Risk Advisor

Jan-2016

Cloud Computing: Addressing Cloud risk- Looking beyond the contracts

B.K. KHARE & CO.

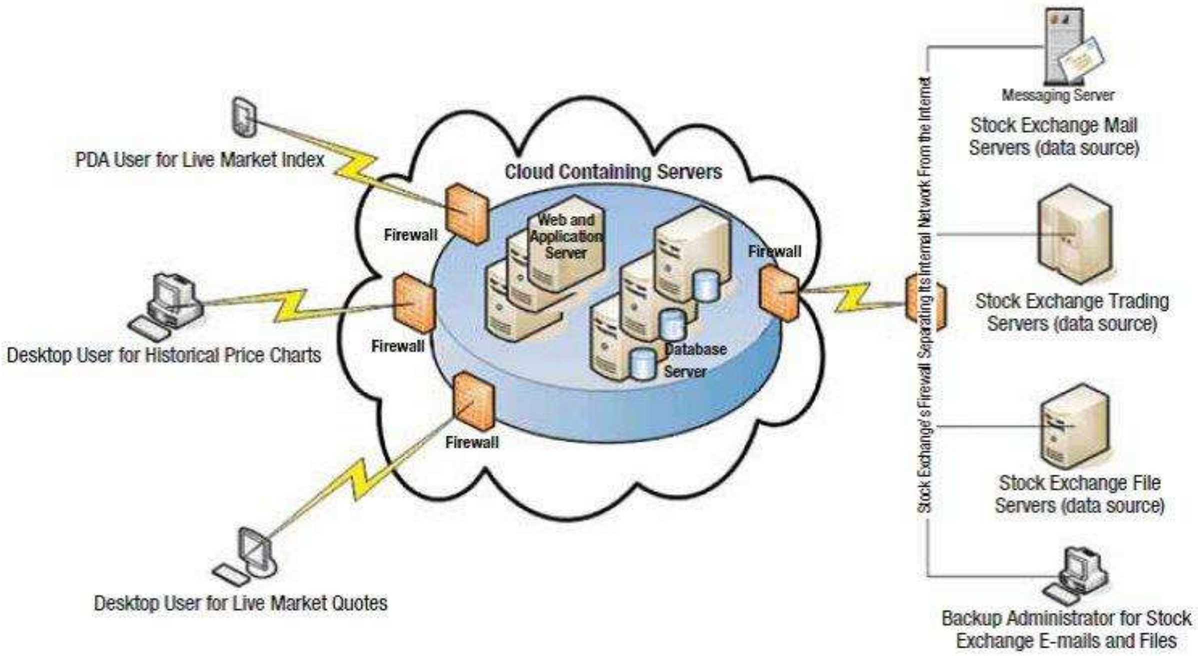
CHARTERED ACCOUNTANTS

706-708, Sharda Chambers,
New Marine Lines, Mumbai 400 020
Telephone: +91-22 2200 0607 / 7318 / 6360, 6631 5835 / 5836

In a quick narrow sense, cloud computing may sound like outsourcing. But, it is quite different and much more than that. In this article, let us have an overview of the concept, understand business benefits in the long run through transformation and leveraging the cloud computing, touch upon various Governance, risk, security considerations and challenges associated with and finally, discuss a case study before we conclude our discussion with Return On Investment and Auditors perspectives, using the research, survey and other publications published by the ISACA, NIST and the Cloud Security Alliance and other agencies.

What is Cloud Computing?

A model for enabling convenient, on---demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Visual depiction of a typical cloud computing environment is as below:


PDA User for Live Market Index
Cloud Containing Servers
Firewall
Web and Application Server
Firewall
Desktop User for Historical Price Charts
Firewall
Database Server
Firewall
Desktop User for Live Market Quotes
Stock Exchange's Firewall Separating its Internal Network From the Internet
Messaging Server
Stock Exchange Mail Servers (data source)
Stock Exchange Trading Servers (data source)
Stock Exchange File Servers (data source)
Backup Administrator for Stock Exchange E-mails and Files

Why Cloud Computing?

The continued influence and innovative use of the Internet has enabled cloud computing to utilize existing infrastructure and transform it into services that could provide enterprises both significant cost savings and increased efficiency.

It offers the opportunity to decouple Organisational IT needs and their infrastructure and possibility of high reward in terms of containment of costs and features such as agility and provisioning speed. By moving IT services to the cloud, enterprises can take advantage of using services in an on-demand model. Less up-front capital expenditure is required, which allows businesses increased flexibility with new IT services. Enterprises are realizing there is a potential to leverage this innovation to better serve customers and gain business advantage. With the evolution of managed services, outsourcing, virtualization and broadband connectivity, cloud computing was inevitable.

Cost benefit analysis of Cloud Computing

Cloud computing brings many advantages to users and vendors. It is likely that, at some point, any device that can access the Internet will be able to run a cloud-based application. Users will not have to worry about storage capacity, compatibility or other similar concerns. Cloud computing can act as a utility grid for vendors and optimize the use of their resources.

The premise of the cloud is that by outsourcing portions of information management and IT operations, enterprise workers will be free to improve processes, increase productivity and innovate while the cloud provider handles operational activity smarter, faster and cheaper. Assuming this to be the case, significant changes to the existing business processes will likely be required to take advantage of the opportunities that cloud services offer.

According to an international white paper, in addition to the financial savings involved with cloud computing, one of this model's strengths is for enterprises to streamline processes and increase innovation. This can translate into more reliable backup, more satisfied customers, increased scalability and possibly even higher margins.

However, there are some downsides to the cloud. For example, a cloud's use is contingent on accessing the Internet and the cloud servers. What should users do if some servers fail to operate and data are not accessible etc.
Results of maturity model study conducted by the ISACA revealed the below summarised benefits, challenges and costs:

Z	
Benefit	**Description**
Tangible	
Cost reduction	Computing cost is shifted from a capital expenditure to an operational cost because the cloud provider supplies the underlying infrastructure as part of the service bundle. In addition, the cloud promises a cost reduction in the following areas: • Labor—IT system administration hours/headcount • Application software (SaaS only) • Licensing purchase and maintenance • Technical support and user support • Maintenance (upgrades, updates, patches, etc.) • Hosting (physical building, power, cooling, etc.)
Enhanced productivity	User mobility and ubiquitous access can increase productivity. Collaborative applications increase productivity and reduce rework.
Optimized resource utilization	Enterprises use only the computing resources they need, thus reducing system idle time waste.
Improved security/compliance	Cloud providers may offer robust security controls as a market differentiation.
Access to skills and capabilities	Customers benefit from top-notch skills and capabilities while avoiding employment costs (recruiting, salary, benefits, training, etc.).
Scalability	On-demand provisioning or computing resources eliminate the cost of capacity planning.
Agility	Agility contributes to cost reduction and productivity enhancement due to faster provisioning of systems: • Faster application deployment (SaaS) • Faster application development/testing (PaaS)
Customer satisfaction	Effective utilization of cloud applications can increase collaboration between the enterprise and its customers or reduce response time to customer inquiries.
Reliability	Cloud providers have redundant sites that can address business continuity and disaster recovery in a more efficient manner.
Performance	Better performance and up-time can result from continuous and consistent operations monitoring by the cloud provider.

Intangible	
Avoidance of missed business Opportunities	A cloud application (SaaS) may be the critical element to land a new business or expand into new markets.
Focus on core business	IT resources can be allocated to support core business functions.
Employee satisfaction/innovation	Mobility and faster performance can improve employee satisfaction and boost innovation.
Collaboration	Real-time collaboration can increase quality and innovation.
Risk transfer	Some risk can be transferred to the CSP (e.g., security breaches, data loss, and disaster recovery); this could represent a tangible or intangible benefit.

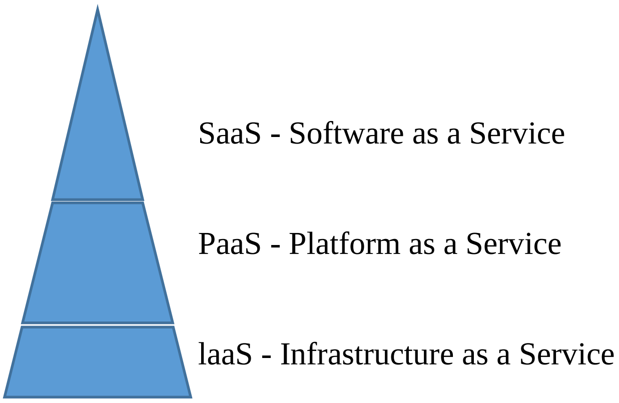
Cloud Challenges	
Challenge	**Description**
Incompatibility	Cloud services may not be compatible with the existing IT infrastructure or specific systems that must be integrated.
Uptime	Cloud vendors may not be able to guarantee agreed-on uptime. In addition, uptime may be impacted by other factors, including the customer's Internet service providers.
Performance	Multitenant models can degrade performance over time if capacity is not properly planned. Internet speed can also negatively impact performance.
Security	Cloud computing represents traditional and new risk that must be accounted for and mitigated accordingly (either by the CSP or the customer).
Compliance	The ubiquitous and abstract nature of the cloud can cause an enterprise's transition from compliance to noncompliance without any notice.
Pay-as-you-go	The enterprise must implement controls to avoid overage charges incurred when systems stay connected after a demand spike is over.
Lock-in (hardware or vendor)	Customers may become locked into a specific technology or a specific cloud vendor, which can prevent portability.
Cloud consumerization	Business units may be able to procure cloud services without involving IT. To prevent this situation, the enterprise must adapt its governance framework to control cloud services procurement
Limited customization (Black Box)	Cloud applications may not be customized every time the business process changes, making the business process a "Black Box" due to costs associated with each modification or application limitations.

Cloud Costs	
Cost	**Description**
Upfront Costs	
Technical readiness	Some investment in bandwidth may be necessary to accommodate the new demand for network/Internet access. Other infrastructure components may need to be upgraded to integrate with cloud services.
Implementation	Professional services may be needed for managing the transition to the cloud.
Integration	Professional services may be needed for integrating in-house and cloud services.
Configuration/customization	This applies to customer-based configuration for SaaS applications.
Training	IT resources may require training to manage cloud vendors and services. Users may need training on new applications.
Organizational change	Processes may require some reengineering to accommodate cloud-specific needs (e.g., change management, resource utilization monitoring, and user access provisioning, internal audit).
Recurring costs	
Subscription fees	These will comprise agreed-on periodic fees (monthly, quarterly, yearly) for the use of cloud services.
Change management	These may comprise the cost associated with the change management process and any cost incurred when requesting system changes.
Vendor management	These are costs associated with monitoring CSP activities, contract management, service level agreements (SLAs) monitoring and enforcement, or any other activity geared to manage service delivery and evaluation.
Cloud coordination	For enterprises running more than one cloud service, a cloud coordination group is necessary to ensure integration and consistency.

End-user support and administration	Some of these costs will be part of the subscription fee while some may be retained by the enterprise.
Risk mitigation	Countermeasures will need to be implemented to control any risk introduced by cloud computing.
Downsize/upsize	Unless otherwise specified in the contract, some vendors may charge for downsizing or upsizing computing resources.
Termination costs	
Revert to on premises or transfer to a different provider	The enterprise may need to revert to an in-house model when/if new regulations or economic problems render the cloud impractical. Some of the possible costs are: • Extracting data from the cloud and validating their accuracy and completeness • Cost to sanitize or shred data from cloud storage and processing hardware • Configuration and provisioning in-house systems to replace cloud services • Penalties for early termination • Reallocation or recruitment of IT resources to support services being reverted. • Reallocation or procurement of physical resources to host services being reverted

Attributes and Characteristics

- Attributes

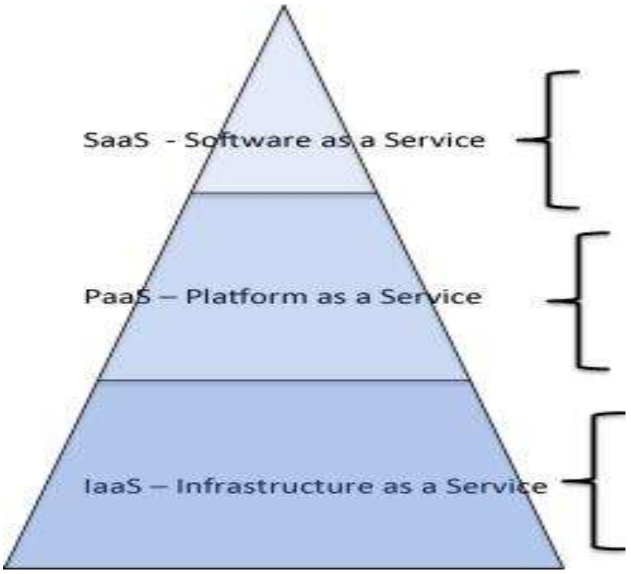

SaaS - Software as a Service
PaaS - Platform as a Service
laaS - Infrastructure as a Service

- All options use standard tool, access is always via a browser (no locally installed software).
- Uses, options, configurations are common to all users.
- Transaction pricing is typically transaction based.
- The lower in the pyramid the more "utility" approach, i.e. 'storage is storage‘.
- Users have little or no control over technical details.

- Characteristics

- **On-demand self-service:** Unilateral and automatic provisioning of computer capabilities.
- **Broad network access:** Capabilities are available / accessible over the network via thick and thin clients on a variety of hardware devices.
- **Resource pooling:** The provider's computing resources are pooled using a multi-tenant model, with different physical and virtual resources dynamically assigned. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre).
- **Rapid elasticity:** Capabilities can be rapidly and elastically provisioned, in some cases automatically.
- **Measured Service:** Cloud systems automatically control/optimize resources via a metering capability. Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models


SaaS - Software as a Service
PaaS – Platform as a Service
IaaS – Infrastructure as a Service

Salesforce.com Google Apps, Google Mail

Standard Servers - Amazon Eleastic Compute Cloud (EC3) Standard Platforms - force.com, AppEngine (Google) Bungee Connect (Java), Long Jump (Java/Eclipse

Networking - Amazon Private Cloud, Dynamic network capacity Storage - Mozy, Carbonite, DropBox

Deployment Options

- **Private cloud**: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community cloud** the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- **Public cloud** the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid cloud** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Why Cloud Computing is different - Risks

Despite the tremendous potential benefits of cloud computing, there are several risks associated with it. The key concerns are related to loss of control, security, integrity, privacy and availability.

As a “new” initiative, cloud computing can bring the potential for high risk. Cloud computing introduces a level of abstraction between the physical infrastructure and the owner of the information being stored and processed.

The company’s responsibility for governing security has not been removed, it is merely different.
Cloud computing is an evolutionary trend with a long history of progress. Below mentioned are certain notable risks associated with:

-Awareness (Case studies)

During an audit, we often hear the phrase, “they handle that.” In other words, the company has signed an agreement for Software as a Service or Infrastructure as a Service and breathes a sigh of relief because its responsibility for security on those systems is supposedly in the hands of the service provider. In actuality, the company’s responsibility for governing security has not been removed, it is merely different, and must be evaluated in the context of the cloud service, the cloud provider and the purpose for which the company is utilizing the service.

- The Department of Energy said "we are not using cloud computing". DoE was, in fact, using cloud computing in four locations to keep up with demands for scientific computing
- Since DoE officials weren't aware they were using cloud computing their auditor pointed out the obvious:

"Without adequate planning, there is an increased risk that users may utilize cloud computing products and services on the Department's networks, unnoticed without undergoing adequate security evaluations"

Under this environment, roles and responsibilities are divided among various parties involved as shown below:

Cloud Decision Framework and Issues deserving attention before the decision

What to pay attention to

- Understand why "cloud" makes sense...be rigorously honest
    - Cost, support expertise, staffing, scalability, time to market
- Understand, intimately, your economics...all of them
    - ROTs are tough to determine but you must try
- Assess the "cloud" service against your Governance, Regulatory, and Compliance requirements
    - Can you still audit and demonstrate compliance to your controls
- Know what you are exactly what you are buying
    - Understand all of the providers terms, costs, and conditions
    - Conduct vendor/service due diligence
    - Who is going to do what, using what standards?
    - How will you know you are getting what you pay for
    - Know how you will exit the service before you sign up
- Decide if you have the expertise to manage the "new" environment

Before moving to the cloud, companies should assess the following:

- Security and Privacy

- Who has access to what?
- Specific measure to insure data privacy? Such as Data segregation and Data recovery?
- Data location and ownership - where exactly will it reside? If there is a problem with regard to jurisdiction or a legal matter, what happens with the data rights?

-Performance, Manageability, and Availability

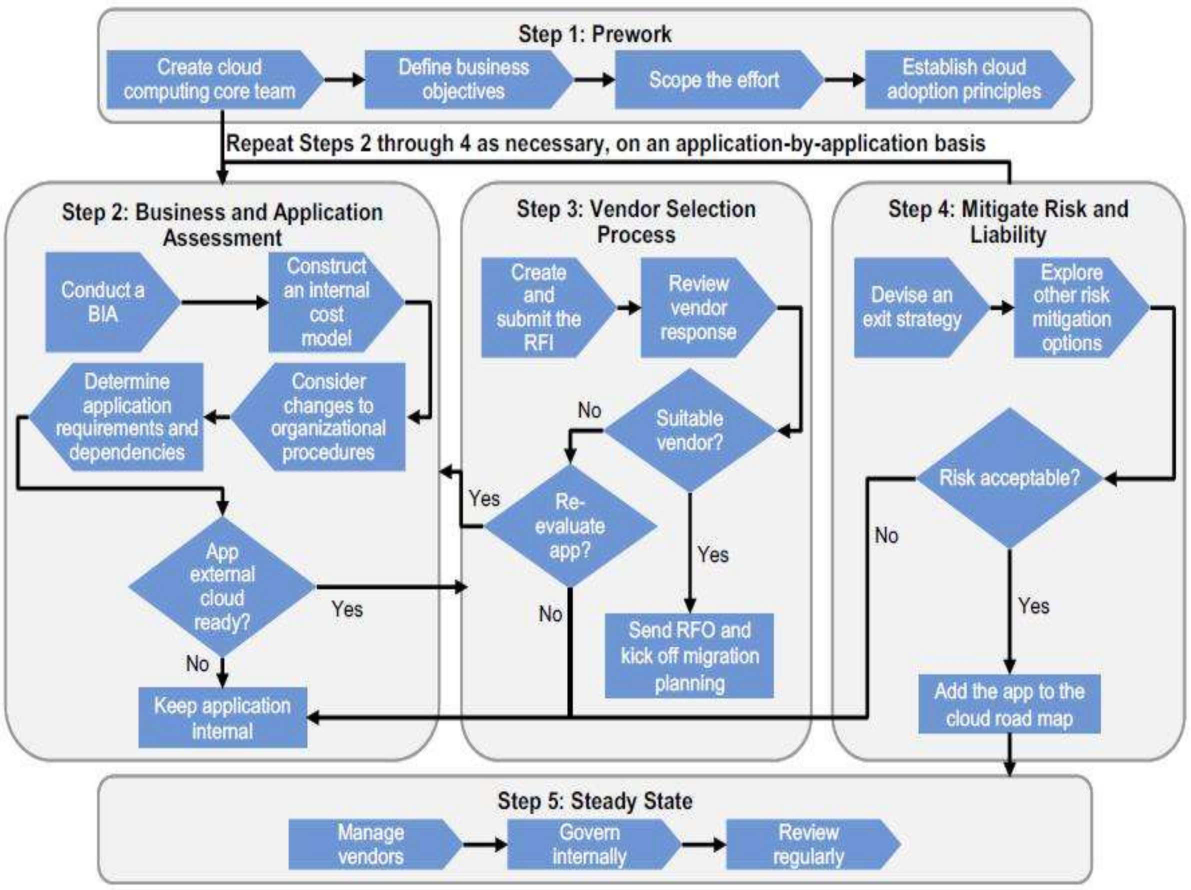
- How will performance be guaranteed?
- Tools to manage service/application
- What happens if the service goes down?

-Governance, Regulatory, and Compliance

- How will controls and compliance be maintained - How will it be known if the provider is complying with the Organisation specific regulatory requirements?
- Long-term viability
- Cloud computing solution "completeness"
- Cloud provider’s financial stability, inter-operability, standards and transparency
- Vendor "lock in
- Right to audit
- Investigative support

Based on the above discussed and other considerations, a well thought decision may be made. Gartner’s Decision Framework (refer below) could provide useful guidance in this regard.

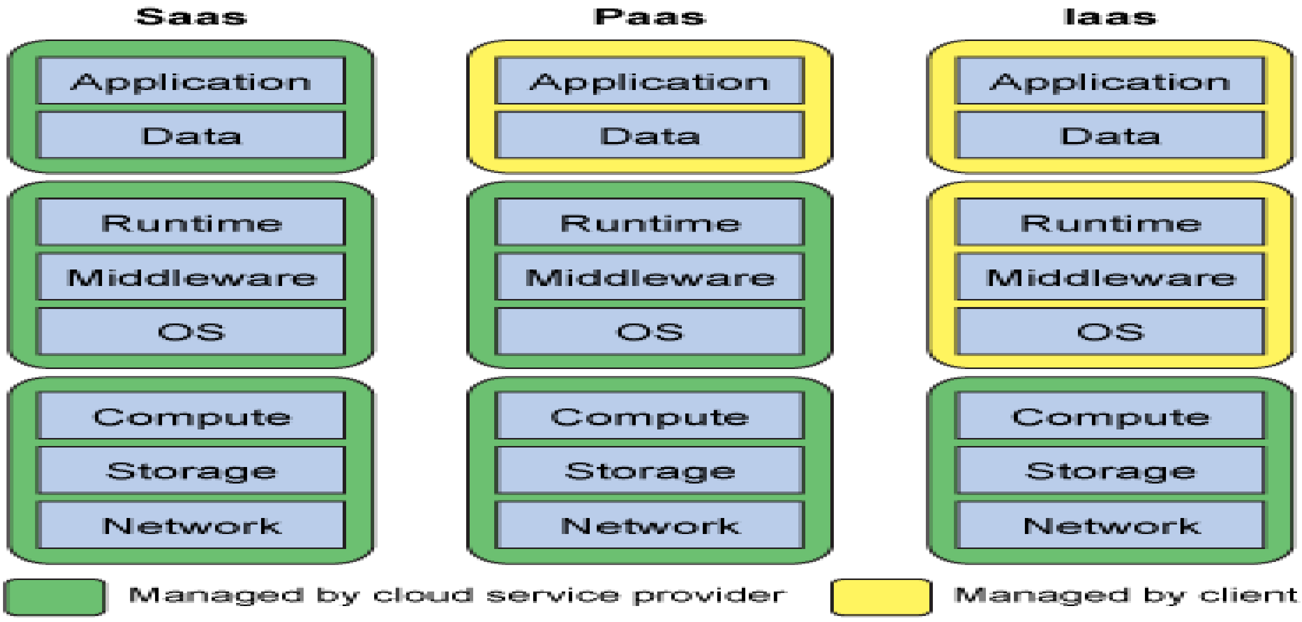
Sample Cloud Decision Framework


Step 1: Prework
Create cloud computing core team
Define business objectives
Scope the effort
Establish cloud adoption principles
Repeat Steps 2 through 4 as necessary, on an application-by-application basis
Step 2: Business and Application Assessment
Conduct a BIA
Construct an internal cost model
Determine application requirements and dependencies
Consider changes to organizational procedures
App external cloud ready?
Yes
No
Keep application internal
Step 3: Vendor Selection Process
Create and submit the RFI
Review vendor response
Suitable vendor?
No
Yes
Re-evaluate app?
Yes
No
Send RFO and kick off migration planning
Step 4: Mitigate Risk and Liability
Devise an exit strategy
Explore other risk mitigation options
Risk acceptable?
No
Yes
Add the app to the cloud road map
Step 5: Steady State
Manage vendors
Govern internally
Review regularly

Source: Gartner (October 2012)

In order to understand the above factors with associated risks and mitigation measured, it is required to understand various parties involved and their roles and responsibilities for deploying a suitable and effective cloud computing model.

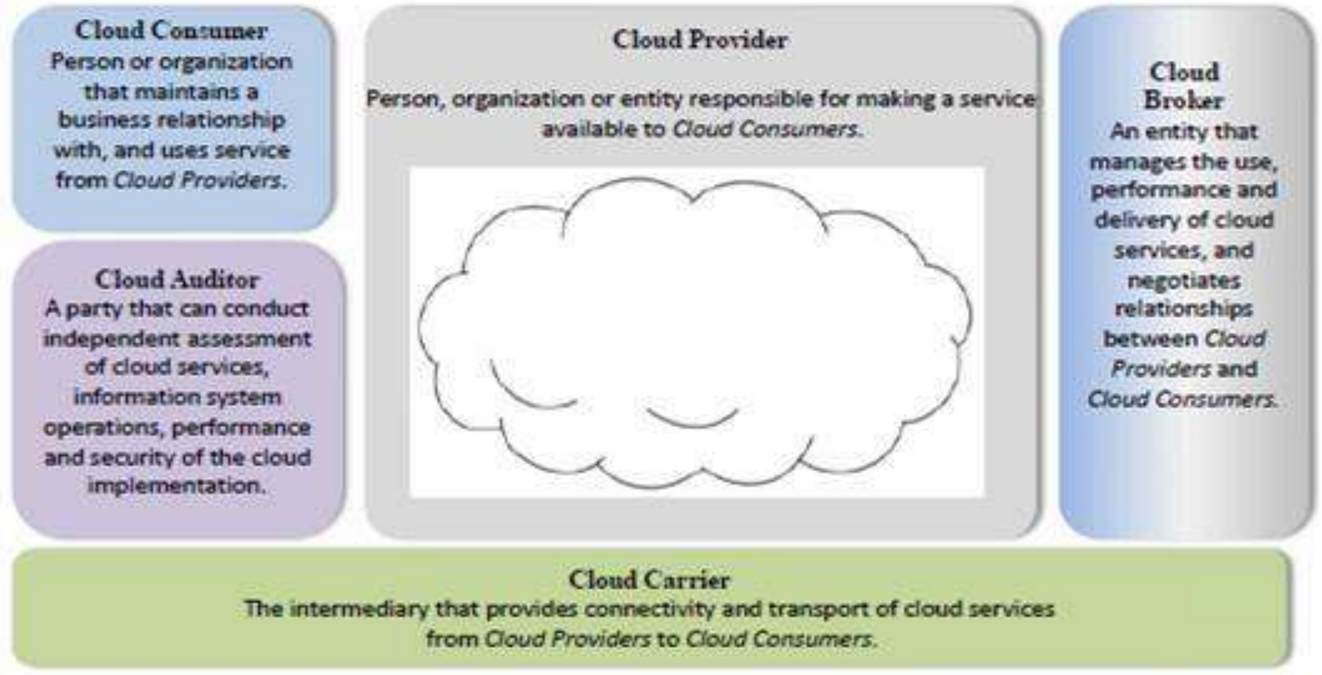
Typical segregation of responsibilities between the user and the service provider is depicted below:



Saas	Paas	Iaas
🟩 Application	🟨 Application	🟨 Application
🟩 Data	🟨 Data	🟨 Data
🟩 Runtime	🟩 Runtime	🟨 Runtime
🟩 Middleware	🟩 Middleware	🟨 Middleware
🟩 OS	🟩 OS	🟨 OS
🟩 Compute	🟩 Compute	🟩 Compute
🟩 Storage	🟩 Storage	🟩 Storage
🟩 Network	🟩 Network	🟩 Network

🟩 Managed by cloud service provider 🟨 Managed by client

Various parties and associated roles in a sample cloud environment are shown below:



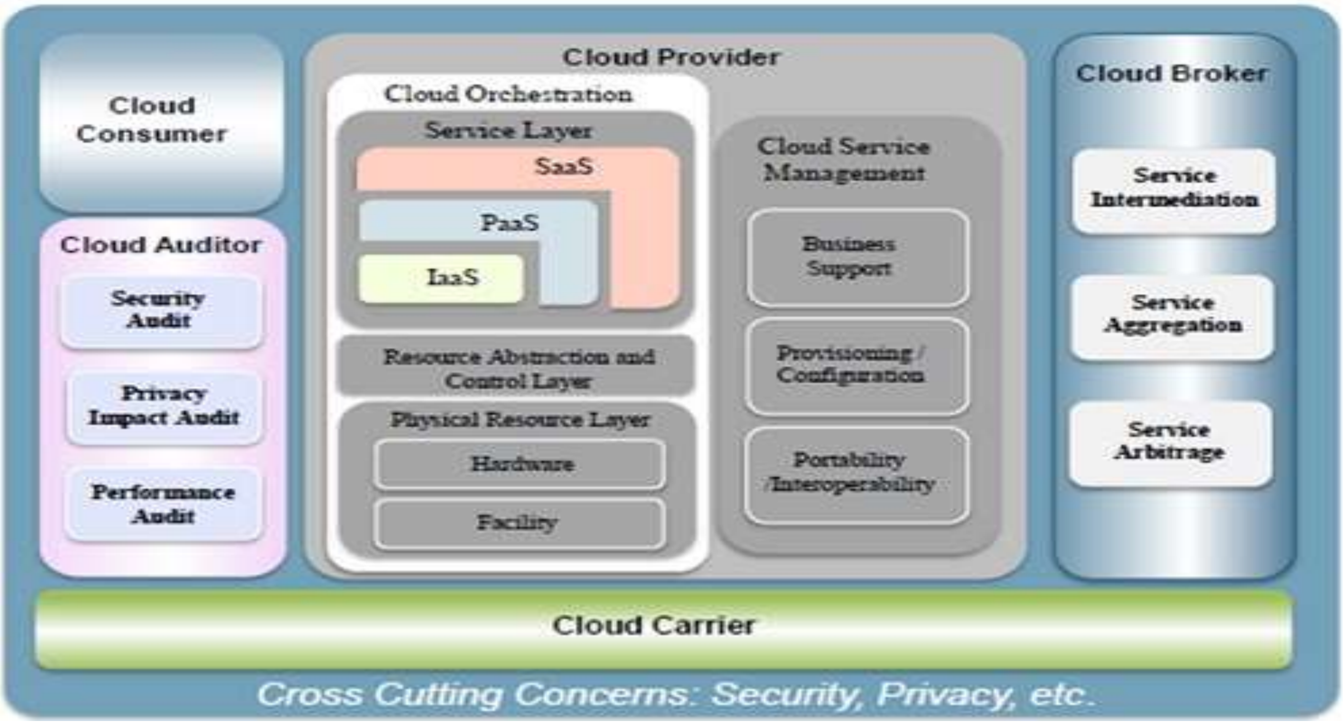
Cloud Consumer
Person or organization that maintains a business relationship with, and uses service from *Cloud Providers.*

Cloud Auditor
A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

Cloud Provider
Person, organization or entity responsible for making a service available to *Cloud Consumers.*

Cloud Broker
An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers.*

Cloud Carrier
The intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers.*



Risk assessment of Cloud Computing environment:

The Gartner Group has specified seven cloud computing security risks to users:
1. **Privileged user access**—Outsourced services bypassing the physical, logical and personal controls IT shops exert over in-house programs
2. **Regulatory compliance**—Users being ultimately responsible for the security and integrity of their own data, even when the data are held by a service provider
3. **Data location**—Users not knowing where their data are stored
4. **Data segregation**—Data in the cloud being in a shared environment alongside data from other customers
5. **Recovery**—Fuzziness about ability to do a complete restoration and the time it takes
6. **Investigative support**—Difficulties in investigating inappropriate or illegal activities
7. **Long-term viability**—Availability of data in their original format after procedural and technical changes in the cloud environment

Further, a collaborative project by ISACA and CSA, the Cloud Market Maturity study reveals that cloud users in 50 countries were least confident about the following issues (ranked from least confident to most confident):

1. Government regulations keeping pace with the market
2. Exit strategies

3. International data privacy
4. Legal issues
5. Contract lock in
6. Data ownership and custodian responsibilities
7. Longevity of suppliers
8. Integration of cloud with internal systems
9. Credibility of suppliers
10. Testing and assurance

Guidance on risk assessment

To conduct a risk-based assessment of the cloud computing environment, there are generic risk frameworks such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise Risk Management—Integrated Framework*.

There are also IT domain-specific risk frameworks, practices and process models such as ISO 27001 and IT Infrastructure Library (ITIL). Bottom-up guidance specific to cloud computing also exists from various bodies such as the Cloud Security Alliance (CSA), European Network and Information Security Agency (ENISA), and the US National Institute of Standards and Technology (NIST). The Cloud Controls Matrix released by CSA is designed to provide security principles to guide cloud vendors and assist prospective cloud clients in assessing overall security risks of a CSP. The NIST guidelines on security and privacy in public cloud computing, which are currently in draft form, contain the guidelines required to address public cloud security and privacy.

COBIT® framework from ISACA fills the gap between generic risk management frameworks and domain-specific frameworks based on the premise that IT risk is not purely a technical issue.

IA Role in effective deployment of Cloud Computing strategy

Any advanced technology solution, while promising benefits, does pose risks to the organisation. However, if key risks to the business are understood and mitigation plans are put in place, they could be well mitigated.

The risks outlined above are generally applicable throughout the cloud computing life cycle. Regardless of whether a particular organization is thinking about moving to the cloud, is in the process of implementing a cloud-based solution, or is already working in a cloud environment, internal audit is well positioned through its role as an assurance function to help management and the board in this regard. Some of the key assurance issues that will need to be addressed are:

Phase	Suggestive role
Defining a cloud strategy	○ Business case evaluation – Alignment with business needs? ○ Cost benefits analysis from Financial, technical, operational and other perspectives? ○ Criticality of the application being sent to the cloud. ○ Country/regional/ Industry regulations that affect the organization’s business and require specific safeguards.
Evaluating vendors	○ Suitability of solution/product offered; Financial and technological stability of vendor? How would this change the technology environment? ○ How are assets protected? Data migration and disaster recover planning? ○ How is responsibility divided? Who will manage the vendor relationship? ○ How do the company's risks and controls align with the prospective vendor's? Right to audit clause? ○ How does the vendor manage multiple tenants? ○ Jurisdiction and other litigation matters? ○ The cloud vendor’s policy on vulnerability management and reporting, commitment to following up on potential security incidents, and ability to respond promptly to reports ○ Gap analysis of Systems and Processes between the current and ought-to be situations?
Implementing a cloud computing model	○ Adherence to the company's change management and other policies. ○ SLAs and OLAs ○ Division of responsibilities ○ Accountability for regulatory compliances, incident management and other processes ○ Adequacy of Data ownership, migration, recovery and other safeguards ○ End user training

Monitoring vendors	○ How the company's relationship with the vendor is managed ○ Contractual (SLA/OLA) compliance and payment processing review
Others (cyclical)	**Transparency -** How much transparency is enough? What needs to be transparent? Will transparency aid malefactors? **Communication protocols**—Information and reporting lines of communication (including escalation procedures). **Trans-border information flow**— physical location of the information (jurisdiction for legal obligations). Country laws governing personally identifiable information vary greatly. **Certification**—Obtaining independent assurance from third-party audits and/or service auditor reports.

Conclusion

Cloud computing is the way forward considering the way most technology companies are advocating its usage themselves and the benefits are obvious. A day may not be far off when Physical IT infrastructure as we understand them today may no longer be available due to this disruptive advancement (Does anyone remember the big IBM data processing machines?). Organisations therefore must deal with the challenge and realise the anticipated benefits (cost, speed and client satisfaction) to the business. For this they must prepare themselves to deal with:

- The regulatory and other requirements,
- Risks associated with this and mitigating controls
- Protecting organisations interests with water tight contracts especially on Data integrity and Business Continuity
- Periodic processes to evaluate and monitor risks once the cloud computing is implemented.

*****

This newsletter is a service to our clients based on a quick appreciation of the cases, notifications, circulars and judgements. The matter has been written in general terms and should be seen as broad guidance only. This document must not be regarded as a professional advice or authoritative opinion. B. K. Khare and Co., its partners, employees and associates do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this document or for any decision based on it