR site capacity will limit the amount of load that this site can take in case of DR simulation. This applies only to Software as a Service deployment model.
Network Security

Network security consists of security services those restrict or allocate access and those distribute, monitor, log, and protect the underlying resources services.

Architecturally, network security addresses security controls at the network in aggregate or those controls specifically addressed at the individual network level. In a Cloud environment, network security is likely to be provided by virtual devices alongside traditional physical devices. Tight integration with the hypervisor to ensure full visibility of all traffic on the virtual network layer is key to implement network security at hypervisor level. These network security offerings include detective, protective, and reactive technical controls.

A Cloud service provider should provide the following network security mechanisms and best practices:

- Backup and network failover systems to maintain availability of network services.
- Network Access Control (NAC) capabilities to provide access to network on a need-to-know and need-to-do basis.
- Security gateways, Access and authentication controls.
- Security products (IDS/IPS, Server Tier, Firewall, File Integrity Monitoring, DLP, Anti-Virus, Anti-spam).
- Intrusion Detection System (IDS) on virtual infrastructure and cross-hypervisor activity where coordinated attacks can disrupt multiple tenants and create system chaos.
- Security monitoring, Traffic / net flow monitoring, and incident response.
- DOS protection/mitigation.
- Secure base services like DNSSEC, NTP, and SNMP. Management network segmentation and security.
- Integration with hypervisor layer.
- Network survivability.
- Secure communication channel between customer and Cloud hosting site.
- Protection of data in transit. Strong encryption algorithms should be used and key exchange should happen in a secure manner.
- Encryption key management under dual control.
- Best practices for changing the encryption key to avoid the possibility of compromise of the encryption key.
- Option to use third party cryptography services.
- SSL decryption or SSL downloader.
- Real time logs / event collection, de-duplication, normalization, aggregation and visualization.
- Flexible log retention periods and flexible policy management.
- Deep packet inspection using one or more of the following techniques: statistical, behavioral, signature, heuristic.
- Integrity monitoring OS (files, registry, ports, processes, installed software, etc.).
- Technical compliance audits of the network.
- Vulnerability assessment – automated probing of network devices for known vulnerabilities and configuration issues.
- Deep protection against viruses and spyware before they enter the enterprise perimeter.
- Malware, Spyware, Bot network analyzer and blocking.

**Virtual Environment Security**

Following are the generic guidelines regarding virtual environment security:

**Resource Allocation**

- Only authorized administrative personnel should have physical access to the host system to prevent unauthorized changes.
- Hash Value of original system files should be verified prior to installation.
- No unnecessary operating systems components (e.g., drivers) should be loaded, and no unnecessary services should be enabled (e.g., printing services, file sharing services).
- BIOS and Boot Loader Password should be used to protect the system from unauthorised access.

**Hardening of OS**

- Set limits on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM so that no one VM can monopolize resources on a system.
- Ensure that host and guests use synchronized time for investigative and forensic purposes.
- Hosts should have accounts necessary for managing VMs only. Use of strong authentication (e.g., two factor authentication) is recommended, but if passwords are used then ensure that they are strong, hard to guess, changed frequently, and only provided to authorize administrators. The credentials used for access to the host OS should not also be used for access to guest OS.
- All unnecessary programs should be uninstalled, and all unnecessary services should be disabled.
- Configuration management of host OS should be centralized to ensure that configurations are standardized.
- Host OS must be patched regularly and in a timely fashion to ensure that the host OS is protecting the system itself and guest OSs properly. In addition, the same patching requirements apply to the virtualization software.
- Always change the vendor supplied defaults.

**Image Encryption**

- Encrypt and protect virtual machine (VM) images and the data they contain throughout their lifecycle.

**VM Monitoring**

- Centralize logging of guest OSs, either on a separate logging system or in a repository.
- Security information and event management (SIEM) solution should considered correlate server and network logs across virtual infrastructures.
Additional VM Security Measures

- Disable USBs on VMs if these are not required to be used.
- Prefer using flash technology which is considered to be more secure rather than magnetic media.
- Keep each virtual machine on a dedicated partition so that if the virtual machine grows outside of normal limits, its impact on other virtual machines will be limited.
- Avoid sharing IP addresses to reduce vulnerabilities.
- Bare metal (type-1) hypervisor would be preferable since it will provide more security than type 2 hypervisor.

Encryption and Key Management

When planning for Cloud deployment, be sure to integrate a holistic encryption strategy covering the following aspects (based on Reference 9).

Reducing the Scope of Encryption

- Depending upon sensitivity, data should be encrypted. An important point to remember is not all data should be encrypted.
- Before migrating any servers, databases, applications or data to the Cloud, consumers should evaluate the nature of the information they would be moving, the sensitivity of that information and whether the provider service location is appropriately secure for that information to reside.
- Some part of the data can be stored using hash or truncation.

Transport Layer Encryption

- Identify the communication points in the Cloud which needed to be encrypted.
- Implement secure socket layer (SSL) whenever there is confidential traffic over web server or unsecured line.
- A VPN gateway can be established to provide choke points for all administrative access.
- Enforcing secure shell (SSH) as a minimum standard.
- Ensure that the provider establishes a secure file transfer protocol (SFTP) process.
- Encrypt SMTP using Transport layer Security (TLS) encrypting (while using email gateways)

Data Layer Encryption

- Follow universal strategies to encrypt structured and unstructured data.
- The various types of data encryption technologies are database encryption, file encryption, and disk encryption.

Key Management

- Establish an end-to-end process for managing and protecting encryption keys.
- It is suggested to follow key management requirements as per PCI-DSS requirements 3.4 to 3.6 and NIST special publication 800-57.
Monitoring

A multipronged approach to monitoring must be implemented to ensure the integrity of orchestration activities. Following are the considerations for security monitoring (based on Reference 9).

Access Monitoring

- Each layer of the orchestration infrastructure has a user account component.
- The self-service Cloud portal where users log on to request their IT services must have user monitoring enabled. It is important to detect anomalous activities at the request layer itself.
- The Cloud orchestration software runs on OS, which has either local or domain account which needs to be validated and monitored regularly. Compromise to privileged accounts or rogue administration at the system layer can be a significant security breach for the orchestration component.
- Users activities conducted within the Cloud orchestration tool must be monitored to ensure the integrity of the orchestration process.
- The network devices within the Cloud environment are accessed via user accounts that need to be monitored. Pay special attention to firewall management access.
- The SAN and hypervisor management consoles must also be monitored for rogue access.
- At the minimum, monitor failed logons. Successful logons are also important to keep for the purpose of time-stamping administrative activities and successful break-in attempts. If possible, log administrative task in the orchestration management console.

Threat Monitoring

- Intrusion detection system (IDSs) should be deployed at the network level for Cloud environment to detect threats.
- Host-based intrusion detection at the self-service portals is recommended. Orchestration management servers need to have added host level protection.
- Turn on application level logging and monitoring from various management consoles.
- Aggregate activity data from firewalls, IDS (network and host), and application logs from management to console to the SIEM (Security Information Event Management) for correlation. Also, send all access monitoring data to the SIEM for correlation.
- Activate both signature detection and anomalous monitoring and assign the right levels of alerting and triage.

Audit Logging

- Audit logs consisting user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
- The audit logs may contain intrusive and confidential personal data.
- Appropriate privacy protection measures should be taken.
- Where possible, system administrators should not have permission to erase or de-activate logs of their own activities.
Monitoring System Use

- Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.
- Usage monitoring procedures are necessary to ensure that users are only performing activities that have been explicitly authorized.
- A log review involves understanding the threats faced by the system and the manner in which these may arise.

Protection of Log Information

- Logging facilities and log information should be protected against tampering and unauthorized access.
- System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.

Administrator and Operator Logs

- System administrator and system operator activities should be logged.
- An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

Fault Logging

- Faults should be logged and analyzed, and appropriate action should be taken.
- Logging of errors and faults can impact the performance of a system. Such logging should be enabled by competent personnel, and the level of logging required for individual systems should be determined by a risk assessment, taking performance degradation into account.
Physical Security

The Cloud infrastructure including servers, routers, storage devices, power supplies, and other components that support operations, should be physically secured. Safeguards include the adequate control and monitoring of physical access using biometric access control measures and closed circuit television (CCTV) monitoring. Providers need to clearly explain how physical access is managed to the servers that host client workload and that support client data.

A security plan for the physical environment should be implemented as follows.

- Ensure that the facility has the appropriate physical security controls to prevent unauthorized access to critical areas within facilities and access to physical assets and systems by intruders or unauthorized users.
- Ensure that all employees with direct access to systems have full background checks.
- Ensure that all third-party providers have policies and procedures in place to distinguish employees from visitors.
- Ensure that the hosting service has adequate natural disaster protection.

Physical security is an IT infrastructure service to create awareness of physical security and coordinate it with IT security. This can include employee badges, RFID readers, surveillance systems, and associated technology or assets. Physical security can include automation related to surveillance, motion detection, object and human identification and tracking, entry control, environmental system monitoring, perimeter control, and power and utility system monitoring.

Physical security increasingly relies on logical access security to protect physical access. The most common examples include access control systems on doors, such as password keypads, biometric scanners, or badge readers. In many cases, these access control systems require that access be granted on a per-person basis. In these cases, the physical security systems rely on the Identity, Access and Entitlement Management system to manage the identities and entitlements (who can access which parts of the physical facility) in an organization.

Logical Security

Logical security is used along with physical security to provide complete security to business critical data and systems. In a Cloud based environment where business critical data and information systems are coexisting at multiple places, logical security has a very important role in securing the data.

Common logical security techniques used for data and system protection are, logical access control (username, password, OTP, RSA Token, Biometric Authentication, etc.), discretionary access control and mandatory access control. These techniques are used for identification, authentication, authorization and accountability of users and systems.
References

10. Security Considerations for Cloud Computing, ISACA.
12. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.
13. COBIT Assessor Guide Using COBIT 5
14. IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. ISACA.
Mr. Madhusudana Rao  
Associate Director, CDAC

Mr. Avinash W. Kadam  
Advisor, ISACA India Task Force

Mr. Naresh Shankaran  
CISO, Citibank India

Dr. Onkar Nath  
CISO, Central Bank Of India

Mr. Thomas John  
AGM (IT), Dena Bank

Dr. G.R.Gangadharan  
Assistant Professor, IDRBT

Mr. Deepak Hoshing  
Head – Architecture, FINACLE &  
Associate Vice President, Infosys Technologies Limited

Mr. Tushar Vartak  
Vice President, IT Risk & Security Management,  
J.P. Morgan Chase Bank N.A.

Mr. C. Sridharan  
DM & CISO, Canara Bank

Mr. Pushpender Rashtrawar  
CISO, Bank of Baroda

Mr. Keshav Metkar  
Manager – IT, Bank of Maharashtra

The contribution of  
Mr. Shaga Praveen, M.Tech. Student, University of Hyderabad & IDRBT and  
Mr. Sai Kiran Vidiyala, Research Associate, IDRBT is acknowledged.