Best Practices for Security in Cloud Adoption by Indian Banks

A White Paper by:
Members of The Open Group Security Forum

Joydipto Banerjee, IBM

Dr. G.R. Gangadharan, IDRBT

Periasamy Girirajan, IBM

Dr V.P. Gulati, TCS

Jim Hietala, VP Security, The Open Group

Sreekanth Iyer, IBM

Atul Kumar, DSCI

Manish Parikh, ATOS

Ravikumar Ramachandran, HP

Bhaskar Tondale, TCS

March, 2015

Best Practices for Security in Cloud Adoption by Indian Banks

This document is provided "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose, and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

If you did not obtain this copy through The Open Group, it may not be the latest version. For your convenience, the latest version of this publication may be downloaded at www.opengroup.org/bookstore.

Best Practices for Security in Cloud Adoption by Indian Banks

Document No.: W152

Published by The Open Group, March 2015.

Any comments relating to the material contained in this document may be submitted to:

The Open Group, 44 Montgomery St. #960, San Francisco, CA 94104, USA

or by email to:

ogpubs@opengroup.org

Table of Contents

Boundaryless Information Flow

TM

Boundaryless Information Flow ™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

Banking has traditionally been a conservative industry with regard to adoption of newer technologies due to the sensitivity of the banking business. In addition, since banks deal with public money, stringent regulation and governance comes into play. Despite their conservative approach, and despite regulatory pressures, the current volatility in the market forces banks and other Financial Institutions (FIs) to look at means to reduce operational costs and bring in innovative products which would provide better market coverage and quick return on investments. IT infrastructure contributes to a significant part of the operational costs of banks.

Cloud computing is an obvious option for banks in order to have efficient and cost-effective IT strategy. When cloud computing was first introduced, cloud maturity levels were low and banks and FIs were apprehensive about adopting cloud computing as they are governed by standards, data privacy, and regulations. The cloud space has now become much more mature and most of the standards and banking regulations have been amended to accommodate cloud computing, which is paving the way for banks to adopt cloud services.

Moreover, the workload in a banking environment varies significantly in a business day. In the past most of the banking infrastructure consisted of a Core Banking Solution (CBS) supported by multi-channel platforms. Nowadays the infrastructure is augmented by advanced analytics, real-time campaign management, and customer experience analytics, which are compute heavy. This clearly suggests the need for a

business case for banking CIO/CTOs to look at cost-effective platforms, including cloud services.

In the recent past we have seen some traction and adoption of cloud services in the banking and financial markets space in India; however, the degree varies based on the appetite for operational cost reduction and openness towards adoption of newer technologies. A number of analyst studies, including ones from Gartner, [1] predict rapid growth in the public cloud services market in India (the most recent Gartner study suggests growth at 33% in 2015).

The benefits of adoption of cloud computing are substantial as evidenced by some of the banks in India, though the industry has to prepare carefully for associated challenges. This White Paper, in addition to discussing the legal environment prevailing in India, discusses security requirements at length and the security remediation measures and security controls for IaaS and SaaS cloud services. The opportunities for cloud computing adoption, along with deployable architectures, are also well articulated and shown.

Cloud computing has its own unique security and compliance challenges which much be understood thoroughly before embarking on it. At the same time, cloud computing presents the opportunity to transform security practices and improve defenses. This White Paper provides insights so that management of various banking institutions can embrace and adopt cloud computing and exercise appropriate governance and oversight for successful business benefits realization at acceptable risk.

[1] Refer to www.gartner.com/newsroom/id/2964917.

Key Stakeholders and Value Propositions

Key stakeholders in the adoption of cloud services by the banking sector in India include:

- Banks and FIs in India: The value proposition for banks and FIs in India includes most of the business benefits described elsewhere in this White Paper, including increased business agility, and decreased costs.
- Government of India, Reserve Bank of India (RBI), and other sector regulators: The value proposition for the government and regulatory agencies includes keeping the banking community in India competitive with other countries' financial sectors, and reducing costs for banking services to individual and commercial banking customers in India.
- Cloud service providers: The cloud service provider community sees obvious value and opportunity in building new services and revenue streams from cloud services aimed at financial organizations in India.

Benefits for the Banking Industry and Challenges to Cloud Adoption

What is the Benefit Cloud Computing Brings to Various Banks?

Banks and financial services organizations traditionally spend the highest percentage of their operating expenses on IT, as compared to other industries. Cloud adoption is identified as high priority for 60% of CIOs across various industries. The benefits of cloud computing which are specific to banks can be grouped into the following categories.

Time-to-Market

When a new product launch is planned in the banking and financial market space, apart from the business analytics and product design, there is a significant readiness required from IT. The product should be supported by core banking, and serviced by all channels. The associated knowledge management needs to be updated. Few product launches would even call for a business process change. This would mean faster development lifecycles and a faster deployment lifecycle are required. Another significant pain-point in new product launches is the predictability of growth. Although a great deal of research goes into the creation of products, most times the growth is unpredictable and can grow both toward the bank and its infrastructure, as well as toward customers. If growth is toward the bank and its infrastructure, then the return on investment is stretched for the deployed licenses and hardware.

Faster development and deployment of capabilities can be addressed by IaaS, PaaS, and SaaS cloud services. And if the bank manages unprecedented growth, then the ability of cloud services to elastically scale would help to achieve this growth without much disruption to business (whereas in a normal state such rapid growth would have triggered additional procurement, downtime, and until more capacity is built and deployed, performance would be impaired).

Workload Optimization

Banking industry workloads are unique when compared to the other industries, in the sense that the variation is very large even within a business day and varies even more significantly on specific days such as year-end and quarter-end. The following are the top three workloads in banking and the schematic diagram (Figure 1) provides a variation of the same on a normal business day:

- Core systems
- Payment systems
- Reporting and analytics

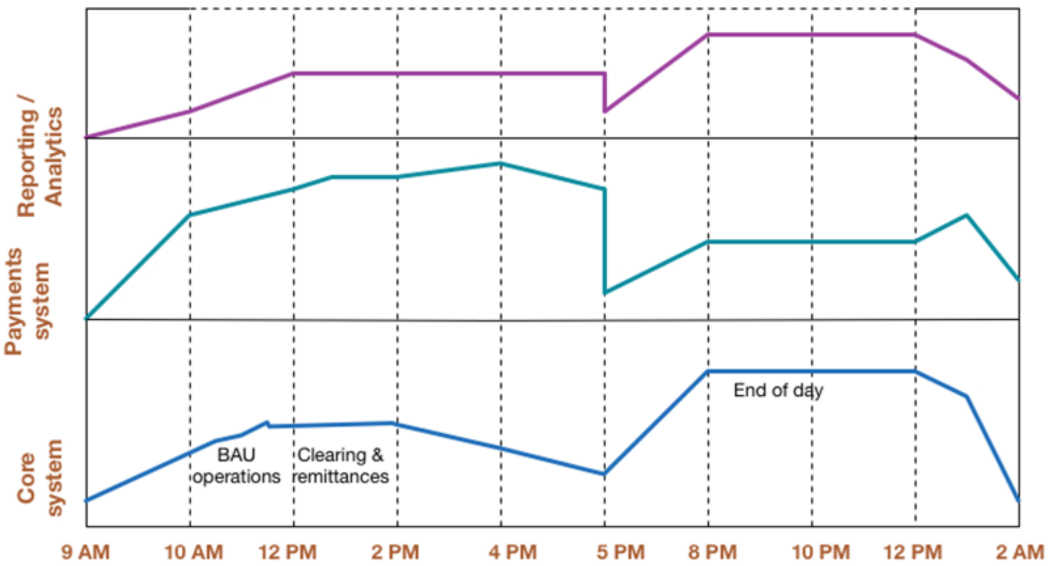

Figure 1: Banking Industry Workloads – Variation during Typical Business Day

As shown in Figure 1, there are peaks and troughs at different times for different applications. With dynamic cloud computing environments the whole workload can be optimized at least to the extent of 20-30% of overall compute capacity.

As described in Figure 2, cloud computing brings in data from a variety of sources, including from customer organizations, and their employees and customers. Metadata can also be brought into the cloud, and generally additional metadata is produced by the cloud service.

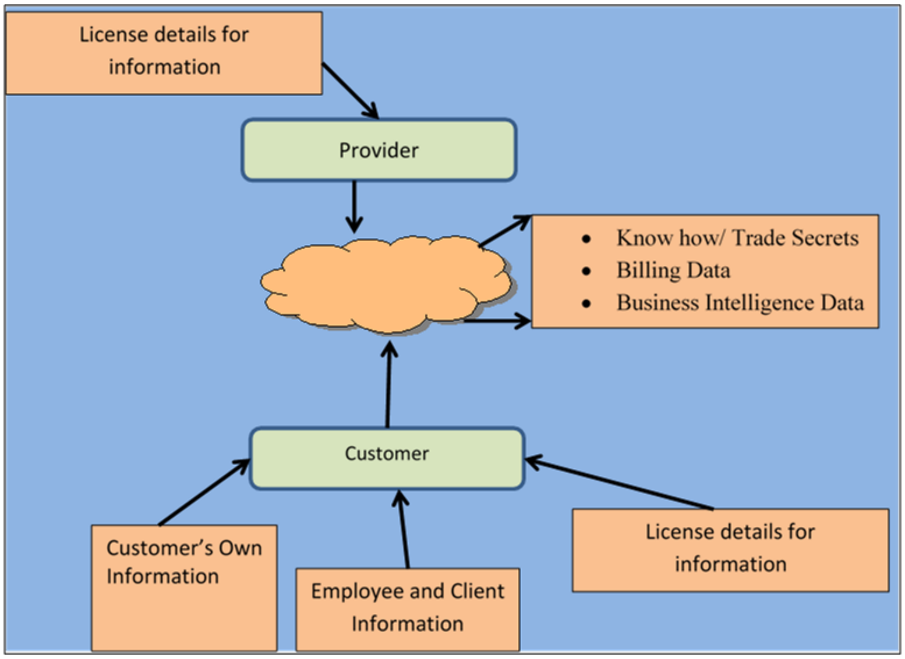
License details for information
Provider
Know how/ Trade Secrets
Billing Data
Business Intelligence Data
Customer
Customer's Own Information
Employee and Client Information
License details for information

Figure 2: Data Sources using the Cloud

One more optimization area is the test and development environment, especially for core systems. Since this caters to almost all business units which are involved in banking operations, there is a need for numerous redundant test and development environments. In a mid-size bank at any point in time there would be at least 10 test environments of the core system. With cloud computing, the compute capacity can be optimized with lower overall cost, as not all business units will be using them at the same point in time.

Funding

In the banking industry there are unknown business demand fluctuations. Maintaining costly infrastructure with low utilization is expensive. Rapid and flexible expansion (and contraction) of service usage through the cloud, while paying based on usage is financially prudent. Savings in capabilities in Disaster Recovery (DR) and testing services (with desired SLAs) in special time periods can be obtained rather than maintaining such services in-house.

Cost rationalization and savings on CAPEX, along with just paying based on usage, users, or any other metrics, helps financial planning and reporting of IT costs. Minimal software tool footprint and efficient use of software licenses are also key outputs of cost rationalization.

Shared Services Model

The banking business consists of certain key business processes which are important differentiating factors to the organization such as the credit rating process, customer segmentation, and targeted marketing. There are certain business processes such as customer on-boarding and outbound mass marketing which are prudent to outsource. For these non-core processes, outsourcing them can bring the cost per transaction and customer acquisition costs down, which are key measures of IT spend and efficiency in banks and FIs.

Using cloud computing, these non-core business processes can be outsourced to vendors who operate on shared services delivery models, while still meeting data privacy requirements.

Adoption of Cloud in the Banking Industry – India Success Stories

There are several early success stories of banks in India adopting cloud computing for optimizing their processes, reducing their costs, and building the capability to scale rapidly. Some of the known/published references are discussed below. It is worth noting that while Urban Co-operative Banks (UCBs) and Regional Rural Banks (RRBs) have been early adopters of cloud computing, as described below, we can expect that larger banks will move towards cloud services as regulatory issues and security challenges are addressed.

Two major software solution providers[2] have provided their Core Banking Solutions (CBSs) to UCBs, RRBs, and district co-operative banks through their own data centers. Some of the major UCBs have also been providing IT support to the small UCBs while leveraging collaborative arrangements among themselves for sharing common IT infrastructures such as data centers and ATM networks. It was observed that these banks were located across India, the geographical proximity or separation was neither a constraint nor a

[2] Refer to the RBI Working Group Report on Cloud Computing Option for Urban Co-operative Banks.

contributory factor, and cloud services were geography-neutral due to availability of good telecommunications networks.

FIs[3] such as Kotak Mahindra Life Insurance, Reliance General Insurance, and IndiaFirst Life Insurance have adopted virtualization solutions to help improve efficiencies of their data centers. Dhanlakshmi Bank has opted to move all of its non-core banking applications to a virtualized solution allowing reuse of old storage boxes. Nawanagar Co-operative Bank has engaged with a cloud service provider to deploy CBS on a hosted cloud services model. ShamRao Vithal Bank partnered with a cloud service provider to offer cloud-based solutions to other co-operative banks in its region.

India is home to a large number of urban and rural co-operative banks. These banks are facing challenges in many aspects and are trying to transform themselves in a complex business environment. Stiff competition is also putting banks under pressure to become more efficient and agile. Four co-operative banks in India – The Co-operative Bank of Rajkot (Gujarat), Shivajirao Bhosale Sahakari Bank (Maharashtra), Goa State Co-operative Bank, and Tumkur Veerashaiva Co-operative Bank (Karnataka) – have adopted hosted solutions to improve their operational efficiency and compete more effectively. As per the company's media release, this solution will enable these banks to set up a cost-effective and energy efficient data center to offer new services like ATM, mobile banking, and online banking to customers. As a customized, pre-packaged data center primarily for small and medium businesses, the solution will also help the banks reduce their energy consumption by 2%.[4]

Pondicherry Co-operative Urban Bank[5] uses a cloud computing solution to offer more customer-centric services and to establish a robust banking operation. By implementing this multi-tenant IaaS on the cloud, the bank will be able to offer state-of-the art financial solutions to its customers including Internet banking, online money transfer, ATM, and mobile banking. This will also help the bank to centralize its mission-critical operations such as real-time transaction processing across its six branches in Pondicherry. This is implemented as a shared private cloud for compute and storage with the ability to rapidly provision capacity for additional branches as required.

YES Bank[6] has adopted cloud computing and has been an early adopter of cloud-based services in banking with the first implementation in payments, online account opening, and remittance services. Cloud computing provides the bank flexibility in faster provisioning at a low cost.

Meghdoot is an open cloud initiative of the Centre for Development of Advance Computing (C-DAC), a cloud computing environment completely based on free and open source software. The Indian Banking Community Cloud has been established using Meghdoot in the Institute for Development and Research in Banking Technology (IDRBT), Hyderabad (established by the RBI). The community cloud was inaugurated by the Governor of the RBI and currently six banks have applications ported into the Meghdoot cloud.

[3] Refer to Zinnov: IT Adoption in BFSI Sector in India.

[4] Refer to Information Week article: Four Co-operative Banks in India Adopt IBM's Data Center Solutions.

[5] Refer to Information Week article: Pondicherry Co-operative Urban Bank Adopts IBM SmartCloud for Core Banking Solution.

[6] Refer to Moneycontrol.com article: Business Transformation of YES Bank through Cloud Computing.

What are the Challenges in Implementing Cloud Computing?

Like any other large-scale platform, design and development of a cloud computing platform comes with its own challenges in different dimensions. With current matured cloud service providers most of the risks can be mitigated; however, the following are the key challenges.

Data Residency Requirements

Most central banks (including the RBI) require that core system banking data needs to physically reside within the geography. Because of this requirement, the choice of cloud computing platforms can be limited. However, some applications which handle non-core banking data such as CRM, HR, and others can still be placed on remote cloud services without data residency issues. There is also the question of how to handle data for subsidiary bank branches located overseas.

Cloud Compatibility and Availability of Services

Another key challenge faced by the banking industry is the compatibility of applications for cloud computing or options for porting them onto the cloud. The percentage of legacy applications is significant in the financial industry when compared to other industries. Moreover, these applications in most cases have been customized to a greater extent which makes moving from in-house legacy applications to a cloud-based offering difficult. The typical implementation and stabilization timeframe for a core banking application is almost five years which makes it difficult for banks to switch to another vendor who offers cloud-based delivery. Only a few vendors in India offer cloud-based core banking which again is targeted for mid-size to smaller banks with a limited set of product features and offerings.

Network Latency

Business process availability is key for smooth operations. Using a cloud-based model, networking adds another dimension of complexity for business availability. There are mechanisms to address this such as redundant Multi-Protocol Label Switching (MPLS) networks from multiple service providers; however, performance and availability remain a challenge. In India, banks are required to operate in rural and semi-urban environments as per RBI guidelines, and network latency can be an inhibitor in such areas.

Data Privacy

Data privacy and security is another challenging aspect which hinders the migration of banks onto the public cloud. Banks capture, store, and process private financial details and demographic information on their customers. Regulations require that banks Know Your Customer (KYC) in on-boarding new customers. In order to comply with these requirements banks need to maintain copies of KYC documents, which could be personal identification documents such as passport information or some other personal identification information. Data privacy becomes very important as any breach of privacy might cost the bank lost customers, as well as possible reputation damage, legal issues, and fines.

Vendor Lock-In

Lock-in reduces the ability to customize and extend, and can create dependencies on vendors and affect business continuity. There can also be concerns at the application and data level regarding the lack of portability between SaaS software available in the market.

Three types of possible lock-in can affect cloud service use:

- **Platform Lock-in**: Cloud services tend to be built on one of several possible virtualization platforms; for example, VMWare or Xen. Migrating from a cloud service provider using one platform to a cloud service provider using a different platform could be very complicated.
- **Data Lock-in**: Since the cloud is still new, standards of ownership – i.e., who actually owns the data once it lives on a cloud computing platform – are not yet developed, which could make it complicated if cloud computing users ever decide to move data off a cloud vendor's platform.
- **Tools Lock-in**: If tools built to manage a cloud computing environment are not compatible with different kinds of both virtual and physical infrastructure, those tools will only be able to manage data or apps that live in the vendor's particular cloud computing environment.

Vendor lock-in is one of the challenges in adopting cloud computing today, but the risks associated with it will be reduced as the cloud computing space becomes more mature. Lock-in risks can also be mitigated with robust SLAs, as defined and agreed with vendors.

Performance

Multiple components and hops are involved starting from the end-user desktop (interface card) to LAN: end-user router, network cloud, perimeter of provider, LAN, and ultimately the application. Business services need to be categorized accordingly for latency. Due to its multi-tenant nature and resource sharing, cloud computing must also deal with the "noisy neighbor" effect. This effect in essence indicates that in a shared infrastructure, the activity of a VM on a neighboring core on the same physical host may lead to increased performance degradation of the VMs in the same physical host, due to issues such as cache contamination.

Storage Issues

Data storage management becomes a critical issue as data, especially finance-related, will be residing in the provider's cloud. Consumers should be able to scale data storage on an as-needed basis, restrict physical location of the data at rest (database, tapes) to handle issues of data sovereignty, ensure that proper processes for data purging and disposing of data storage hardware are followed, and administer access controls for their data.

Efficient SLAs

Creating standard contracts and SLAs where expectations are clearly enumerated from both sides is crucial for cloud adoption. For example, banks including Commonwealth Bank of Australia, Bank of America, and Deutsche Bank were part of an alliance (Enterprise Cloud Leadership Council) to create some standards to compare apples with apples when buying cloud services. In the case of IaaS cloud services, they typically operate on a shared responsibility model. The IaaS vendor generally takes responsibility for running and hosting back-office services, but the responsibility for securing the data lies with the customer. This is true for most IaaS cloud services.

Change Management Issues

Infrastructure utilization may be 10% on average, but when the bank needs 100% usage, it is critical that it is available, secure, and resilient. Consequently, banks have a reluctance to downsize their internal resources.

Each choice around cloud computing effectively means "decommissioning" a portion of the IT and process stack, ranging from business capabilities to infrastructure. The human capital perspective may also be critical, since cloud service providers will not welcome any significant transfer of staff that would affect their business model. All of these considerations underline the need to prioritize both strategy and execution in moving to the cloud.

Legal and Compliance

There are various risks monitored and managed by banks including operational (or transaction) risk, legal/compliance risk, strategic risk, reputation risk, and credit risk. The risk management, compliance, and liability reduction principles that apply to FIs' technology services activities across the board logically also apply with equal force to FIs' cloud computing activities.

One legal and compliance issue brought by cloud computing and cloud-hosted data is cross-border data flow – the need to observe the differing data protection rules of each country through which a data set may pass. For example, data security guidelines from RBI need to be followed while creating contracts with cloud service providers for Indian banks. Data should reside within the boundary of jurisdiction of the particular country. The bank should know where the data is stored.

An important legal and compliance issue with cloud computing is the problem of who is in "possession" of the data. If a cloud computing company is the "possessor" of the data, the possessor has certain legal rights. If the cloud computing company is the "custodian" of the data, then a different set of rights would apply. The next problem in the legalities of cloud computing is that of legal ownership of the data. Many terms of service agreements are silent on the question of ownership.

These legal issues are not confined to the time period in which the cloud-based application is actively being used. There must also be consideration for what happens when the provider-customer relationship ends. In most cases, this event will be addressed before an application is deployed to the cloud. However, in the case of provider insolvencies or bankruptcy the state of the data may become blurred.

Forensic Investigations

A bank will face challenges to investigate any frauds happening in a cloud computing environment, as investigators have to rely on cloud service providers who may not be in the same jurisdiction and also the data may be distributed, geographically spanning multiple locations in virtual storage. Taking down servers in a cloud computing environment impacts other customers. There may be significant quantities of data to investigate and investigators cannot take the whole disk like they do in traditional environments. Chain of custody is almost impossible in cloud computing environments. In addition, cloud service providers often focus primarily on restoration of service after an incident, while investigation can be an afterthought. Finally, from a technological standpoint, it is uncertain whether data can be retrieved when a VM is de-allocated.

Compliance

The RBI provides some best practices for governing IT environments at banks. There are also certain domain-specific compliance regimes such as PCI-DSS (Payment Card Industry – Data Security Standard) for all payment-related businesses. The credit card brands which enforce PCI compliance can apply fines of $100,000 for non-compliance, and they can also eliminate a retailer or card processor's ability to process transactions.

The PCI guidance says that clients will need to verify all locations and the flow of their data to ensure compliance and meet legal obligations in each country. The most difficult requirement of the PCI-DSS guidelines when looking at cloud computing is PCI data segmentation, in which client environments are separated from one another and cardholder data environments are segregated from non-cardholder data to limit the scope of PCI compliance. Another challenging aspect of PCI compliance is managing the shared responsibility between merchants and providers. A third is the need to run a PCI project on an ongoing basis, while constantly updating providers' proof of compliance.

Encrypting the data before sending it to the cloud will help to secure information, meet compliance requirements, and ensure that audits are successful, but may also raise costs.

Private clouds will play a pivotal role in core banking, enabling banks to keep control over the location of sensitive customer data, but they may lack the cost savings of public cloud services.

Governance

Another category of challenges in adopting cloud computing arises from governance. Whereas in on-premises computing, governance is limited to the enterprise, in cloud computing, some governance issues remain with the enterprise, while others have to be managed by the cloud service provider. An example would be change control and upgrades to system infrastructure and software, which affect the customer, but which will involve governance decisions from the cloud service provider.

Finally, some other risks and compliance challenges associated with implementing cloud computing, and moving workloads to cloud services, include:

- A change in mindset is needed within the FIs to move from an operations and technology outcome-related view to a business service delivery model.
- Not enough major trusted players are delivering to the levels of expectation that have been established in the current on-premises computing environment.
- There is insufficient proof of success of the service providers enabling business to outsource the full spectrum of service capabilities more effectively, efficiently, and to manage scale in an elastic manner.
- There is a lack of solution maturity across technical, functional, operational, commercial, and partnership models at a level that can support the FI.
- There can be increased probability of risk and exposure to potential issues related to business operations, confidentiality, and compliance which are critical in the financial service industry.
- Long-term cost impacts are unknown, especially considering the scale and criticality of services to the financial business; in addition, moving to cloud-based models is a strategic shift and it will be difficult to reverse once the institutions have gone down this path.
- Large FIs may not be convinced of the benefits of the solution. These large FIs have developed an efficient business and technology operation, including lean data centers, shared service models, standardized platforms, and embedded innovation investments. There exists a perception that cloud computing would provide more scaled economics than service innovation.
- Perceived commoditization and reduced ability to customize, extend, and differentiate with the external services provided.

- Question marks around availability and reliability of the services provided and ability to provide consistent quality of service to support peak business requirements.
- Pain of integration into the enterprise which (for FIs) is overtly complex, global, diverse, and heterogeneous consisting of significant (>60%) custom-built applications within the portfolio.

Legal and Regulatory Context for Indian Banks

A working group was created by the RBI for exploring use of cloud computing in UCBs. It comprised experts from the RBI, software industry, and academia. Based on their analysis of the banking sector, technological trends in cloud computing, and use of cloud-like solutions by UCBs (such as IT support offered by these banks to other banks, which include data center and DR sites, ATMs, payment gateways, etc.), the working group has suggested its approach for cloud adoption in UCBs. In its recommendation, the working group suggested:

"Cloud computing is an emerging technology for which standards and technology management processes are still evolving. It has many complexities and uncertainties which need to be understood. In view of the sensitive nature of banking services as well as limitations of the target banks for managing this technology, the working group recommends caution while adopting cloud computing solutions for the target UCBs until such time that issues are resolved satisfactorily."

Moreover, the working group recommended cloud adoption for support and surrounding services, and non-financial applications in banks which help in gaining experience on cloud usage. Further research and development by banks and the software industry was also recommended particularly in the areas of cloud governance, cloud management, and security technology. As few banks have already adopted private cloud services, the working group recommended identification of adequacy of risk mitigation measures and to address concerns regarding data security and data privacy in the multi-tenancy environment.

In one of the circulars released by the RBI,[7] usage of IT was identified as a critical element for survival and growth of banking institutions. In the line of advice to UCBs to adopt CBS as soon as possible, the circular mentioned:

"A large number of software is available today, including cloud-based solutions, and UCBs may adopt the model that meets their bank's requirement."

In a keynote address on "Indian Banking: The New Landscape",[8] Dr. K.C. Chakrabarty, Deputy Governor, RBI highlighted the importance of technology adoption such as cloud computing and big data that can help the banking industry grow from the perspective of both scale and scope of the economy. According to Dr. Chakrabarty:

"Banking technology is poised to make a big leap in the near term towards integrating customer data across banking platforms, facilitating trade in a more secure manner, developing virtual desktops and private clouds to centralize information across desktops by making them available to different employees on an as-needed basis, enabling speedier transaction processing and faster settlements."

[7] RBI Cir. No. 42/09.18.300/2012-13: Implementation of Core Banking Solutions (CBS) by Urban Co-operative Banks (UCBs).

[8] Refer to: http://rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=872.

The RBI Working Group Report on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds,[9] provided recommendations on adoption of cloud computing in banks. Cloud adoption may demand attention to security and legal issues applicable to cloud computing as these are still evolving and a bank needs to be cautious and carry out due diligence to assess the risks comprehensively before considering cloud computing.

Emerging technologies such as cloud computing have given rise to unique legal jurisdictions for data and cross-border regulations. Banks should take care of the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically and upon any significant changes introduced by the service provider.

There are various elements that are required to be undertaken while considering a move onto the cloud:

- As per the RBI policies, when an Indian bank's subsidiary is established outside India, that subsidiary should follow local regulations and RBI regulation.
- While moving onto the cloud the location of the data centers is a critical aspect to be considered and, as per RBI regulation, the data center of the subsidiaries of Indian banks established outside the country should be located in India. When a foreign bank establishes a subsidiary in India, its data center should be located in India, as mandated by the RBI.
- In case of ATM transactions, it is required to be connected to the switches. If Indian bank ATMs are operating in other nations, they can be connected to either local switches or Indian switches (because they are linked via their payment consortiums such as Mastercard/Visa, etc.).

Information Technology (Amendment) Act 2008

The Information Technology (Amendment) Act (ITAA) 2008, which is an amendment to the Information Technology Act 2000, provides various provisions for security and privacy that are applicable to the cyber domain including cloud computing. Banks adopting cloud services are also required to comply with these regulatory norms. Figure 3 shows the provisions in the ITAA 2008 applicable to cloud computing.

[9] Refer to: http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf.

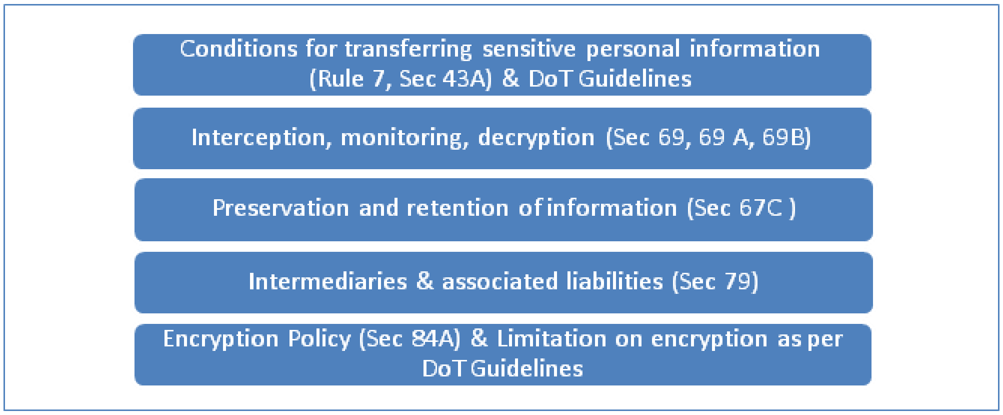
Conditions for transferring sensitive personal information (Rule 7, Sec 43A) & DoT Guidelines
Interception, monitoring, decryption (Sec 69, 69 A, 69B)
Preservation and retention of information (Sec 67C)
Intermediaries & associated liabilities (Sec 79)
Encryption Policy (Sec 84A) & Limitation on encryption as per DoT Guidelines

Figure 3: ITAA 2008 Cloud Computing Provisions

Security of sensitive personal information of the end-users (individuals) of cloud services is essential. Provisions are made in the ITAA 2008 to ensure the same. Section 43A of the ITAA 2008 applicable to service providers requires that they protect sensitive personal information by following reasonable security practices. Section 43A of the ITAA 2008 deals with security practices and procedures that cloud service providers need to undertake to protect sensitive personal information from any security and privacy breach such as unlawful access, use, alteration update, or disclosure of information. The rules issued in Section 43A explicitly define sensitive personal information and reasonable security practices.

These reasonable security practices and procedures on the one hand can be perceived as a burden on service providers, but on the other hand are seen as helping to increase trust in cyberspace and cloud computing. This increased trust encourages users to use the cloud computing platform for its critical operations. As the banking sector is always considered to be a critical sector, building trust would be the key enabler in the adoption of cloud computing for main-line operations.

Businesses are obliged to comply with law enforcement for national security and cyber crime investigations. These obligations will continue to exist in the cloud and therefore the banks and the cloud service providers need to be aware of such legal requirements in India and work out legal arrangements amongst themselves for compliance. Sections 69, 69A, and 69B of the ITAA 2008 facilitate the interception, monitoring, and decryption of the information with a defined legal process. This is also supported by the regulatory provisions for preservation and retention of information which is covered under Section 67C of the ITAA 2008 (rules are yet to be notified). This may be considered as an enabler to the cyber forensics and investigation processes, which is essential in case of fraud or breach. It has been identified in various surveys and statistics that frauds and breaches are frequently driven and motivated by financial gains. Regulatory provisions made under the ITAA 2008 become essential when cloud computing is being used for financial operations by the banks.

Encryption standards are essential to strengthen the security of the data residing in the cloud. Variance in the legal and regulatory requirements *vis-à-vis* minimum and maximum limits on the strength of encryption standards creates challenges for cloud service providers when it comes to meeting monitoring, decryption, and interception-related regulatory requirements. In this regard, the 40-bit limit on the encryption standard as part of the DoT's telecom licensing conditions and Section 84A (encryption policy) of the ITAA 2008 are applicable. The government is yet to release encryption standard u/s 84A. SSL/28-bit encryption must be used as a minimum level of security as per RBI's Internet banking guidelines. Regulatory norms are not specifically defined for cloud computing and are made technology-neutral. As cloud computing is subject to these provisions, service providers and bodies like banks who adopt cloud computing to serve their customers are required to comply with these regulations.

There has been lot of debate and various interpretations on the applicability of Section 79 of the ITAA 2008 to banks – whether banks are intermediaries or not.

The ITAA 2008 definition of intermediaries is as follows:

"Intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores, or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online-market places, and cyber cafes."

As defined, it seems clear that cloud service providers would be considered intermediaries under Section 79 of the ITAA 2008.

The due diligence prescribed in the rules in Section 79 seems to be aimed at intermediaries that are offering B2C services, providing access/sharing capabilities and where the users can interact; i.e., post, modify, and delete electronic records. These provisions may not be applicable to banks. Banks do not allow content (customer financial records or transactions) to be accessed by or shared amongst the public, community, or groups of individuals, and the content cannot be hosted, displayed, uploaded, modified, published, transmitted, updated, or shared by the users. All changes in the information stored by banks are rule-based and stringent controls are in place to limit access and restrict who can change information.

The provisions laid out in Information Technology Rules 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) which may have an impact on cloud computing are as follows.

Section 3 defines "sensitive personal data" or information which relates to:

1. Passwords
2. Financial information such as bank account, credit card or debit card, or other payment instrument details
3. Physical, physiological, and mental health condition
4. Sexual orientation
5. Medical records and history
6. Biometric information
7. Any detail relating to the above clauses as provided to the organization for providing service
8. Any of the information received under the above clauses by the organization for processing, stored, or processed under lawful contract or otherwise

Provided that any information that is freely available or accessible in the public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

The next relevant section is Section 8 which speaks on reasonable security practices and procedures and points out that compliance with ISO/IEC 27001 can be considered as compliance with reasonable security practices and procedures. However, readers are advised to go through the provisions with the guidance of a legal counsel.

Understanding the Requirements in Detail

Identity and Access Management

Access segregation, application segregation, and in particular data segregation have to be done using advanced technology and a clear-cut process and guidelines must to be laid down for the same.

Privileged access to data has to be monitored and controlled.

In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for critical activities like fund transfers and changing customer-related details through an Internet banking facility.

Infrastructure Security

Maintain detailed inventory of information of assets and classification of information/data.

Information security needs to be considered at all stages of an information asset's (hardware, software, data) lifecycle which typically includes: planning and design; acquisition and implementation; maintenance and support; and disposal so as to minimize exposure to vulnerabilities.

Robust network protection strategy and layered security based on the principle of defense-in-depth is an absolute necessity for banks.

Banks need to scan frequently for vulnerabilities and address discovered flaws proactively to avoid the likelihood of having their computer systems compromised. Automated vulnerability scanning tools need to be used against all systems in their networks on a periodic basis.

Cloud Reliability: The SLA should clearly reflect uptime and performance parameters and alternatives for contingency situations for provider infrastructure (including network).

Network: The network connecting users to cloud services becomes a critical component for any cloud-based applications. It poses questions of availability on a continuous basis, security risk for critical data in transmission, vulnerability to virus/worms/DoS attacks to name a few, physical cable cutting, natural disasters, etc. Network outages have to be considered and contingency planning has to be in place for such events.

Remote Access: Strong controls need to be initiated against any remote access facility. The management should establish policies restricting remote access and be aware of all remote access devices attached to the bank's systems. These devices should be strictly controlled.

Latency: Clear-cut demarcation and responsibility, network optimization tools, web acceleration technologies, and application capabilities to an extent can assure levels of acceptable performance.

Client Device/Application Protection: Protecting the cloud computing consumer's client device (e.g., a computer running a web browser) so as to control the exposure to attacks is recommended.

Data Security

Data security measures need to be in place. Banks need to define and implement procedures to ensure the integrity and consistency of all critical data stored in electronic form, such as databases, data warehouses, and data archives.

Cryptographic techniques need to be used to control access to critical and sensitive data/information in transit and storage. This requires strong encryption using a robust algorithm with keys of required strength used for web sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. The same diligence and security controls (encryption and access control) should be applied to stored data. Cryptographic algorithms must be applied for encryption and digital signature. Understand how cryptographic keys are managed and who has access to them. Ensure that cryptographic keys are adequately protected.

Direct back-end updates to the database should not be allowed except during exigencies, in the event of a genuine business need and after due authorization as per relevant policy.

Off-line Data Synchronization: This is critical for any network-based application to take care of outages at the network or consumer level. Technology adopted should be capable of taking care of version control and re-sync data.

Data Storage Management: Consumers should be able to scale data storage on a demand basis, restrict physical location of the data at rest (database, tapes, etc.) to handle issue of data sovereignty, ensure proper process for data purging and disposing of data storage hardware, and administer access control over the data.

Data transfer from one process to another or from one application to another, particularly in respect of critical or financial applications, should not have any manual intervention in order to prevent any unauthorized modification. The process needs to be automated and properly integrated through a “straight through processing” methodology with an appropriate authentication mechanism and audit trails.

In the event of data pertaining to Indian operations being stored and/or processed abroad – for example, by foreign banks – there needs to be suitable controls like segregation of data and strict access controls based on “need to know” and robust change controls. The bank should be in a position to adequately prove the same to the regulator. The regulator’s access to such data/records and other relevant information should not be impeded in any manner and the RBI would have the right to cause an inspection to be made of the processing center/data center and its books and accounts by one or more of its officers or employees or other persons.

Data Protection: Analyze the SaaS provider’s data protection mechanisms, data location configuration, and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity, and availability needs of the organization that will be using the subscribed SaaS application.

Secure Data Deletion: Require that cloud service providers offer a mechanism for reliably deleting data at a consumer's request.

Application Security

Every application affecting critical/sensitive information (for example, impacting financial, customer, control, risk management, regulatory, and statutory aspects), must provide for detailed audit trails/logging capability with details like transaction ID, date, time, originator ID, authorizer ID, and actions undertaken by a given user ID. Other details like logging the IP address of the client machine, terminal identity, or location also need to be recorded. Alerts regarding use of the same machine for both maker and checker transactions need to be considered. The logs/alerts/exception reports with regard to systems should be analyzed and any issues need to be remedied at the earliest.

Any changes to an application system/data need to be justified by genuine business need and approvals, supported by documentation, and subject to a robust change management process.

For all critical applications, either source code must be received from the vendor or a software escrow agreement needs to be in place with a third party to ensure source code availability in case the vendor goes out of business. Product updates and program fixes must also be included in the escrow agreement.

Robust system security testing needs to be carried out.

A multi-tier application architecture needs to be implemented for critical e-banking systems like Internet banking which differentiates session control, presentation logic, server-side input validation, business logic, and database access.

Information Systems Acquisition, Development, and Maintenance

Banks need to carry out due diligence with regard to new technologies/systems since they can potentially introduce additional risk exposures.

Any new business products introduced, along with the underlying information systems, need to be assessed as part of a formal product approval process which incorporates, inter-alia, security-related aspects and fulfillment of relevant legal and regulatory prescriptions.

Banks need to have a documented migration policy specifying a systematic process for data migration and for ensuring data integrity, completeness, and consistency. Explicit sign-offs from users/application owners need to be obtained after each stage of migration and also after the migration process has been completed. Audit trails need to be available to document the conversion, including data mappings and transformations.

Information security assurance needs to be obtained through periodic penetration testing exercises, audits, and vulnerability assessments.

An assessment of the strengths and weaknesses of critical Internet-based applications, other critical systems, and networks needs to be carried out before each initial implementation, and at least annually thereafter. Any findings need to be reported and monitored using a systematic audit remediation or compliance tracking methodology.

Banks need to implement a "change management" process for handling any changes in technology and processes to ensure that the changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner and environment.

IT Governance, Risk Management, and Compliance

A board-approved cloud computing strategy/plan document should be created. An IT policy needs to be framed for regular management of IT functions and to ensure that detailed documentation in terms of procedures and guidelines exists and is implemented.

Risk Assessment: The core competence of information security management for a bank. The risk assessment must, for each asset within its scope, identify the threat, vulnerability combinations that have a likelihood of impacting the confidentiality, and availability or integrity of that asset – from a business, compliance, and/or contractual perspective. Risk assessments should consider not just the likelihood of threat occurrence, but the impact to the business for each risk scenario.

Audit & Compliance

Consumers have to adhere to a variety of regulations as stipulated by the respective industry regulators. Consumers, who are ultimately responsible for their data processed on providers' systems, will need to require assurances from providers that they are aiding in compliance of the appropriate regulations. This will require independent third-party audit on a regular interval basis to ensure that the provider is meeting compliance requirements on a continuous basis. Providers will have to agree on audit and investigative support, and these provisions can (and should) be made part of SLAs. Consumers also need to know the legal jurisdiction and be able to get legal remedies for any failure on the part of the provider to meet contract terms.

The audit trails should satisfy a bank's business requirements apart from regulatory and legal requirements. They should also be facilitating the conduct of audit, serving as forensic evidence when required and assisting in dispute resolution including for non-repudiation purposes. Audit trails should be secured to ensure the integrity of the information captured and preservation as evidence.

Digital evidence needs to be considered as a form of legal proof. It needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by the concerned personnel. A policy needs to be in place in this regard.

Critical functions, for example, relating to financial, regulatory, and legal, MIS, and risk management, need to be done through proper application systems and not manually or in a semi-automated manner through spreadsheets which pose risks relating to data integrity and reliability. Use of spreadsheets in this regard should be restricted and should be replaced by appropriate IT applications in a phased manner within a definite timeframe.

Security and audit processes of critical service providers/vendors need to be assessed regularly.

Commercial banks should implement globally accepted standards and best practices such as an ISO/IEC 27001-based Information Security Management System (ISMS) or one based on the O-ISM3 standard from The Open Group for their critical functions. Additionally, other reputable security/IT control frameworks may also be considered by banks.

Security Information and Event Management

Banks need to have monitoring processes in place to identify suspicious events and unusual behavioral patterns that could impact the security of IT assets.

A robust process needs to be in place for "effective malware control". Typical controls to protect against malicious code use layered combinations of technology, policies, and procedures and training. The controls are preventive and detective/corrective in nature.

There should be arrangements for monitoring and reporting of the information security condition of the organization, which are documented, agreed with top management, and performed regularly.

Given the multiplicity of devices and systems, banks should deploy suitable automated tools for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis.

Security Incident Management: A robust incident management process needs to be in place to maintain the capability to manage incidents, to enable containment of exposures, and to achieve recovery within a specified time period.

Business Continuity and Disaster Recovery (DR): Banks should plan for alternative resources if vendors have to withdraw or suspend their services.

Disaster Recovery (DR): Service providers should follow industry standards for DR site and set-up, proper processes, and perform frequent DR drills.

Service Agreement: This is another area where consumers have to ensure that all aspects of cloud services are taken care of in terms of performance, outages, penalty, DR, portability, exit provision, and data security, to name a few.

Portability and Interoperability: Consumers should be able to migrate from an existing system to the cloud, or from one service provider to another, or back to the consumer from the cloud with minimal effort. As for interoperability, consumers should be able to use other service providers' cloud services as demand requires (cloud bursting) or in situations where the cloud services of the provider are severely stressed.

People & Physical Access

Training/Awareness Programs: Training on information security for employees and vendor personnel should be performed regularly, and effectiveness of the training should be tracked.

All banks have a dedicated team to take care of the security of the physical infrastructure. This team should conduct regular security audits of various offices to check for deviations/lapses. It is the responsibility of this team to ensure that physical assets and data copied on magnetic/optical media do not go out of the offices of the bank without authorization.

Potential Areas or Opportunities for Cloud Adoption

This section describes potential areas in banking where cloud services can possibly be leveraged.

IT Infrastructure

Today Indian banks are finding ways to support banks' operations through optimal investments. Towards this, the power of cloud computing is leveraged through virtualization, consolidation, etc. Since most of the banks have already made huge investments in IT infrastructures, the tendency is more towards implementing private cloud. However, for any new investments cloud computing is considered an excellent option to avoid large IT investment upfront.

There is huge potential for Indian banks to adopt cloud computing technologies at the infrastructure layer. The cloud provides a scalable, robust, and highly available IT infrastructure to support growth and expansion plans at a fraction of the cost without the bank having to make huge capital investments.

Core Banking

The changes in banking and regulatory requirements have driven Indian banks today to implement a Core Banking Solution (CBS). This solution requires an IT infrastructure aligned to the bank's business growth plan and one that meets the bank's DR requirements.

Core banking is one of the toughest workloads to migrate onto the cloud. However, within core banking there can be specific workloads which can be migrated which are mostly around the customer servicing area, such as:

- Cash management
- Know Your Customer (KYC) validation
- Credit rating business process
- Anti-money laundering check
- Regulatory and compliance reporting which is generated out of core banking

These workloads peak at specific time periods in a day and the usage remains flat most of the day. A better return on investment can be obtained by approaching this model. The core transactional engine can still remain in-house so that there is no risk involved with respect to cloud computing.

Many banking software vendors have started offering their CBSs on the cloud today. Considering the growing demands from small, mid-size, and co-operative banks the solutions offered on the cloud are going to get better and will see increased implementation on the ground.

Customer Relationship Management (CRM)

CRM is already a common candidate for cloud computing and most banks already have CRMs deployed on the cloud (e.g., Salesforce.com). The key CRM functions are as follows:

- Customer management and on-boarding
- Customer analytics
- Agent/business correspondent management
- Customer servicing

CRM is one of the least risky applications which can be migrated to the cloud. The benefits are as follows:

- Most cloud CRM vendors provide multi-channel access which can be leveraged from day one
- Time to go-live is almost zero
- Attractive pricing and advantage to use the latest trends and features which arise in the CRM space

Mobile Banking

Mobile applications are ideally suited to running in the cloud because it is often infeasible to connect mobile clients directly into internal systems, whereas all mobile clients can readily connect to publicly available cloud services. Banks are now offering mobile applications to online banking customers and partners for checking balances, ordering new check books, or stopping payment orders.

Business Analytics

The information management layer is another key candidate for cloud adoption. The usage of analytics, warehouse, and reporting platform is almost flat throughout the day except for the end-of-day operations where there is peak usage as most operational, regulatory, statutory branch reports are generated. Most customer segmentation and analytical models will be run during business hours except for real-time campaign management where there is a need for real-time analytical output. The usage pattern between the following platforms can be optimized through the use of cloud computing:

- Analytics
- Warehouse
- Campaign management
- Reporting

Another best practice is to have this environment operational in the DR cloud which would help achieve further reduction in the IT footprint of the banks.

Corporate Functions

Human Resources (HR)

Managing HR is not seen as a business function that provides any significant competitive advantage to a bank. In fact, all processes around HR are mostly common across many types of industry verticals. Cloud-based HR applications (SaaS) are available that cover the entire process cycle of HR; e.g., recruitment, talent management, compensation management, payroll, and exit management.

Procurement

The entire value chain of procurement makes a suitable candidate for the cloud for the following reasons:

- Cloud applications are based on industry best practices and hence can result in more efficient, transparent processes.
- Cloud applications for procurement provide rich functionalities; e.g., reverse auctions, and portals for vendors.
- Cloud applications for procurement have standard integration options for account payable modules within all standard ERP packages.

Learning Management System (LMS)

The elasticity offered by the cloud provides a distinct advantage in LMSs, as costs incurred are only on a pay-per-use basis as against CAPEX incurred for on-premise solutions. Other benefits are:

- Standardization of content type (SCORM) makes it easy for switching between cloud service providers.
- LMS cloud service providers offer huge repositories of ready-made learning content spread across several topics; e.g., leadership, management, soft skills, etc.

Intranet

Sourcing the intranet platform on the cloud for employee collaboration, knowledge management has the following distinct advantages:

- Avoidance of huge infrastructure costs for intranet development, UAT, production systems
- Reduced time-to-market with standard, configurable features
- Rich features (web 2.0, social media connect) on the intranet

Email Service

Cloud service providers can offer email services and management. With the necessary security levels to meet compliance requirements, banks can outsource email to cloud service providers. This is an attractive option for banks as it provides lower-cost operating models and the ability to scale this non-core function as per the requirement.

Back-Office Operations and Infrastructure

Back-office operations deal with customer transactions carried/emanating from the branches of a bank including the verification of the various details of transactions, scrutinizing the allied documentation and inputting the details in the related systems/core banking systems. Cloud service providers' support for back-office operations may include:

- A mechanism to upload the scanned documents into the cloud service
- Instant access to all documents from anywhere with an Internet connection and on different devices
- A secure, centralized location for information

- Ensured compliance with government regulation through permanent online document storage
- Mechanism to provide metadata to the content uploaded
- Indexing for faster search of the content and search options to search content
- Strict enforcement of access control to the uploaded documents

Other Key Systems – Integration and Considerations

1. **Aadhaar**: Unique Identification Authority of India (UIDAI) offers a range of authentication services that enable a resident to authenticate themselves by providing relevant identity information such as demographics, biometrics, and One-Time Pin (OTP). Aadhaar-enabled applications primarily use electronic systems to deliver services. These applications are expected to be used in government as well as other sectors. Indian banks are adopting Aadhaar authentication to identify and authenticate the resident as part of their service delivery.

2. **Payment Gateway**: In payment gateway systems, only the last four digits of credit card numbers, debit card numbers, or account numbers are available. Some specific card validations may be performed, such as setting validation masks for cards (before sending a card for approval it is checked for a validation mask and if it succeeds, only then is it sent for approval).

3. **Inter-Bank Systems**: The inter-bank payment system consists of the Inter-Bank Clearing System (IBCS) and the Settlement Accounting Processing System (SAPS).

4. **Inter-Bank Clearing System (IBCS)**: The IBCS handles the clearing of all domestic electronic inter-bank payments. The IBCS comprises a Low-Value Sub-System (LVSS) and a High-Value Sub-System (HVSS). It is envisaged that in time HVSS will be used for time-critical high-value payments, and that LVSS will become predominantly a bulk payments system. Clearing of LVSS payments is conducted at a central clearing center or regional clearing center located in the main cities. Clearing of HVSS payments should be performed in real-time by the SAPS located at the Central Bank.

5. **Settlement Accounting Processing System (SAPS)**: SAPS interacts with systems, initially just the IBCS, that require settlement of inter-bank payments. SAPS holds and maintains the centralized settlement accounts which are an integral part of the inter-bank payment system. The central administration workstation is located in Central Bank and has general settlement account creation, monitoring, and amendment facilities; the head office of each bank will be able to monitor its own banks’ settlement account. SAPS supports two settlement mechanisms: Real-Time Gross Settlement (RTGS) of time-critical high-value electronic payments, and periodic net settlement of low-value electronic and paper-based payments. SAPS processing is conducted at the Central Bank.

6. A timetable for the processing of inter-bank payments on a typical business day should be defined. Each bank will, subject to certain rules, choose how and when to enter inter-bank payment instructions into the IBCS. It will also be able to decide whether an individual credit payment is to be entered into HVSS or LVSS. Clearing and settlement cycles for inter-bank payments will vary, as follows: high-value credit payments in HVSS will be cleared and settled immediately provided that there are sufficient funds on the originating (i.e., the payer) bank’s settlement account; low-value credit payments and pre-authorized debit payments in LVSS will generally be cleared and settled at the end of the business day. In defined circumstances, clearing and settlement will also occur at other times. Thus,

there will be same-day settlement of low-value payments provided that payment instructions are entered into LVSS before the cut-off time.

Solution Architecture and Components

Figure 4 provides an end-to-end perspective of the banking architecture for a typical bank in India.

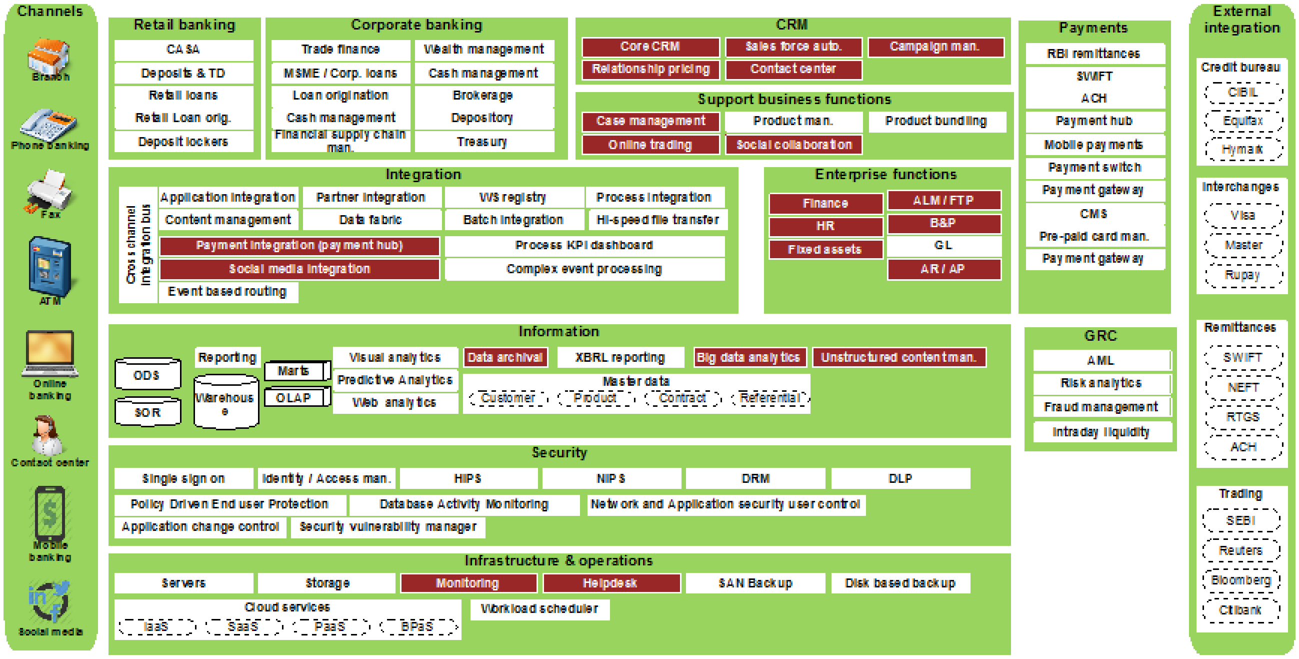

Figure 4: Typical Banking Solution Architecture

The potential cloud computing workloads have been highlighted. However, the ISMS policies of different banks would dictate different workloads. Banking Workloads for Cloud (below) provides typical workloads.

Banking Workloads for Cloud Computing

Following is a priority list of candidate applications in FIs to consider moving to cloud computing:

1. Common Services – corporate functions (Finance, HR, Marketing, Legal), enterprise content management, enterprise integration services, governance risk and compliance
2. Customer Analytics and CRM – sales force management, campaign and communication, analytics, performance management, customer information
3. Delivery Channels – mobile applications, Internet banking, branch, ATM, telephone/IVR, POS/merchant, call center, kiosk
4. Client Sales and Servicing – accounts, charges, statements, credits, transaction servicing, complaint management, communication management, query management, relationship management, collateral management
5. Payments
6. Retail Banking Platforms, Core Banking
7. High Performance Computing
8. IT Development – application development and maintenance, technology management
9. Application Infrastructure – application technology components, infrastructure components
10. Credit Risk Analysis
11. Websites, Email, Workforce Productivity
12. Trade Settlement

Batch Workloads

Typical batch workloads tend to process huge volumes of data such as the number of fund transfer transactions in a particular period of the day. Generally, batch workloads are executed on a regular schedule. A public cloud environment may be a good choice for handling these batch workloads.

Transactional Workloads

Transactional workloads emerge from the automation of business processes. In a banking environment, retail banking, corporate banking, investment banking, and treasury applications generate transactions. These transactions are customer-facing and highly critical involving financial data. These critical transactional workloads are best suited to a private cloud.

Analytical Workloads

Banks may intend to use analytical services in a cloud computing environment to make sense of the vast amounts of data for different purposes including CRM and fraud analytics. Most of these workloads are not in real-time environments.

Database Workloads

Database workloads are the most common type of workload. Most of the banks may prefer to rely on a private cloud where data is not exposed externally.

Database environments account for significant cost in the overall core banking environment. Due to business reasons, banks at an average would have 10-15 test environments for individual business units, migration, etc., and not all of them would be loaded at the same point in time. A good cloud usage scenario would be to have a test/development cloud wherein a consolidated compute capacity is available for business and can be allocated as desired at different points in time.

Risk Assessment for Banking Workloads

Workloads to be considered for deployment to cloud services should undergo a risk assessment. It is important to understand the risks specific to each workload, and to each cloud service deployment scenario. Risk assessments should explore specific risk scenarios, and should take into account the probability of occurrence as well as the impact of the risk scenario. The different types of applications, workloads, and data will necessarily present different risks.

For each of the workloads mentioned above, risk assessments should take into account the relevant impact of a loss event, and they should do so in the context of the type of cloud service deployed, or being considered.

Batch, transaction, and database workloads with high volumes of data can have large impacts due to loss of availability (if, for example, the cloud service had downtime). Similarly, another threat or risk scenario, theft of information, could have significant impact.

Analytical workloads would likely have impacts that are not as severe as the other workload types, in the event of loss of availability.

In each risk scenario to be considered, it is important to identify such factors as threat actors, contact frequency, threat capability, control strength, vulnerability, and loss magnitude in analyzing risk. It is also important to evaluate each of these in the context of the cloud type, whether IaaS, PaaS, or SaaS, and whether the cloud service is public, private, or hybrid, as these will have significant influence on the risks.

Useful references to help prepare a solid risk analysis for cloud computing workloads include The Open Group Risk Taxonomy Standard (O-RT) and Risk Analysis (O-RA) standards.

Selecting Appropriate Deployment and Delivery Models

Cloud services function at different layers, and include varying types of functionality. Figure 5 shows relevant banking applications positioned as IaaS, PaaS, or SaaS cloud services.

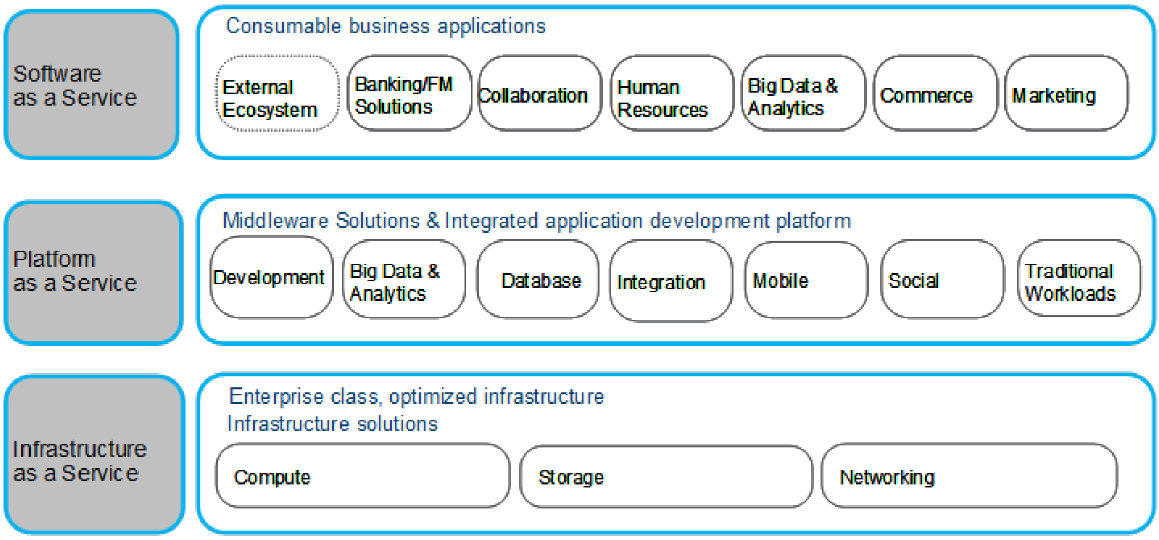

Figure 5: Workloads and Cloud Service Model

Choosing an appropriate target cloud computing delivery model involves considering many variables and weighs cost *versus* risk. As shown in Figure 6, cloud services which are private in nature provide higher levels of control, while public cloud services can provide lower costs.

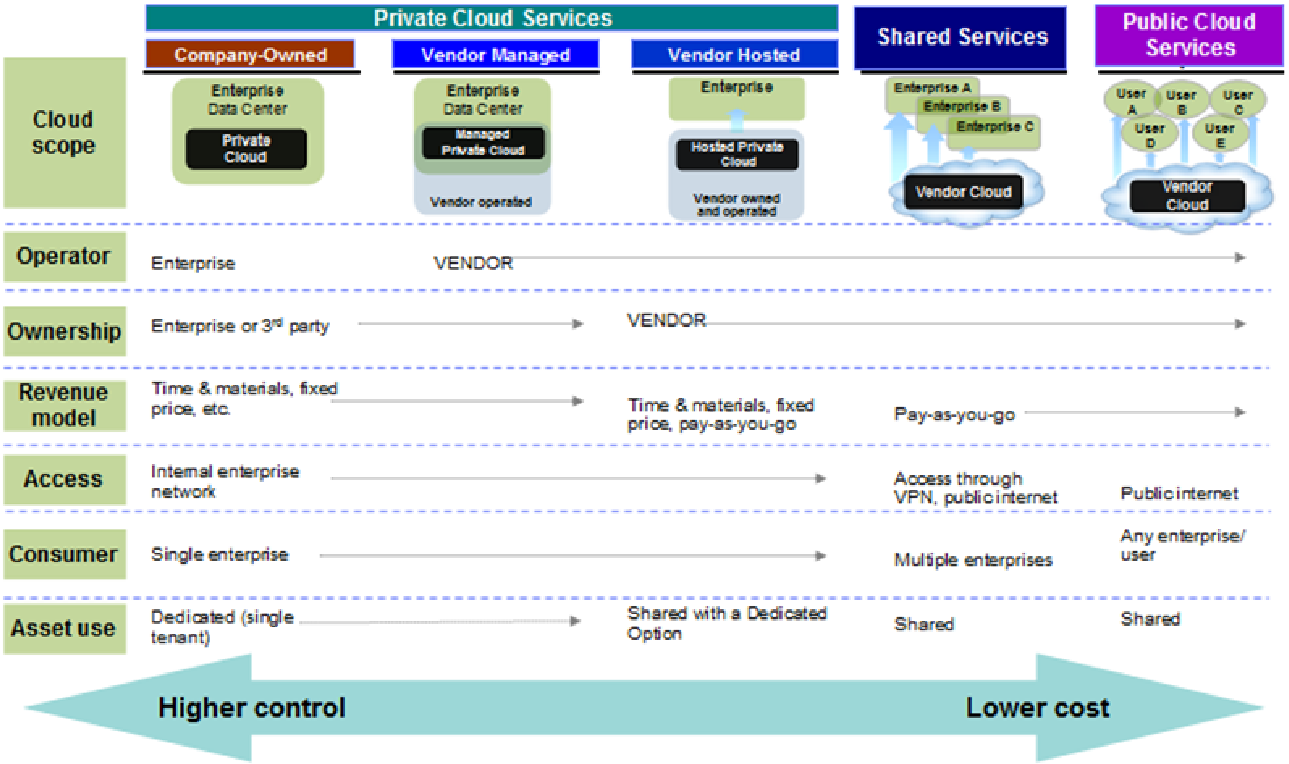

Figure 6: Private, Shared, and Public Cloud Services

In the initial phases of cloud adoption, it is expected that banks will own and operate the cloud themselves with service providers taking increasing ownership and control of the cloud infrastructure as cloud computing matures and more rigorous controls become available. Banks should go with a hybrid model; private clouds for sensitive data and public cloud to store other information. Security concerns deter moving critical banking applications to the public cloud. Public cloud services can play a big role in banks' horizontal and back-office processes not directly involved in sensitive customer data.

Service Development

Component	Potential Cloud Solution	Comments
Application Development	Public cloud	PaaS and SaaS delivery model. Will start off as Private cloud and evolve into Community or Public model; most possibly delivered by the IT service provider.
Application Assurance	Private cloud	
Development Infrastructure	Private and/or Public cloud supporting multiple technology platforms	
Technology Proofing & Selection	Public and/or Community clouds the IT service provider provided by IT/Technology vendors	
Service Proofing & Selection	Community clouds set up by service vendors	

Customer Services

Component	Potential Cloud Solution	Comments
ATM, Kiosk, Call Center	Private cloud delivering services across the global enterprise	SaaS delivery model. Service standardization across these channels. Differentiation is delivered by product features then channel capabilities.
Branch, Online Functions	Private cloud supporting standard functional suite	SaaS delivery model. Potential for core banking providers to offer Community cloud solutions product features then channel capabilities.
Mobile-based Functions	Private cloud supporting standard functional suite	SaaS delivery model. Diversity of devices, carriers, and technologies will enable common solutions rather than individual investments.
Content Management	Private cloud delivering enterprise-wide services	SaaS delivery model. Potential for technology vendors to deliver Public cloud solutions.

Component	Potential Cloud Solution	Comments
Business Partner-delivered Functions	Public cloud delivering software applications	SaaS-based delivery model. Functionally and usage-rich applications. Seamlessly integrated with internal services.

Core Business Services

Component	Potential Cloud Solution	Comments
Core Account Engines Lending Services (Retail & Commercial)	No movement from the banking institutions on core engines	Potential opportunity for COTS providers to offer Community/Public cloud-based solutions. Parts of the process like origination, KYC, customer on-boarding, collections, etc. would become business-enabling services.
Cards & Payment Services	Private clouds delivered by service providers	SaaS delivery model. The migration to a cloud-based model will be incremental with different aspects of card processing moving to cloud-based solutions.
Wealth & Investment Management Services *and* Investment Banking Services	No movement from the banking institutions on products and advisory services	Niche and high revenue portfolio; parts of the service portfolio will be split into business-enabling services which could be delivered from the cloud (reconciliation, reference data, etc.).
Trading & Market Infrastructure	No change	Highly mature, capacity-intensive at the same time as high revenue and compliance impact.
Governance, Risk Management, and Compliance Services	Private cloud	Moving towards enterprise coverage and seamless integration across the three practices. Standardization, coverage, and cost pressures will force a cloud-based model.

Business-Enabling Services

Component	Potential Cloud Solution	Comments
Origination	Private and/or Community cloud	SaaS delivery model. Covering account management, documentation, collateral, validation, underwriting and fulfillment, fraud management, and AML.

Component	Potential Cloud Solution	Comments
Transaction Processing	Initiating as Private clouds, with potential to become Public based on the commodity nature of the functional services	SaaS delivery model. Funds management, cheque processing, payments, chargeback, authorization and interchange settlement, corporate actions, custody operations, treasury operation, and portfolio management.
Customer Servicing	Private cloud	Enquiries, exception management, and informational service delivery, fraud management, and AML. Organization-specific services that enable differentiation like cross-sell/up-sell, product/service reconfiguration, etc.
Reference Data Management	Private cloud	SaaS model. Private services managing internal enterprise reference information, seamlessly integrated with the external reference information including market data, price, corporate actions, and ratings.
Collections and Reconciliation	Initiating as Private clouds, with potential to become Public based on the commodity nature of the functional services	Full range of services with technology, applications, and operations delivered on SaaS model internally. Covering standard reporting and analytics requirements.
Analytics & Reporting	Private cloud	Covering performance analytics, competitive analytics, predictive analytics, segmentation and behavior analytics, etc. that enable differentiation.

Securing Banking Applications on the Cloud

Laws and regulations currently in place in India restrict banks and other financial organizations from placing certain kinds of applications and customer data in shared computing services such as cloud computing.

As is the case elsewhere in the world, laws and regulations in India will have to evolve to address the desired use of cloud services in the financial sector. The RBI Working Group Report on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds, which looked at information security issues in electronic banking for financial services organizations in India, contained this high-level suggestion relative to cloud computing:

"Given that control, security, and legal issues on cloud computing are still evolving, a bank needs to be cautious and carry out due diligence to assess the risks comprehensively before considering cloud computing."

The Report also provided some useful information about the perceived benefits of cloud computing and concerns about cloud computing, which focused primarily on security and privacy concerns. These are reprinted in Appendix A: Cloud Computing Concerns. Beyond the changes required in laws and regulations, it is clear that for cloud computing to succeed in the financial sector in India, cloud services will need to address the set of concerns identified in the Report, as well as others.

The balance of this section explores the security considerations applicable to the two most common forms of cloud services: IaaS and SaaS.

Security Considerations for IaaS and SaaS

In the case of SaaS-based cloud services, customers typically have less ability to deploy security controls directly into the cloud computing environment. This means that to satisfy their security requirements, customers planning to use SaaS services need to request necessary security capabilities as a part of an RFP process, and then ensure that their contracts and SLAs contain appropriate provisions regarding those security controls, including "right to audit" clauses.

Another approach to securing information in SaaS cloud services is to use third-party security gateways. These are generally deployed as proxy devices that sit between the customer's network and the cloud service. Common functions for these gateways are data encryption and access control. These security gateways provide a means to add a level of security that augments that provided by the cloud service provider, and (in the case of data encryption) to do so in a way in which the cloud computing customer controls the encryption keys.

With IaaS cloud services, customer organizations have a greater degree of responsibility for deploying security controls. A couple of examples illustrate this point. If the customer's intended use of an IaaS cloud service requires the deployment of an application with a multi-tier web architecture, and the security requirements dictate that the data be encrypted in the cloud computing environment, or that a web application firewall be deployed to control web access to the application, the customer organization will need to deploy these controls to their cloud computing environment (and manage these security controls).

Possible security controls that may be deployed into IaaS and SaaS cloud computing infrastructures are shown along with a description of their relevance in each environment in Appendix B: Security Controls for IaaS and SaaS Cloud Services.

Relationship to Other Activities

There are a few other initiatives in India that relate to cloud usage by the banking sector. These include a study and report undertaken by the Institute for Development and Research in Banking Technology (IDRBT), a report put forth by the IEEE on cloud usage for emerging markets, and an Indian state data center initiative.

The IDRBT report, Cloud Security Framework,[10] provides a good overview of cloud service types, key security issues, legal issues, and guidance on best practices and organizational and operation security considerations.

The IEEE document, IDRBT Community Cloud for Indian Banks,[11] describes a pilot approach to providing community clouds for Indian banks.

Beyond these initiatives in India, the UK Government G-Cloud Initiative can also be studied regarding the issues/challenges and how to overcome them in sourcing cloud services.

The UK Government G-Cloud is an initiative targeted at easing procurement by public sector bodies in departments of the UK Government of commodity IT services that use cloud computing. The G-Cloud consists of:

- A series of framework agreements with suppliers, from which public sector organizations can call off services without needing to run a full tender or competition procurement process
- An online store – the “CloudStore” – that allows public sector bodies to search for services that are covered by the G-Cloud frameworks

The service began in 2012, and had several calls for contracts. By May 2013 there were over 700 suppliers – over 80% of which are small and medium enterprises. £18.2 million (US$27.7 million) of sales were made by April 2013. With the adoption of the Cloud First policy in the UK in late February 2014, sales have continued to grow, reportedly hitting over £50M in February 2014. These are based on procurement of some 1,200 providers and 13,000 services, including both cloud services and (professional) specialist services as of November 2013 (Source: Wikipedia).

More details from a law and regulatory perspective can be found in Chapter 5: Public Sector and Cloud Contracts in Christopher Millard’s book: Cloud Computing Law.

[10] Refer to the IDRBT Report: Cloud Security Framework for Indian Banking Sector.

[11] Refer to the IEEE Report: Indian Banking Community Cloud (IBCC).

Appendix A: Cloud Computing Concerns

(This text is reprinted from the RBI Working Group Report on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds.)

Perhaps the biggest concerns about cloud computing are security and privacy. The idea of handing over important data to another company worries some people. Corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under lock and key.

Privacy is another matter. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing companies will need to find ways to protect client privacy by implementing reliable authentication techniques.

A cloud computing system must ensure backup of all its clients' information.

Some questions regarding cloud computing are more legal. Does the user or company subscribing to the cloud computing service own the data? Does the cloud computing system, which provides the actual storage space, own it? Is it possible for a cloud computing company to deny a client access to that client's data? Several companies, law firms, and universities are debating these and other questions about the nature of cloud computing. Thus, there are issues relating to data security and privacy, compliance, and legal/contractual issues.

A few examples of cloud computing risks that need to be managed include:

- Enterprises need to be particular in choosing a provider. Reputation, history, and sustainability should all be factors to consider. Sustainability is of particular importance to ensure that services will be available and data can be tracked.
- The cloud service provider often takes responsibility for information handling, which is a critical part of the business. Failure to perform to agreed service levels can impact not only confidentiality but also availability, severely affecting business operations.
- The dynamic nature of cloud computing may result in confusion as to where information actually resides. When information retrieval is required, this may create delays.
- The geographical location of data storage and processing is not definite unlike traditional data centers. Trans-border data flows, business continuity requirements, log retention, data retention, and audit trails are among the issues that contribute to compliance challenges in a cloud computing environment.
- Third-party access to sensitive information creates a risk of compromise to confidential information. In cloud computing this can pose a significant threat to ensuring the protection of IP, trade secrets, and confidential customer information.
- The contractual issues in the cloud services can relate to ownership of IP, unilateral contract termination, vendor lock-in, fixing liability, and obligations of cloud service providers, exit clause, etc.
- Public clouds allow high-availability systems to be developed at service levels often impossible to create in private networks, except at extraordinary costs. The downside to this availability is the potential for

commingling of information assets with other cloud computing customers, including competitors. Compliance to regulations and laws in different geographic regions can be a challenge for enterprises. At this time there is little legal precedent regarding liability in the cloud. It is critical to obtain proper legal advice to ensure that the contract specifies the areas where the cloud service provider is responsible and liable for ramifications arising from potential issues.

- Due to the dynamic nature of the cloud, information may not immediately be located in the event of a disaster. Business continuity and DR plans must be well documented and tested. The cloud service provider must understand the role it plays in terms of backups, incident response, and recovery. Recovery time objectives should be stated in the contract.

Service providers must demonstrate the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change, and destruction. Key questions to address are: What employees (of the provider) have access to customer information? Is segregation of duties between provider employees maintained? How is different customers' information segregated? What controls are in place to prevent, detect, and react to breaches?

Appendix B: Security Controls for IaaS and SaaS Cloud Services

The security control matrix below identifies various security controls that may be considered for cloud services. For each control, the source of the control requirement in Indian law, regulation, or guidance is noted (where applicable), and the relevance of the control to IaaS and SaaS-based cloud services is noted.

Note: This categorization and set of specific cloud computing security controls is based upon those defined in the Cloud Security Alliance Critical Controls Matrix.

Table 1: Security Control Matrix

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
Compliance	Audits	Audit plans, independent audits, and third-party audits.	IT Amendment Act, 2008	✔	✔
	Liasons, Contact with Authorities	Contacts with relevant authorities to be maintained in accordance with laws, regulations, and contractual requirements.		✔	✔
	Regulatory Mappings	Requirements stemming from statutes, regulations, and contracts to be defined, and mapped to information systems.	IT Act, 2000 IT Amendment Act, 2008	✔	✔
	Intellectual Property	Controls including policies, process, and procedures to safeguard IP, and the use of proprietary software.		✔	✔
Data Governance	Ownership, Stewardship	Controls to designate stewardship and assigned responsibilities for data.		✔	✔
	Classification	Controls to classify data based on type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality, and third-party obligations.	IT Act, 2000 IT Amendment Act, 2008	✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Handling and Labeling	Controls to create polices and procedures for handling, labeling, and security of data and objects which contain data.			✔
	Retention Policy	Controls establishing policies and procedures for data retention and storage.	IT Act, 2000 IT Amendment Act, 2008	✔	✔
	Secure Disposal	Controls creating policies and procedures and mechanisms for the secure disposal and complete removal of data from all storage media.		✔	✔
	Non-production Data	Controls including policies and procedures that prevent production data from being used in non-production environments.			✔
	Information Leakage	Controls (technical or process) that prevent data leakage.			✔
	Risk Assessments	Data governance risk assessments conducted at regular intervals, the goals of which are to identify where sensitive data is stored and transmitted, and to ensure compliance with retention periods and end-of-life policies, and to ensure that data is classified and protected from unauthorized use.	RBI Working Group UCBs Gopalakrishna Committee Report	✔	✔
Facility Security	Policy	Controls including policies and procedures to maintain a safe and secure working environment.		✔	✔
	User Access	Controls limiting access to data and information assets in the facility to authorized users.	IT Amendment Act, 2008 (§79)	✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Controlled Access Points	Physical security controls including fences, walls, barriers, guards, gates, physical authentication mechanisms, reception desks, etc. put in place to safeguard sensitive data.		✔	✔
	Secure Area Authorization	Controls to secure ingress and egress points.		✔	✔
	Unauthorized Persons Entry	Controls to monitor ingress and egress points such as service areas where unauthorized personnel may enter the premises, and to isolate unauthorized persons from data storage and processing facilities.		✔	✔
	Off-site Authorization	Controls requiring authorization prior to relocation or transfer of hardware, software, or data to an off-site premises.		✔	✔
	Off-site Equipment	Controls including policies and procedures for security and asset management for use/disposal of equipment used outside the organization's premises.		✔	✔
	Asset Management	Inventory of critical assets maintained with ownership, defined, and documented.		✔	✔
Human Resources	Background Screening	Subject to local laws, performing background verification of employees, contractors, and third-party users.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Employment Agreements	Requiring employment agreements, which specify information security responsibilities for employees, contractors, and third parties, and which are required before granting access.		✔	✔
	Employee Termination	Controls specifying responsibilities for performing employment termination, or change in employment procedures.		✔	✔
Information Security	Management Program	An Information Security Management program has been developed, documented, approved, and implemented including administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction.		✔	✔
	Management Support/ Involvement	Executive and line management support for information security through documented direction, commitment, explicit assignment, and verification of implementation.		✔	✔
	Policy	A formal information security policy document, approved by management, is communicated and published to employees, contractors, and third parties.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Baseline Requirements	Baseline security requirements are established and applied to the design and implementation of applications, databases, systems, and network infrastructure and information processing. Compliance with security baseline requirements must be reassessed annually or upon significant changes.		✔	✔
	Policy Reviews	Management review of the information security policy at intervals or as a result of changes to the organization.		✔	✔
	Policy Enforcement	Control includes a formal disciplinary or sanction policy for employees who have violated security policies and procedures.		✔	✔
	User Access Policy	Requires user access policies and procedures, documented, approved, and implemented for granting and revoking access to applications, databases, and server and network infrastructure.		✔	✔
	User Access Restriction/ Authorization	Control requires user access to applications, systems, databases, network configurations, and sensitive data and functions to be restricted and approved by management. In the context of the Indian banking sector, this may also include use of the Aadhaar user authentication capability.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	User Access Revocation	Requires timely deprovisioning, revocation, or modification of user access to systems, information assets, and data upon change in status of the employee, contractor, or third party.		✔	✔
	User Access Reviews	Management review of levels of user access, at planned intervals and documented.		✔	✔
	Training/ Awareness	For all contractors, third-party users, and employees of the organization a security awareness training program shall be established. All individuals with access to organizational data shall receive appropriate awareness training updates.		✔	✔
	Industry Knowledge/ Benchmarking	Networking, specialist security forums, and professional associations shall be used to maintain industry security knowledge and benchmarking.		✔	✔
	Roles/ Responsibilities	Contractor, employee, and third-party user roles and responsibilities shall be documented relating to information assets and security.		✔	✔
	Management Oversight	Requires managers to develop awareness of and compliance with security policies, procedures, and standards that are relevant to their area of responsibility.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Segregation of Duties	Controls include policies, process, and procedures to enforce and assure proper segregation of duties. May include technical controls to mitigate any risks arising from unauthorized or unintentional modification or misuse of the organization's information assets.		✔	✔
	User Responsibility	Control requires users to be aware of responsibilities for: • Maintaining awareness and compliance with published security policies, procedures, and standards • Maintaining a safe and secure working environment • Securing unattended equipment		✔	✔
	Workspace	Control requires policies and procedures for clearing visible documents containing sensitive data when a workspace is unattended and enforcement of workstation session logout for a period of inactivity.		✔	✔
	Encryption	Control requires policies, procedures, and mechanisms for encrypting sensitive data in at-rest and in-transit		✔	✔
	Encryption Key Management	Requires policies, procedures, and mechanisms for effective key management to support encryption of data.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Vulnerability/ Patch Management	Requires policies and methods for vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated and vendor-supplied security patches are applied in a timely manner.		✔	✔
	Anti-virus/ Malicious Software	Control requires anti-malware programs to be capable of detecting, removing, and protecting against malicious or unauthorized software, with antivirus signature updates at least every 12 hours.		✔	✔
	Incident Management	Policies and procedures shall be established to triage security-related events and ensure timely and thorough incident management.		✔	✔
	Incident Reporting	Reporting information security events in a timely manner. All contractors, employees, and third-party users must be aware of their responsibility.	ITAA, 2008 (§79)	✔	✔
	Incident Response Legal Preparation	Forensic procedures including chain of custody shall be required for collection, retention, and presentation of evidence to support potential legal action subject to the relevant jurisdiction, in the event that a follow-up action after an information security incident requires legal action.		✔	✔
	Incident Response Metrics	Monitoring and quantifying the types, volumes, and costs of information security incidents.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Acceptable Use	Policies and procedures are developed, approved, and published for the acceptable use of information assets.		✔	✔
	Asset Returns	Return of all assets owned by the organization within a defined and documented timeframe once the employment, contract or agreement has been terminated, for employees, contractors, and third-party users.		✔	✔
	e-Commerce Transactions	e-Commerce-related data traversing public networks should be classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner as to prevent contract dispute and compromise of data.		✔	✔
	Audit Tools Access	Audit tools that interact with the organization's information systems shall be segmented and restricted to prevent compromise and misuse of log data.		✔	✔
	Diagnostic/ Configuration Ports Access	Access to diagnostic and configuration ports shall be restricted to authorized individuals.		✔	✔
	Network/ Infrastructure Services	SLAs (in-house or outsourced) shall clearly document security controls, capacity and service levels, and business or customer requirements.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Portable/ Mobile Devices	Control requires policies and procedures and measures implemented to limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and PDAs.		✔	✔
	Source Code Access Restriction	Access to application, program, or object source code shall be restricted to authorized personnel on a need-to-know basis. Records shall be maintained regarding the individual granted access, reason for access, and version of source code exposed.		✔	✔
	Utility Programs Access	Control requires that access to utility programs capable of overriding system, object, network, VM, and application controls be restricted.		✔	✔
Legal	Non-disclosure Agreements	Requires non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data.	ITAA, 2008 (§79)	✔	✔
	Legal, Third-party Agreements	Requires that third-party agreements, which impact the organization's information assets, shall include explicit coverage of all relevant security requirements.	ITAA, 2008 (§79)	✔	✔
Operations Management	Policy	Requires policies and procedures for all personnel to adequately support the services operations role.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Documentation	Requires system documentation (e.g., administrator and user guides, architecture diagrams, etc.) be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features		✔	✔
	Capacity/ Resource Planning	Requires that availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with regulatory, contractual, and business requirements.		✔	✔
	Equipment Maintenance	Requires policies and procedures to be established for maintenance, ensuring continuity and availability.		✔	✔
Risk Management	Program	Develop and maintain an ERM program to manage risk to an acceptable level.	RBI Working Group UCBs Gopalakrishna Committee Report	✔	✔
	Assessments	Risk assessments shall be performed at regular intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods.	RBI Working Group UCBs Gopalakrishna Committee Report	✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Mitigation/ Acceptance	Risk decisions shall be taken based upon risk assessments, with risks mitigated to acceptable levels, or accepted based on risk criteria.	RBI Working Group UCBs Gopalakrishna Committee Report	✔	✔
	Business/ Policy Change Impacts	Requires that risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain effective.	RBI Working Group UCBs Gopalakrishna Committee Report	✔	✔
	Third-party Access	Identification, assessment, and prioritization of risks posed by business processes requiring third-party access to information systems and data. Organizations shall apply resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access.	RBI Working Group UCBs Gopalakrishna Committee Report	✔	✔
Release Management	New Development/ Acquisition	Requires management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities.		✔	✔
	Production Changes	Requires changes to the production environment to be documented, tested, and approved prior to implementation.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Quality Testing	Requires monitoring and evaluation to ensure that standards of quality are being met, and that quality evaluation and acceptance criteria for information systems, upgrades, and new versions are established, documented, and tested.		✔	✔
	Outsourced Development	Systematic monitoring and evaluation for all outsourced software development must include security requirements, independent security review of the outsourced environment, certified security training for outsourced software developers, and code reviews.		✔	✔
	Unauthorized Software Installations	Policies, procedures, and mechanisms to restrict the installation of unauthorized software.		✔	✔
Resiliency	Management Program	Business continuity and DR policies, processes, and plans. The resiliency management program shall be communicated to all organizational participants on a need-to-know basis prior to adoption and shall also be published, hosted, stored, recorded, and disseminated to multiple facilities, which will be accessible in the event of an incident.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Impact Analysis	A method for determining the impact of disruption to the organization: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third-party service providers • Understand threats to products and services • Determine impacts resulting from planned or unplanned disruptions • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives • Estimate the resources required for resumption		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Business Continuity Planning	Business continuity plans include: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures • Method for plan invocation		✔	✔
	Business Continuity Testing	Business continuity plans shall be tested periodically to ensure effectiveness.		✔	✔
	Environmental Risks	Protective controls against damage from natural causes and disasters as well as deliberate attacks.		✔	✔
	Equipment Location	Equipment should be located away from high-probability environmental risks, and supplemented by redundant equipment located a reasonable distance away from environmental threats, hazards, and opportunities for unauthorized access.		✔	✔
	Equipment Power Failures	Controls and security mechanisms and redundancies to protect equipment from utility service outages (e.g., power failures, network outages, etc.).		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Power/ Telecomm-unications	Telecom equipment and cabling shall be protected from interception or damage and designed with redundancies, alternative power sources, and alternative network routing.		✔	✔
Security Architecture	Customer Access Requirements	Requirements for customer access (including contractual and regulatory) should be addressed prior to allowing access.		✔	✔
	User Identity Credentials	User credential and password controls for applications, databases, and server and network infrastructure should be implemented. These controls should address resets, password expiration, password reuse, password strength, lockout durations, and other parameters affecting security.		✔	✔
	Data Security/ Integrity	Ensure security through encryption, access controls, and data leakage prevention, and ensure the integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third-party shared service provider to prevent improper disclosure, alteration, or destruction complying with legislative, regulatory, and contractual requirements.		✔	✔
	Application Security	Use industry accepted security standards (i.e., OWASP for web applications) to ensure application security.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Data Integrity	Deploy data input and output integrity routines (i.e., reconciliation and edit checks) for application interfaces and databases to prevent errors.		✔	✔
	Production/ Non-production Environments	Separate production and non-production environments.		✔	✔
	Remote User Multi-factor Authentication	Use multi-factor authentication where appropriate for all remote user access. In the context of the Indian banking sector, the Aadhaar identity and authentication mechanism provides this capability.		✔	✔
	Network Security	Network environments should be designed and configured to restrict connections between trusted and untrusted networks. Network access should be reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale and compensating controls. Network architecture diagrams should identify high-risk environments and data flows that may have regulatory compliance impacts.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Segmentation	Network and system components should be separated by firewalls to facilitate these requirements: • Business and customer requirements • Security requirements • Compliance, legislative, regulatory, and contractual requirements • Separation of production and non-production networks and systems • Protect and isolate sensitive data		✔	✔
	Wireless Security	Implement policies, procedures, and mechanisms to protect wireless environments.		✔	✔
	Shared Networks	Restrict access to systems with shared network infrastructure to authorized personnel in accordance with security policy.		✔	✔
	Clock Synchronization	Synchronize system clocks of information processing systems within the organization to an external accurate time source.		✔	✔
	Equipment Identification	Use automated equipment identification as a method of connection authentication.		✔	✔

Category	Controls	Description	Control Requirement Source (India law, regulation, guidance)	Relevant to SaaS?	Relevant to IaaS?
	Audit Logging/ Intrusion Detection	Maintain audit logs recording user access activities, authorized and unauthorized access attempts, system exceptions, and information security events. Retain logs per security policies. Analyze logs periodically, and restrict access to log files.		✔	✔
	Mobile Code	Prevent unauthorized mobile code from executing.		✔	✔

Abbreviations and Acronyms

AML	Anti-Money Laundering
ATM	Automated Teller Machine
B2C	Business to Consumer
BAU	Business As Usual
BFSI	Banking, Financial Services, and Insurance
CAPEX	Capital Expenditure
CBS	Core Banking Solution
CCM	Critical Controls Matrix
C-DAC	Centre for Development of Advance Computing
CIO	Chief Information Officer
COTS	Commercial Off-The-Shelf
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CTO	Chief Technology Officer
DoS	Denial of Service
DoT	Department of Telecommunications (India)
DR	Disaster Recovery
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
FI	Financial Institution
HR	Human Resources
HVSS	High-Value Sub-System
IaaS	Infrastructure as a Service
IBCC	Indian Banking Community Cloud
IBCS	Inter-Bank Clearing System
IDRBT	Institute for Development and Research in Banking Technology
IP	Intellectual Property

ISMS	Information Security Management System
IT	Information Technology
ITAA	Information Technology (Amendment) Act
IVR	Interactive Voice Response
KYC	Know Your Customer
LAN	Local Area Network
LMS	Learning Management System
LVSS	Low-Value Sub-System
MIS	Management Information System
MPLS	Multi-Protocol Label Switching
O-ISM3	Open Information Security Management Maturity Model (The Open Group)
O-RA	The Open Group Risk Analysis Standard
O-RT	The Open Group Risk Taxonomy Standard
OTP	One-Time Pin
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCI	Payment Card Industry
PCI-DSS	Payment Card Industry – Data Security Standard
PDA	Personal Digital Assistant
POS	Point of Sale
RBI	Reserve Bank of India
RFP	Request For Proposal
RRB	Regional Rural Bank
RTGS	Real-Time Gross Settlement
SaaS	Software as a Service
SAPS	Settlement Accounting Processing System
SCORM	Sharable Content Object Reference Model
SLA	Service-Level Agreement
SSL	Secure Sockets Layer

UAT	User Acceptance Testing
UCB	Urban Co-operative Bank
UIDAI	Unique Identification Authority of India
VM	Virtual Machine

References

The following documents and websites are referenced in this document.

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- Cloud Security Alliance (CSA): Critical Controls Matrix (CCM); refer to: https://cloudsecurityalliance.org/research/ccm.
- Gartner: Gartner Says Indian Public Cloud Services Market Will Reach $838 Million In 2015; refer to: www.gartner.com/newsroom/id/2964917.
- IEEE Report: Indian Banking Community Cloud (IBCC); refer to: www.idrbt.ac.in/ibcc.html.
- Information Technology (Amendment) Act (ITAA) 2008; refer to: http://en.wikipedia.org/wiki/Information_Technology_Act_2000.
- Information Week article: Four Co-operative Banks in India Adopt IBM's Data Center Solutions; refer to: www.informationweek.in/informationweek/press-releases/239387/-operative-banks-india-adopt-ibms-center-solutions?utm_source=referrence_article.
- Information Week article: Pondicherry Co-operative Urban Bank Adopts IBM SmartCloud for Core Banking Solution; refer to: www.informationweek.in/informationweek/press-releases/239567/pondicherry-operative-urban-bank-adopts-ibm-smartcloud-core-banking-solution.
- Institute for Development and Research in Banking Technology (IDRBT) Report: Cloud Security Framework for Indian Banking Sector; refer to: www.idrbt.ac.in/publications/Frameworks/Cloud%20Security%20Framework%20(2013).pdf.
- ISO/IEC 27001: Information Security Management; refer to: www.iso.org.
- C. Millard: Cloud Computing Law, October 2013.
- Moneycontrol.com article: Business Transformation of YES Bank through Cloud Computing; refer to: www.moneycontrol.com/news/business/business-transformationyes-bank-through-cloud-computing_845455.html?utm_source=ref_article.
- RBI Cir. No. 42/09.18.300/2012-13: Implementation of Core Banking Solutions (CBS) by Urban Co-operative Banks (UCBs); refer to: http://rbi.org.in/Scripts/NotificationUser.aspx?Mode=0&Id=7888.
- RBI Working Group Report on Cloud Computing Option for Urban Co-operative Banks (UCBs); refer to: http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/RWGFUF031012.pdf.
- RBI Working Group Report on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds; refer to: http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf.
- Right to Information Act 2005; refer to: http://en.wikipedia.org/wiki/Right_to_Information_Act.
- The Open Group Standard: Open Information Security Management Maturity Model (O-ISM3), February 2011 (C102); refer to: www.opengroup.org/bookstore/catalog/c102.htm.

- The Open Group Standard: Risk Analysis (O-RA), October 2013 (C13G); refer to: www.opengroup.org/bookstore/catalog/c13g.htm.
- The Open Group Standard: Risk Taxonomy (O-RT), October 2013 (C13K); refer to: www.opengroup.org/bookstore/catalog/c13k.htm.
- Zinnov Management Consulting: IT Adoption in the Banking, Financial Services, and Insurance (BFSI) Sector in India; refer to: www.zinnov.com/download.php?file=189.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

Further information on The Open Group is available at www.opengroup.org.