Guide to Cloud Computing for Accountants 2019

Digital Accounting and Assurance Board
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)

Contents

Introduction

The Institute of Chartered Accountants of India

The Institute of Chartered Accountants of India (ICAI) is a statutory body established by an Act of Parliament, viz. , The Chartered Accountants Act, 1949 (Act No.XXXVIII of 1949) for regulating the profession of Chartered Accountancy in the country. ICAI is the one amongst accountancy bodies in the world, with a strong tradition of service to the Indian economy in public interest.

Over a period of time, ICAI has achieved recognition as a premier accounting body not only in the country but also globally, for maintaining highest standards in technical, ethical areas and for sustaining stringent examination and education standards. Since 1949, the Chartered Accountancy profession in India has grown leaps and bounds in terms of

- Members and student base.
- Regulate the profession of Accountancy
- Education and Examination of Chartered Accountancy Course
- Continuing Professional Education of Members
- Conducting Post Qualification Courses
- Formulation of Accounting Standards
- Prescription of Standard Auditing Procedures
- Laying down of Ethical Standards
- Monitoring Quality through Peer Review
- Ensuring Standards of Performance of Members
- Exercise Disciplinary Jurisdiction
- Financial Reporting Review
- Input on Policy matters to Government

Digital Accounting and Assurance Board of ICAI

ICAI has constituted "Digital Accounting and Assurance Board" (DAAB) for fostering a cohesive global strategy on aspects related to digital accounting and assurance, through sharing of knowledge and practices amongst the members. DAAB is endeavouring to identify, deliberate and highlight on issues in accounting (including valuation) and assurance (including internal audit) issues in the digital world.

DAAB is focusing on issues in accounting and assurance arising from the high pace of digitisation, including use of artificial intelligence in audit, big data analytics in audit, relevance of sampling, valuation of data as an asset, impairment testing of digital assets, insurance of data - valuation and premium fixation, etc. The Board is taking up initiatives to develop knowledge base through position papers and articles on issues relating to impact of technology on accounting and assurance.

Foreword

Advancement in Digital technology across geographies and industries has made cloud computing infrastructure and applications as one of the fastest growing category in IT expenditure. Cloud computing creates multiple possibilities for each and every organisation irrespective of its size and is a great productivity enabling tool which can create foundation for a flexible innovation infrastructure. In last few years, cloud computing has become a mature and reliable technology providing access to core business applications, analytics and collaboration tools.

Keeping in view the growing importance of this innovative technology, the Institute of Chartered Accountants of India (ICAI) through its Digital Accounting and Assurance Board (DAAB) has released "Guide to Cloud Computing for Accountants". This Guide provides useful insights on basic concepts of cloud computing, deployment models, potential concerns and opportunities for Chartered Accountants in cloud computing environment.

I compliment CA. Manu Agrawal, Chairman, DAAB, CA. Dayaniwas Sharma, Vice-Chairman, DAAB, and other members of the Board for this excellent and timely publication. I am sure that this Guide will highlight emerging practices that will help our members in exploring a new stream of opportunities arising out of cloud computing environment.

CA. Prafulla P. Chhajed
President, ICAI

New Delhi
July 01, 2019

Across the globe, extensive digitisation is the trend for providing digital solutions and technologies that involve automated processes leading to effective, cost-reducing and value-adding services. Emerging technologies are driven by market competition and also trigger transformation of accountants' competencies for developing specialist skills in emerging areas, including machine learning, big data, business intelligence, blockchain, cybersecurity, etc.

Cloud computing is today's leading driver of emerging technological landscape and organisations are making it an integral part of their digital initiatives. Analytics and machine learning capabilities that are housed in the cloud are also frequently offered alongside thereby leading to exponential growth in adoption of cloud. Accountants can play a crucial role in developing intelligent platform-independent and cloud-based systems which are interrelated in ecosystems and tailored to the requirement of individual entity/ organisation.

I compliment this excellent "Guide on Cloud Computing for Accountants" being released by the Digital Accounting and Assurance Board. I am confident that this publication on emerging technology will help our members to embrace technological trends and provide value added services in digital era.

CA. Atul Kumar Gupta
Vice President, ICAI

New Delhi
July 01, 2019

Preface

Technological developments are reinventing the accounting profession and a host of trends, such as artificial intelligence, machine learning, blockchain and robotics will accelerate developments even further. Digital Accounting and Assurance Board (DAAB) of ICAI is working towards research on emerging technologies for identifying opportunities and challenges created by emerging technologies for the chartered accountants.

DAAB has released "*Guide to Cloud Computing for Accountants*" which provides an overview of basic concepts of cloud computing and focuses on this emerging technology with the perspective of chartered accountants. This Guide covers Cloud Computing architecture, environment and service model; Cloud Computing service delivery; Issues, concerns, challenges relating to Cloud Computing, etc. Further, the Guide touches upon opportunities for chartered accountants in Cloud Computing for assurance and consulting area. The Guide also covers assurance aspects in detail which includes – Identity and Access Management, Data Protection, Technology Risks, Operations and Regulatory aspects.

At this juncture, we wish to place on record sincere gratitude to CA. Anand Jangid and Dr. Onkar Nath for taking time out of their pressing preoccupations and contributing in preparation of draft of this important publication of the Board.

We would like to express our gratitude to CA. Prafulla P. Chhajed, President ICAI and, CA. Atul Kumar Gupta, Vice President, ICAI for their continuous support and encouragement to the initiatives of the Board. We also wish to place on record our gratitude for the all Board members, co-opted members and special invitees for providing their invaluable guidance and support to various initiatives of the Board. We also wish to express sincere appreciation for CA. Jyoti Singh, Secretary, DAAB, for her technical inputs in finalizing this Guide.

We are sure that the members and other interested readers would find this Guide beneficial for exploiting the infinite opportunities and enhancing their relevance in digital era.

CA. Manu Agrawal
Chairman, DAAB

CA. Dayaniwas Sharma
Vice-Chairman, DAAB

New Delhi
July 01, 2019

1. Introduction

There are many different ways of viewing cloud computing. It's a technology, a collection of technologies, an operational model, a business model; just to name a few. It is at its essence, *transformative* and *disruptive*. It is a new operational model and set of technologies for managing shared pool of computing resources. Computing services ranging from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. Since we are in an era of tough competition, this new economic model for computing has found fertile ground and is seeing massive global investment.

National Institute of Standards and Technology (NIST) defines cloud computing as:

"Cloud computing is a model for enabling ubiquitous, 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 efforts or service provider interaction."

In simpler terms, cloud is a set of resources, such as, processors and memory, which are put in a big pool. As per the requirement, cloud assigns resources to the client, who then connects them over the network. Further, clouds are multi-tenant by nature, i.e., multiple different consumers share the same pool of resources but are isolated and segregated from each other.

It is important to note that cloud computing can refer to several different service types, including Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The risks and benefits associated with each model will differ and so will the key considerations in contracting for this type of service.

Cloud computing has become a great solution for providing a flexible, on-demand, and dynamically scalable computing infrastructure for many applications. Cloud computing also presents a significant technology trend, and it is already obvious that it is reshaping information technology processes and the IT marketplace. For cloud computing to reach the full potential promised by the technology, it must offer solid information security.

This Guide covers the basic concepts of cloud computing, its concerns, assurance and challenges. The objective of this publication is to include the information which may be more relevant and useful to the accounting, auditing and consulting professionals.

1.1 Cloud Computing – Essential Characteristics

Following are essential characteristics of Cloud Computing as defined by NIST –

(i) Resource Pooling is the most fundamental characteristic of cloud computing. The provider abstracts resources and collects them into a pool, portions of which can be allocated to different consumers.

(ii) Cloud provides usage on-demand self-service, i.e., consumers manage their resources themselves, without having to talk to a human administrator.

(iii) All resources on cloud are available over a network and there is no direct physical access.

(iv) Rapid elasticity allows consumers to expand or contract the resources they use from the pool thereby enabling them to match resource consumption with demand.

(v) Measured service meters what is provided to ensure that consumers only use what they are allotted, and, if necessary, to charge them for it.

Further, ISO/IEC 17788 lists six key characteristics, the first five of which are identical to the NIST characteristics. The only addition is multitenancy, which is distinct from resource pooling.

1.2 Business Key Objectives of moving to the Cloud

Cloud computing offers tremendous benefits to any size or type of organiasation in terms of economy, agility and resiliency. It allows small businesses to scale up with lesser investment and enhanced security. Technology creates opportunity to business to grow without worrying about the IT capital budget. Cloud not only helps to reduce present capital spending but also allows a business to forecast the future IT costs based on its growth trajectory. For any organization, to reap key benefits of cloud computing it is very necessary to understand and adopt cloud native models, and adjust architectures and controls to align with the features and capabilities of cloud platforms.

Benefits to business from cloud computing are at all levels of management including following as mentioned in figure below;

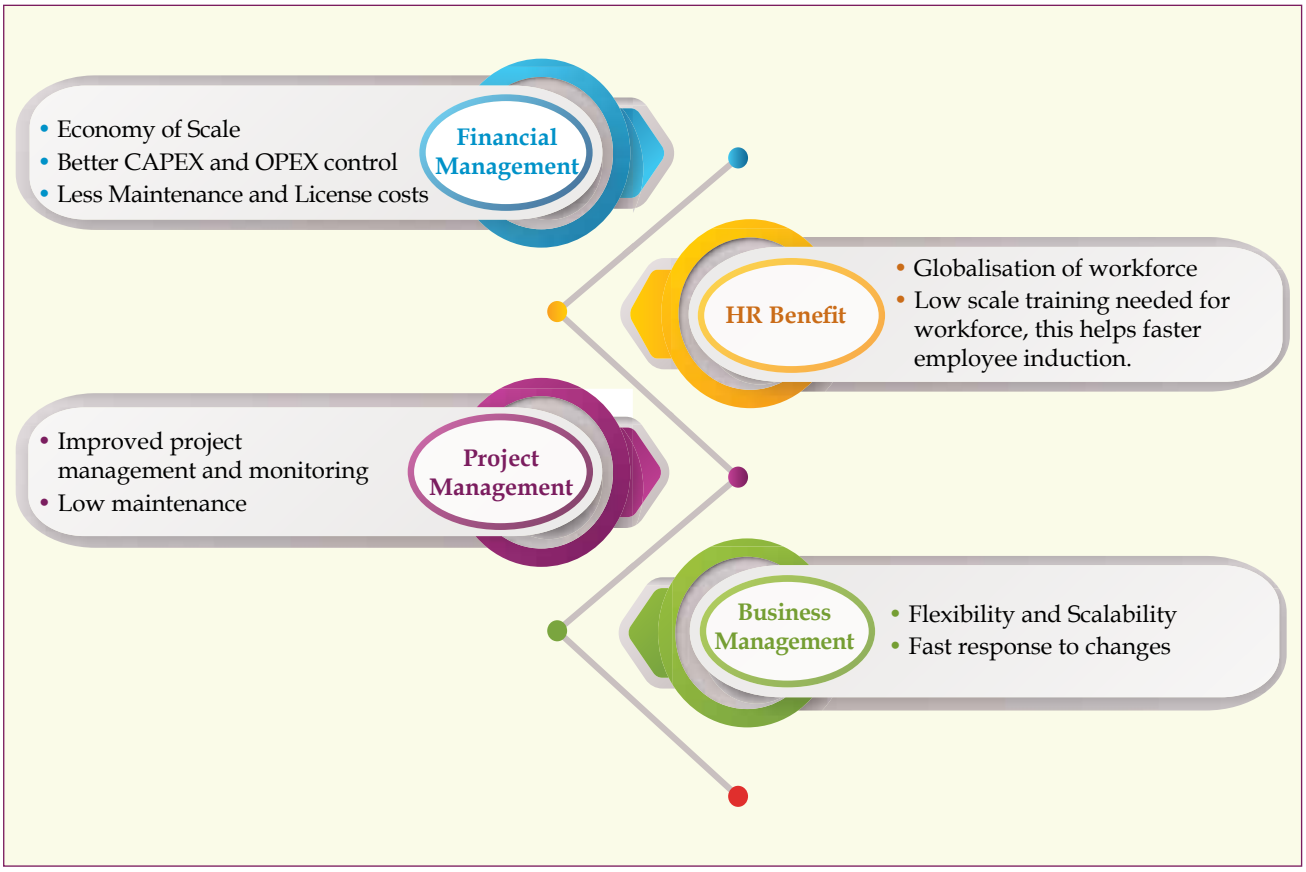
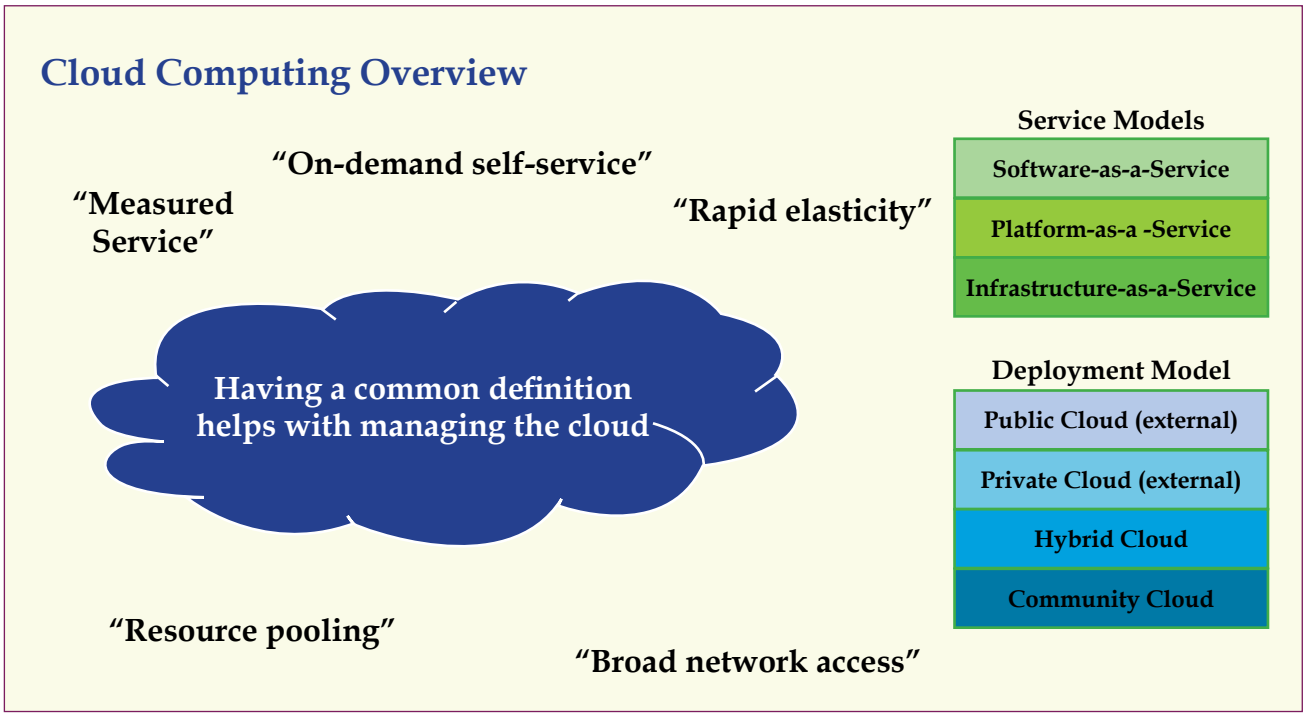


Figure: Business Benefits at Management Levels

2. Cloud Computing Architecture, Environment and Service Model



2.1 Cloud Computing Overview — Deployment Models

Cloud computing technology is deployed in following four general types, based on the level of internal or external ownership and technical architectures-

Public Cloud **-** Cloud computing services from vendors that can be accessed across the Internet or a private network, using systems in one or more data centers, shared among multiple customers, with varying degrees of data privacy control.

Private Cloud - Computing architectures modeled after Public Clouds, yet built, managed and used internally by an enterprise. It uses a shared services model with variable usage of a common pool of visualized computing resources. Data is controlled within the enterprise.

Hybrid Cloud **-** A mix of vendor Cloud services, internal Cloud computing architectures, and classic IT infrastructure, forming a hybrid model that uses the best-of-breed technologies to meet specific needs.

Community Cloud **-** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, objectives. 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.

2.2 Cloud Computing Overview — Service Delivery

Different types of Cloud computing services are grouped into following specific categories:

1. Infrastructure as a Service (laaS)

   - Definition: Delivers computer infrastructure, typically a platform visualization environment as a service. Service is typically billed on a utility computing basis and amount of resources consumed.
   - Customization: Customization where technology being deployed requires minimal configuration.
   - Operational notes:
     i. Easier to migrate applications.
     ii. User of Cloud maintains a large portion of the technical staff (Developer, System Administrator, and DBA).

2. Platform as a Service (PaaS)

   - Definition: Delivers a computing platform as a service. It facilitates deployment of applications while limiting or reducing the cost and complexity of buying and managing the underlying hardware and software layers.
   - Customization: Moderate customization, i.e., build applications within the constraints of the platform.
   - Operational notes
     i. Applications may require to be re-written to meet the specifications of the vendor.
     ii. User of the Cloud maintains a development staff.

3. Software as a Service (SaaS)

   - Definition: Delivers software as a service over the Internet, avoiding the need to install and run the application on the customer's own computers and simplifying maintenance and support.
   - Customization: Limited customization, i.e., existing applications likely not be able to migrate.
   - Operational notes:
     i. Applications may require to be re-written to meet the specifications of the vendor.
     ii. User utilizes the vendors IT staff and has limited to no technical staff.

Cloud Computing Overview - Service Delivery

Responsibility Chart-Your Organizations vs Cloud Vendor

3. Security Frameworks and Standards for Cloud Computing

A security framework is a coordinated system of tools and behaviors in order to monitor data and transactions that are extended to where data utilization occurs, thereby providing end-to-end security. The benefits of security frameworks are to protect vital processes and the systems that provide those operations.

The leading frameworks and guidelines to meet regulatory requirements are as follows:

- Cyber security Framework (NIST, 2013, 2014; SANS, 2016).
- Control Objectives for Information and Related Technology (COBIT 2019).
- Cloud Security Alliance (CSA) provides comprehensive guidance on how to establish a secure baseline for cloud operations. CSA maintains the Security, Trust and Assurance Registry (STAR) cloud provider registry (CSA, 2015).
- Sherwood Applied Business Security Architecture (SABSA) is used for information assurance architectures and risk management frameworks and integrates security and risk management into IT architecture methods and frameworks (SABSA, 2015).
- General Data Protection Regulation (GDPR) lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
- ISO/IEC 17788:2014 provides an overview of cloud computing along with a set of terms and definitions and is applicable to all types of organizations.
- Statement on Standards for Attestation Engagements 18 (SSAE 18) reports include SOC 1, financial reporting; SOC 2, IT controls; and SOC 3, attestation.

3.1 Purposes for Cloud Security Framework

Cloud Security consists of following three components –

(i) Infrastructure Security – It is the foundation for operating securely in the cloud and encompasses the lowest layers of security, from physical facilities through the consumer's configuration and implementation of infrastructure components. In a nutshell, it covers fundamental components that everything in the cloud is built from, including computer (workload), networking and storage security.

(ii) Application Security – It encompasses an incredibly complex and large body of knowledge, everything from early design and threat modeling to maintaining and defending applications. Cloud computing mostly brings security benefits to applications, but as with most areas of cloud technology, it does require commensurate changes to existing practices, processes, and technologies that were not designed to operate in the cloud.

(iii) Data Security and Encryption – Data security is key enforcement tool for information and data governance. Data security controls tend to fall into three buckets – controlling what data goes into the cloud; protecting and managing the data in the cloud; enforcing information lifecycle management security.

Cloud security framework should have the following objectives -

- Multi-tenant isolation.
- Multi-Cloud Services integrated application at different CSPs.
- Backup and Recovery of information (import/export across CSP's).
- Business Continuity and Disaster Recovery.
- Inter-Cloud Information Exchange between CSPs.
- Load balancing multi-tenant users in cloud.
- Reduce human intervention in provisioning and management.

3.2 Area coverage by Cloud Security Framework

CSF shall be applicable to both Cloud Applications (CloudApps) and Cloud Operations (CloudOps). Some of the intended areas of requirements that may be expected to be covered by CSF are: –

- Guidelines and Procedures
- Best Practices
- Policies and Standards
- Governance and Audit
- Regulations and Compliance
- Configuration Management
- Incident Management and Information Reporting
- Risk Management

3.3 Cloud Control Matrix

The foundations of the Cloud Controls Matrix (CCM) rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as, the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers.

As a framework, the CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. The CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

4. Issues, concerns and challenges relating to Cloud Computing for CAs

4.1 Issues of Cloud Computing governance

Cloud Computing governance can be divided into Technical Issues, Legal Issues and Business Issues.

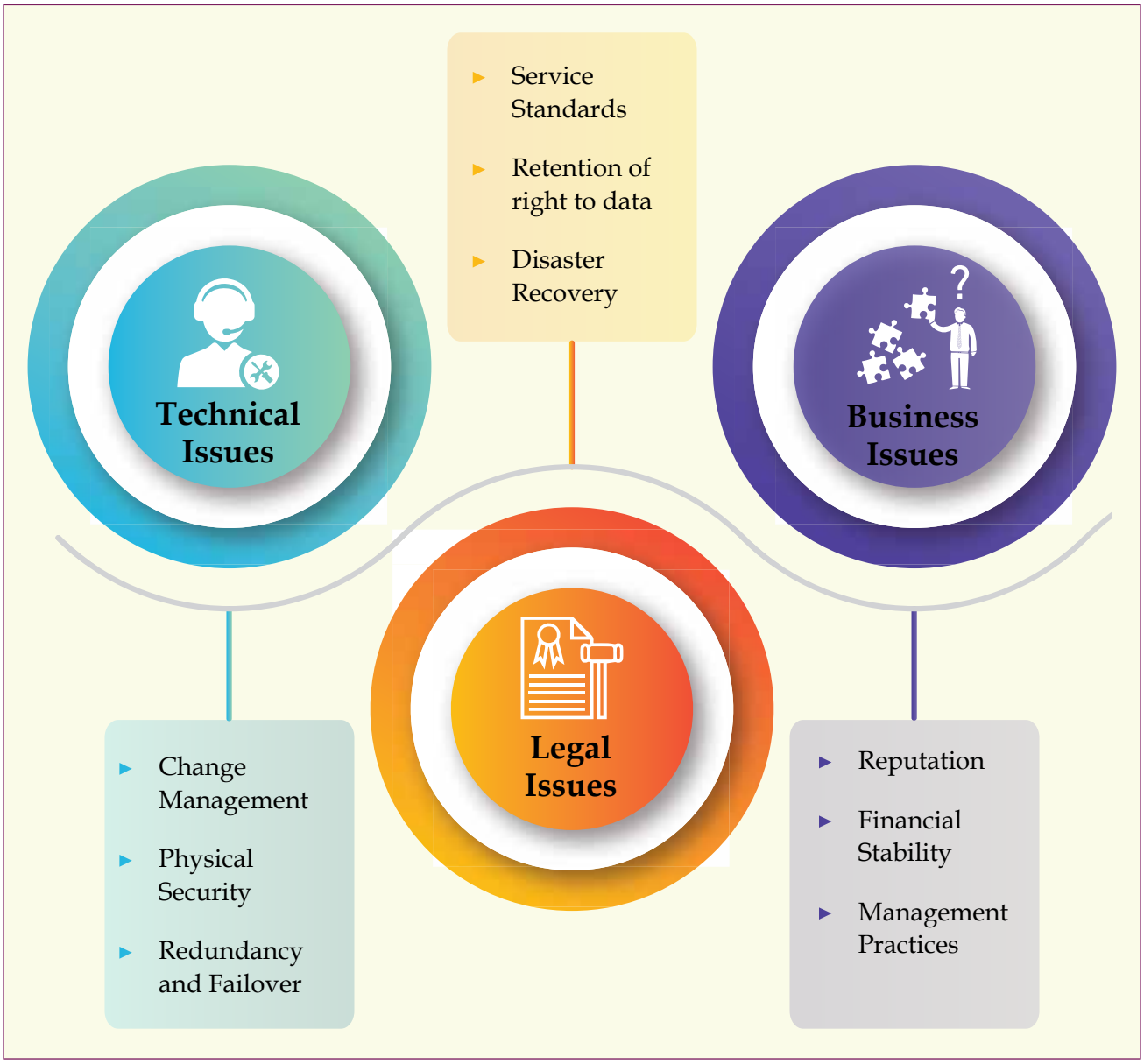
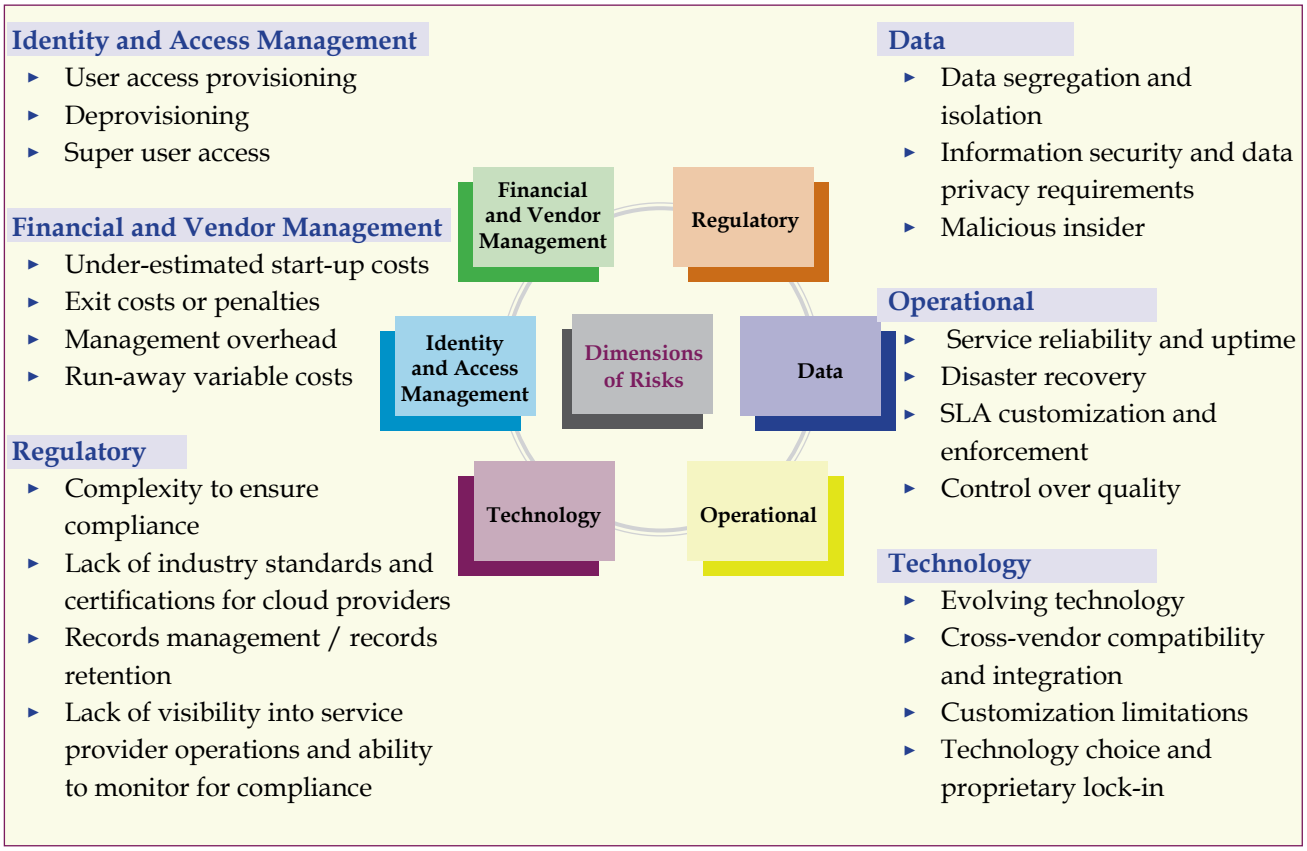


Figure: Issues of Cloud Governance

4.2 Dimension of Cloud Risk Assurance Perspective



4.3. Cloud Computing – Potential Concerns

There are numerous concerns in cloud adoption, but following are the potential major concerns:

- ***Vendor/ Data Locking:*** Vendor lock-in is a situation usually the result of proprietary technologies that are incompatible with those of competitors in which a customer using a product or service cannot easily transit to a competitor's product or service. However, it may also be outcome of inefficient processes or contract constraints, among other things. Cloud Data Management Interface (CDMI) extends support in case of need. Following precautions should be taken to avoid vendor lock-in situation:
  - Ensure data access for interoperability capability
  - Be aware of proprietary data formats
  - Escape the pull of data gravity
  - Avoid adopting proprietary services and APIs
  - Don't limit by distinctive performance characteristics.
- ***Data Leakage:*** Data leakage is a complex challenge for organizations and the most critical threat cloud computing poses for organizations today is the loss of sensitive and personal data and information - both deliberately and inadvertently. Unfortunately, cloud data breaches are on the rise because many organizations don't leverage best practices. The risk of data leakage increases as more employees use their personal devices for work without a strict and robust security policy in place. Following are the strategies to avoid data leakage:

- ***Classify Data:*** All data in the cloud should be classified so that according to roles and responsibility appropriate access may be provided. Adoption of data classification standard may help to have consistency across the database.

- ***Encrypt Data*** – Data should be essentially encrypted in the cloud. It helps to maintain confidentiality of data that is being used in cloud storage as well as sensitive data in transit. The possession of encryption key should be with the cloud customer. Also, ensure that the network sessions in use are secure/encrypted. Unsecured network session like, hotspots should not be used.

- ***Change Passwords*** – Implement robust password policy. Invest in a password program to store all the passwords in a safe and secure place. Avoid single point of failure.

- ***Generate awareness amongst staff*** - Generating awareness is essential to stopping the inadvertent leak of sensitive data and information. Train the staff to make sure they know how to handle situations like, phishing email or a fake phone call.

- ***Set Permissions*** - Permissions should be on a need-to-know basis to avoid any information being accessed by the wrong people. Setting document sharing as 'viewer' rather than 'editor' is a good idea too. Make sure access is immediately taken away from any employee who is no longer with the organization.

- ***Cloud bleed:*** It is a security bug discovered on February 17, 2017 affecting Cloud flare's reverse proxies, which caused their edge servers to run past the end of a buffer and return memory that contained private information such as HTTP cookies, authentication tokens, HTTP POST bodies, and other sensitive data. As a result, data from Cloudflare customers was leaked out and went to any other Cloudflare customers that happened to be in the server's memory on that particular moment. Some of this data was cached by search engines.

4.4 Cloud Computing - Challenges for Chartered Accountants

Since Chartered Accountants use data pertaining to clients/ customers, the software they use on cloud is subject to following challenges as detailed:

(i) ***Confidentiality*** - Confidentiality ensures that only the authorized party can access data, which is there in the cloud. This way the cloud service provider can guarantee the user that his data does not get into the wrong hands and also increases the user's trust in cloud computing and help it grow further. Moreover, if the cloud server user has control over his data, it would further increase the security. Security is an important aspect of cloud computing due to more number of parties, devices and applications involved and because of this the threat of compromise of data is high. This also happens because of the increase in point of access.

Since confidentiality plays a major role in protecting organizational or individual data, information security protocols should be implemented at various different layers of cloud applications. There is always a possibility that the data stored in the cloud may mingle with other user's data. Data can also be compromised unintentionally due to data remanence. It is the residual representation of the data that remains even after efforts are made to erase the data. Confidentiality can also be compromised due to non-trustworthy cloud service providers (CSP). Confidentiality can be ensured through better encryption techniques.

(ii) ***Integrity*** - Integrity, in terms of data security, is nothing but the guarantee that data can only be accessed or modified by those authorized to do so, in simple word it is process of verifying data. Data Integrity is very important among the other cloud challenges. As data integrity gives the guarantee that data is of high quality, correct, unmodified.

After storing data to the cloud, user depends on the cloud to provide more reliable services to them and hopes that their data and applications are in secured manner. But that hope may fail sometimes if the user's data may be altered or deleted. Sometimes, the cloud service providers may be dishonest and they may discard the data, which has not been accessed or rarely accessed to save the storage space or keep fewer replicas when promised. Moreover, the cloud service providers may choose to hide data loss and claim that the data are still correctly stored in the Cloud. As a result, data owners need to be convinced that their data are correctly stored in the Cloud. So, one of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers.

(iii) ***Availability*** - One of the most important areas for consumers is security, performance and availability when it comes to cloud computing. Availability refers to the uptime of a system, a network of systems, hardware and software that collectively provide a service during its usage. Traditionally, the availability of these has been limited to local installations of hardware and software resources which businesses and consumers have deployed and maintained.

With the advent of cloud services there is a considerable shift of these resources into the cloud. While cloud computing presents some cost effective benefits for the consumers and businesses, it is also extremely important for the cloud service providers to offer environments that are highly scalable and high in availability. This will in many ways dictate the credibility of these cloud services. Regardless of the size of an organization, prolonged downtime of the service might be disastrous to its business, customer loyalty and brand value.

(iv) ***Authenticity -*** Data authenticity also means that a digital object is indeed what it claims to be or what it is claimed to be. Authentication, in the cloud context, is the process of validating and guaranteeing the identity of cloud service subscribers or users. It is deemed essential since its strength directly impacts the reliability and security of the cloud-computing environment.

Both cloud providers and chartered accountants are concerned about security issues as the important aspects of cloud authentication service provisioning include Identity Management, Authentication, Access Control and Authorization, Security Policy Management, Key and Certificate Management and Fraud and Anomaly Detection.

(iv) ***Data Privacy*** - Cloud computing presents some serious challenges to data privacy of the chartered accountants. This data may be private and a CA is bound under the terms and conditions of the CSP storing the person's information. In fact, many cloud-based social media rely on their leverage on an individual's private information to make profits. Therefore, it is highly probable for these companies to have clashes with their customers regarding their privacy policies. Data loss and data breaches were recognized as the top threats in cloud computing environments in 2018. Whether a CSP can securely maintain customers' data has become the major concern of cloud users.

To help customers recover in case of service failures, data proliferation is conducted in the cloud where customers' data is replicated in multiple data centers as backups. However,

the distributed storage for multiple data copies may increase the risks of data breaches and inconsistency.

First, due to the heterogeneity of security settings for the multiple storage devices, the overall security level of the data is only determined by the weakest link in the chain. Attackers can obtain the data if any one of the storage devices is compromised.

Second, the multiple data copies need to be synchronized when customers make any data updates, including insertion, modification and deletion. The failures of data synchronization will lead to data inconsistency. Last but not least, it is more challenging for Cloud Service Users (CSUs) to track the appropriateness of a CSP's data operations. For example, it is extremely difficult to ascertain whether the CSP will completely delete all the data copies when such a request is made by the cloud user. External auditing processes are required to supervise a CSP's data operations.

(v) ***Licensing issues in cloud computing*** - The three basic license types are per-user, per-device and "enterprise." Paying per user is a tried-and-true method wherein a user is granted a license to use the application or server. This is subdivided into concurrent users and total users. A concurrent-user license simply means that you are licensed up to x number of users simultaneously. You can have 25 concurrent licenses and 2,500 users, but as long as only 25 people are using the system at one time, all is well. If the license is based on total users, 25,000 licenses are needed.

Per-device licenses vary widely. Again, there is the per-concurrent device and total device model, but there is also the "per processor" model, most often seen in databases and large applications. These licenses are given based on the total number of processors (or processor cores) present in a host system. An organisation may have a SQL server, for example, with eight single-core processors serving up an application with 10 or 10,000 users, each accessing that database. In this case, it pays per processor in the host system.

Then there is the "enterprise" license, the all-you-can-eat smorgasbord of licensing. Whether you have 10 users, 10 devices, 10 thousand users or a million devices, an enterprise license can cover all. Of course, each of these licenses goes deeper. To put an application out to a user population inside an organisation, one must license the server operating systems, the applications, the databases and the end users, plus any development tools and middleware.

While complex, this is merely a math-game of knowing what model best supports the needs of the organization and those consuming the application.

Software licensing in a cloud computing model should be much simpler, however, there may be some crucial issues. Some software vendors are innovating and offering customers a "pay as you go" model in the cloud, where customers pay based on utilization—per hour, per day or even per user—others still don't have policies to make their software cloud-friendly. In some cases, taking their software to a cloud infrastructure can make a project cost prohibitive.

Practically, cloud service vendors tend to license their application or service based on machine account or client, but they do it many ways which are different than a client might expect based on his experience with software and hardware. Many applications and services are delivered by the service providers on the subscription basis, usage model, or both which tie it to the client. The impact of cloud computing on bulk software is quite arduous to measure.

Customers have faced lot of challenges in the cloud service as per software licensing is concerned it may be either hardware based licensing, or CPU based licensing or tracking of the software licensing. This is the nature of the services and hence will need to evolve.

In one of the worst case scenarios, vendors allow customers (users or even service providers) to license the whole hardware and run the software on as many virtual machines (VMs) as they need on that hardware.

This is feasible when the software is needed on a large volume of VMs, for example an operating system that will run a considerable amount of VMs. However, when the software needs to run only on a few VMs, this can become very expensive. The main issue is to license not one whole hardware box but all the hardware boxes running in the cloud infrastructure. This is because in a cloud model, a VM can be running on a given hardware now and on another in the next hour. A possible workaround in this case is to design the infrastructure so that only specific boxes will run that software.

Another scenario, a virtual CPU (vCPU) in a cloud model is not necessarily equivalent to a physical core. It might use a percentage of it, and sometimes, to get the same computing power you'd have on one physical core, you need to use several vCPUs. This could be an inhibitor from a cost perspective, because if a software vendor considers a vCPU to be the same thing as a physical core, the license cost could be multiplied by three or four.

Tracking software licenses was always a critical and difficult task. Although automation solutions are available, it is definitely still not easy. The tip here is when planning to use software in a cloud infrastructure, an organization should make sure to determine the way to track its usage smartly and generate reports to assure compliance aspects.

(vi) ***Data Ownership*** - When a business decides to use a cloud provider, they are essentially taking data and handing it over to a third party. The big question is, after this happens, who owns that data? The client obviously believes that since it's originally their data, it should remain so, but it's also important to note that a cloud provider retains possession of it. So does the cloud provider have any rights to it?

After all, providers are often under some sort of expectation to protect and secure that data. Part of the problem stems from the definition of what data is, in that it is hard to define in the first place. Is data property, not unlike a car or a computer? Should it even be considered property? What is a cloud provider's role in all this? Some may wish to say once data has been handed over to a provider, that vendor now owns it. However, others say the provider is only acting as a custodian of that data, a virtual caretaker that is obligated to give it right back up the moment the real owner requests it.

There are two types of data of chartered accountant that are stored in the cloud. The first category is the data that is created by the user before uploading it in the cloud and the other category is data that is created on the cloud platform itself. Data that is produced prior to any upload into a cloud platform may be governed by the appropriate copyright laws depending on the cloud server while the data that is generated after storage brings about a whole new dimension of ownership.

A number of cloud services tend to acquire user data and store it. The user will not be able to retrieve this data after he provided it and, hence, needs a detail evaluation. For instance,

CAs audit data and customer personal information does not permit other services to access all the user data. In this particular case, personal data such as, the numbers, email address of the customer or regulators cannot be retrieved by third party services through any other software.

A number of companies try to remain relevant by preserving all access to the clients' data to themselves. Some free services reserve the right to keep user data within their platforms while others take ownership of only a part of the data uploaded to their servers. So it seems wise to not use any cloud service that retains ownership of part or all of a user's data.

All issues that will come about as a result of the process of storing data in the cloud, boils down to clarity. Hence, it is advisable to have a clear definition of all the advantages, disadvantages and costs associated with a certain cloud platform. This will help to better understand and appreciate the cloud operations revolving around data management.

(vii) ***Backup Challenges*** - Perhaps one of the biggest concerns that organizations have about cloud backup and disaster recovery is that of security. A well-executed data protection plan backs up all the information that an organization might need to restore to ensure that the business can continue operating.

A challenge around backups is that if a nefarious third party gets access to that backed up data, they have access to all of the critical information generated by and owned by the organization. If you look at the advertising around off-site storage of backup data, much of it uses imagery of something of a cross between a nuclear bunker and a bank vault. This imagery is used because it is designed to reassure organizations that their backed up data is in a secure location, somewhat similar to a bank vault.

With a traditional off-site backup provider, access to the backup tapes involves multiple layers of security. Someone can't just turn up at the off-site backup provider and request tapes. They must provide appropriate physical identification before someone hands over the tapes. An additional layer of security allows organizations to encrypt the backup media so that the data stored there cannot be accessed by anyone except for a person who has access to the decryption key.

Encrypting backed up data means that even if someone at the backup storage facility did manage to steal backup media, they couldn't recover the data stored on the tape. The cloud doesn't provide those obvious external signifiers of security. Imagery around the cloud involves long rows of server racks, rather than Fort Knox style security.

Organizations that are unsure of the process might be concerned that someone may be intercepting protected data as it is transmitted from the organizational site to the cloud. These organizations might also be concerned that data stored in the cloud may be accessible to hackers.

The reality is that, if properly implemented, protected data can be protected by encryption before it even leaves the organization's network, it can also be encrypted in transit to the cloud and at rest while it is stored in the cloud. The key to ensuring that protected data remains secure is to partner with an organization that is experienced in securely shifting and storing protected data in the cloud.

5. Opportunities for Chartered Accountants in Cloud Computing

Cloud computing opens a new, wide area of opportunities for accountancy professionals, which includes following:-

a. Making cost benefit analysis for clients as to whether to deploy cloud computing or in-house computing;

b. Consultation for the implementation of cloud computing facilities including migration to this technology from existing ones;

c. Training to the user staff as regards the operating of these facilities;

d. Direct and indirect taxation consultancy to cloud service providers, including international taxation consultancy;

e. Management consultancy and assistance to management in

   i. The process of conversion from traditional computing system to cloud based.

   ii. Training employees regarding the operation of system under the cloud based system.

   iii. The type of cloud computing environment the organization should adopt.

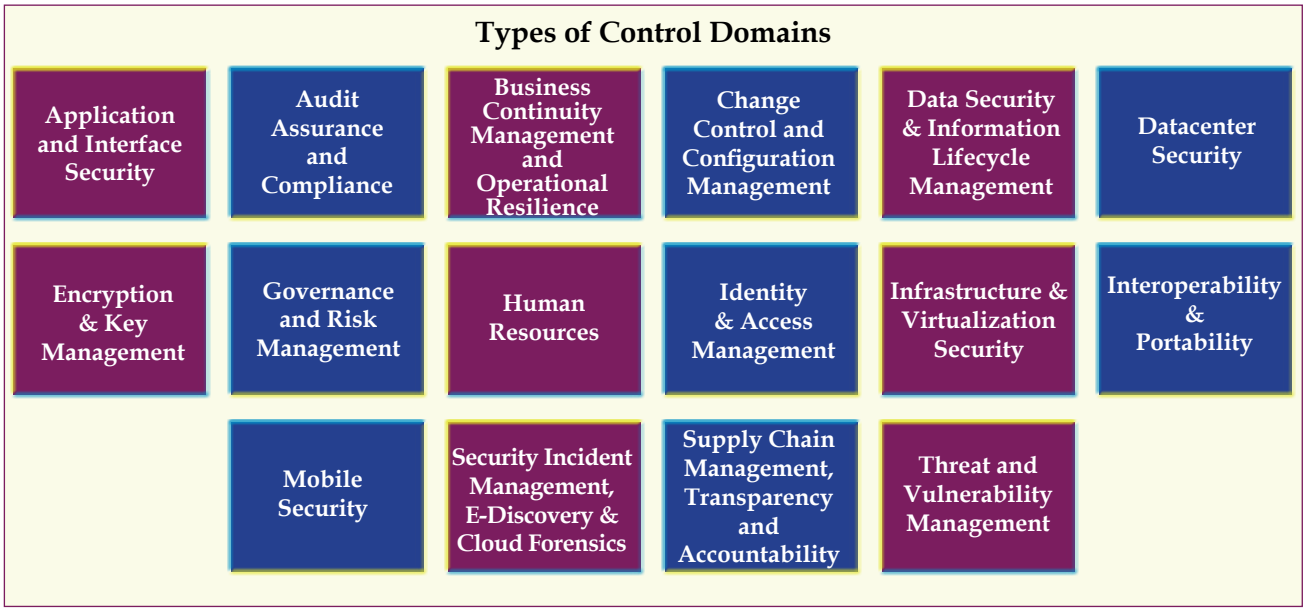
   iv. Selecting the suitable service model to increase ROI.

f. System audit of these facilities.

5.1 Consulting

Following are consulting areas for chartered accountants in cloud environment -

- Cloud Vendor Evaluation
- Cloud Contract Negotiation
- Cloud Implementation Advisor in Organization
- Providing Advisory role in control implementation(CCM ver 3.0.1)
  - **Cloud Control Matrix** is a matrix published by Cloud Security Alliance (CSA) which has a list of all the controls that should be in place for an optimal Cloud Environment. Version 3.0.1 is the latest version. Matrix consists of controls that have been included in various Regulations, Standards and Frameworks. The CCM provides the architectural relevance of the applicability of controls – Physical, Network, Compute, Storage, Application, and Data. CCM provides the Corporate Governance relevance and the Cloud Service Delivery Model Applicability of controls (SaaS, PaaS, IaaS).



5.2 Assurance

Assurance in cloud computing can be provided by measuring and checking cloud service providers' ability to securely deliver cloud services in accordance with industry cloud best practices, standards and regulatory compliance.

This helps customers know which cloud provider delivers the best cloud assurance score and history, a measure of cloud trust they can depend on. A strategic and logical cloud assurance framework enables safe and secure adoption of Cloud Computing. It can provide senior management and business leaders with the confidence that cloud assurance has been undertaken.

Cloud Assurance includes a five-step process:

- Monitoring
- Audit/ Compliance
- SLA
- Certification
- Testing

Auditing Cloud Computing offers an independent supplement to security considerations for Cloud Computing.

Besides the generic approach to minimizing risk to the organization through a careful review of the contract, supporting appendices and service level agreements (SLAs), it is recommended that the auditor supplements the review by first identifying the type of cloud that is being contracted. The auditor's approach may cover:

- Cloud-based governance of enterprise IT (GEIT)
- Cloud-based IT service delivery and support
- System and infrastructure life cycle management for the cloud
- Global regulation and cloud computing
- Business continuity and disaster recovery

Specifically, auditing Cloud Computing points to risk related to cloud computing, which enables users to do a deep dive on business continuity processing for the application. There are usage scenarios to be considered within the context of the cloud that the auditor has to ask as part of due diligence.

The auditor needs to view the venture and IT risk from a business point of view, not just as boxes on a checklist. Some questions to ask are obvious, such as those regarding the risk to the enterprise if the vendor were to go bankrupt or not be able to continue servicing the client. But high-level business and control questions grouped around categories of governance need to be asked as well. The checklist used by auditor to guide the review not be locked in to a style of cloud, deployment model or type of customer. The auditor must have the vision and perform due diligence to ask questions that may not have an answer, and enterprises should be cautious of the questions for which there is no answer.

Following is an illustrative checklist covering major audit objective(s) and key areas to be focused by an auditor while auditing cloud computing. It may be noted that for every audit assignment professional judgment should be used for framing audit scope, audit plan and format of audit report.

1. **Identity and access management**	
Audit Objectives(s)	**Key Areas to Focus on during Audit**

Identity and Access Management: Verify that approved personnel are granted access to service based on Identity and Access Management.
 	
Audit Objective(s)
 	
Identity and Access Management: Verify that only approved personnel are granted access to service based on their roles, and that access is removed in a timely manner upon the personnel's termination of employment and/or change in their roles that does not require the said access.
	• Physical Security
	• Hosting and Data Logical Security
	  ○ Segregation of tiers; hosting encryption methods
	  ○ Accessibility from the open Internet, over permissive rules that open wide range of ports.
	• Authentication and Authorization
	  ○ Length/ strength of passwords, systems to enforce/ control password security/ reset rules
	  ○ Use of hardware/ software token.
	• Only authorized users are granted access rights after proper approval.
	• Access for transferred employees is modified in a timely manner.
	• Unauthorized access to cloud computing resources is removed promptly.
	• Periodic review of super-user and regular access to cloud applications.
	• Connection and data transmission.
	• Secure connectivity such as, VPN IPSec, SSL, HTTPS where secure data is being transmitted for regular users or administrators.

2. **Data Protection**	
Audit Objectives(s)	**Key Areas to Focus on during Audit**
Sufficiency of the data protection policies, procedures and practices at the Cloud Service providers as well as the user organization.	• Type and sensitivity of Data sent to and potentially stored in the cloud. • Data protection requirements (business confidential information, etc.,). • User organization's policies and procedures to protect data stored at third-parties. • Co-mingling of your data with others tenants of the cloud application. • Vendor's overall capability maturity to meet the requirements. • Understand the level of access (create/read/ update/delete) that the vendor's personnel have to the data, particularly for confidential information. • If the vendor is unable to provide the right level of data protection, User organization can put mitigating controls in place, such as removing sensitive data elements before sending it to the cloud or encrypting sensitive data. • Understand the circumstances, if any, in which the vendor may disclose organisation's data without your prior consent. Is that acceptable to the organization? • After potential termination of contract, portability of data and metadata (for e.g., format of the output/extract from the vendor) and purging of data by the service provider to be ensured.
3. **Technology Risks**	
Audit Objectives(s)	**Key Areas to Focus on during Audit**
Unique risks related to the use of virtual operating system with cotenants.	• Is primary service provider utilizing another sub-service provider? For e.g., there are several examples where a SaaS provider is utilizing an laaS provider. Do you know whether your primary service provider ls protecting you adequately from the risks inherent with utilizing an IaaS provider? • Hypervisor technology (virtual machine software) is being utilized and whether it is patched ?

Unique risks related to the use of virtual operating system with cotenants.	• What is the process for monitoring and patching for known vulnerabilities in hypervisor technology ? • Segregation of duties (SOD) considerations both from a technology as well as business perspective, for e.g. , from a technology SoD perspective does one person have access to the host and guest operating systems as well as the guest database. From a business perspective, for financially significant applications, just because an application is in the cloud does not diminish the importance of segregating access within the application. • Logging of access to the applications and data, where relevant. • Protection of access logs from inadvertent deletion or unauthorized access.
4. **Operations**	
Audit Objectives(s)	**Key Areas to Focus on during Audit**
Assess procedures related to incident management, problem management, change and access management in context of use of Cloud services.	• Operational process documentation: policy, procedures, roles and responsibilities. • Effectiveness of Service Level Agreement (SLA) monitoring. • Appropriate use of monitoring tools and reports. • Communication protocol/who at your (user) organization is notified by the vendor during scheduled outage windows and non-scheduled outages. • In case of SaaS, coordination of release schedule and sign-off/approval for change, management and testing of new functionality within the application. • Does your organization (user) have a periodic backup of data at the cloud Service provider, particularly in case of SaaS. • Assignment of responsibility at the user organization for periodic review of availability and performance reports provided by the service provider.

5. **Regulatory**	
Audit Objectives(s)	**Key Areas to Focus on during Audit**
Compliance with regulatory requirements over the protection of information.	• Regulatory requirement, such as, Sarbanes Oxley Act (controls over initiation, authorization, processing and recording of transactions) or privacy, such as Health Insurance Portability and Accountability Act (HIPAA) or other applicable Privacy Breach notification laws. • Intrusion detection and protection at the cloud service provider. • Does the vendor know whom to notify when a breach happens? For e.g., from Microsoft's Office365 website: "Our notice be typically delivered **by email to one or more of the administrator(s)** the customer has listed in the online services portal. It is the customer's responsibility to ensure contact information remains up to date." Do you want important legal notices served to your system administrators?

5.2.1 Approach for Assurance of Cloud Service provider

As per Standard on Auditing (SA) 300 "Planning an Audit of Financial Statements", issued by ICAI, the auditor shall establish an overall audit strategy that sets the scope, timing and direction of the audit, and that guides the development of the audit plan. Following is an illustrative approach for providing assurance to Cloud Service Provider –

(i) Preparation

- Develop audit plan, control objectives and review steps.
- Interview IT business leaders to understand organization 's position/ vision of cloud.
- Select relevant cloud services/projects as audit samples.

(ii) Fieldwork

- Gather documentation and evidence in regards to audit objectives.
- Interview stakeholders and analysts.
- Perform tests design and operational effectiveness against audit review steps.

(iii) Findings

- Document gaps with controls objectives and related risks.
- Provide recommendation to address issues identified during audit.

5.2.2 Some Common Audit Findings

Following are some illustrative audit findings –

- Password settings for cloud resources (applications, virtual servers, etc.) does not comply with user organization's password policies. Sometimes the cloud vendor resources do not support the user organization's policy requirements, but several times, the cloud administrators at the user organizations are not aware.
- Port settings on cloud server instances not appropriately configured (administrator added exceptions to administer cloud from their home computer and mobile device).
- Lack of policy and procedures for appropriate handling of security and privacy incidents.
- Terminated users found to be active on applications in the cloud (even though the individual's network access was terminated) and there was no IP range restriction.
- Employees transferred out of a certain department had access to cloud resources even though they had been transferred to another department a few months ago.
- Service provider's SOC report had not been reviewed for impact to user organization.
- Sensitive data (PII) in the cloud was found to be not encrypted. Sometimes, the user organization is not aware that sensitive data resides in the cloud. Most commonly, with the use of cloud for test environments, sensitive data is not scrambled/de-identified before being sent to the cloud. It might even be the case that third-party development vendor might be doing that.
- Use of shared accounts to administer the cloud.

Following are some points that an auditor should consider while performing an audit of the organization who uses cloud for storage and processing of data:-

- Auditor have to verify that only authorized individuals have access to cloud computing resources based on their roles and responsibilities. Access is removed in timely manner when any employee is terminated or/and when their roles gets changed.
- Auditor have to check about the type and sensitivity of data stored in the cloud. As loss, leakage or unavailability of data can cause loss to business reputation and revenue or may also result in non-compliance of regulations.
- Auditor have to verify the sufficiency and appropriateness of policies, practices and procedures for the protection of data stored in the cloud.
- Auditor have to check the risk associated with the change of technology. He should evaluate how the new technology is being adopted and what are the benefits users are getting against the costs they have incurred.

- Auditor have to review the terms of Service level Agreement (SLA) for the protection of data stored on the cloud and clauses for the termination of contract between organization and cloud service provider.
- Auditor have to check the procedures that are related to incident management, problem management and change management in the context of cloud computing.
- Auditor have to check the legal and regulatory requirement that an organization are required to comply for the protection of data which is stored in the cloud.
- Auditor have to assure that confidential and sensitive data should be encrypted in the cloud.
- Auditor have to go through the access logs and assure the protection of access logs from inadvertent deletion or unauthorized access.
- Auditor have to understand the level of access that vendor's personnel of Cloud Service Provider (CSP) have on the data particularly for confidential information.
- Auditor also have to consider Segregation of Duties (SoD) so that one person does not have two or more mingled responsibilities.
- Auditor have to check the Intrusion detection and protection practices at the Cloud Service Provider.
- Auditor have to assure that if there is any lack of policy and procedures for appropriate handling of security and privacy incidents.
- Auditor have to assure that password settings are strong at cloud and according to the organizational policies.
- Auditor have to ensure about the proper disposal of data to prevent from any unauthorized disclosure.

5.3 Governance

Cloud computing governance is a general term for applying specific policies or principles to the use of cloud computing services. The goal is to secure the applications and data when they are located locally.

Cloud computing governance is a view of IT governance focused on accountability, defining decision rights and balancing benefit or value, risk, and resources in an environment embracing cloud computing. Cloud computing governance creates business driven policies and principles that establish the appropriate degree of investments and control around the lifecycle process for cloud computing services.

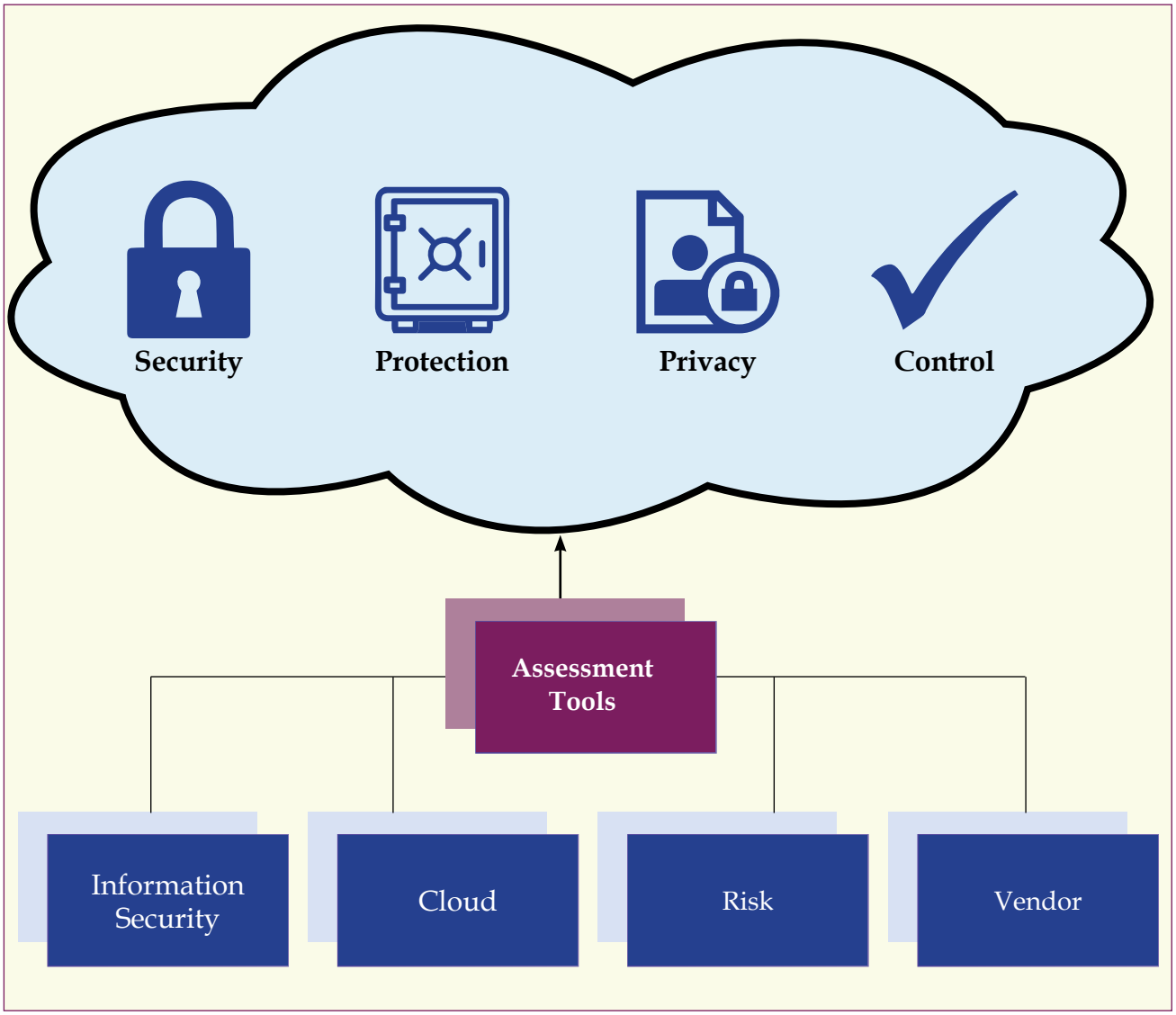


Figure: Cloud Computing Governance Framework

The Cloud Governance Framework shown above includes four main areas – security, protection, privacy, and control. Cloud providers must enable their customers to comply appropriately with these regulations.

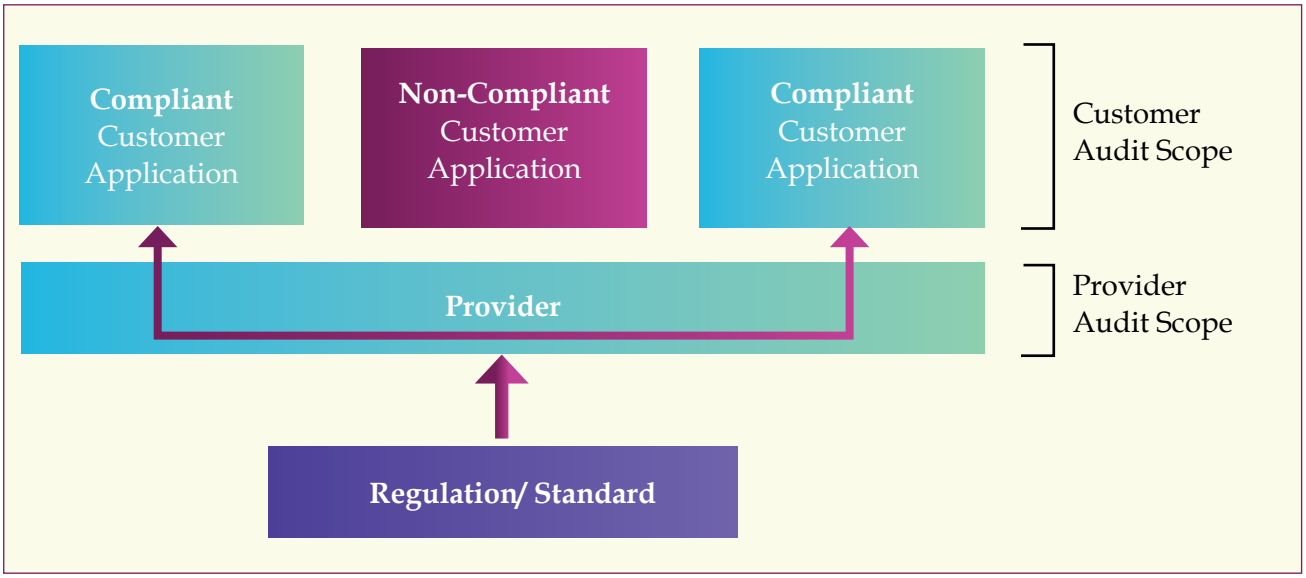
Business Continuity and Data Recovery plans must be in place to maintain in case of a disaster or an emergency. In addition, there must be an audit trail and logs that can be properly secured and maintained for as long as required and are accessible for the purpose of forensic investigations.

The landscape of governance models and standards includes models and standards that satisfy the following criteria:

- Driven by business governance while addressing IT governance;
- Global and not specific to any geography;
- Not specific to any one industry domain;
- Align with existing governance models and standards.

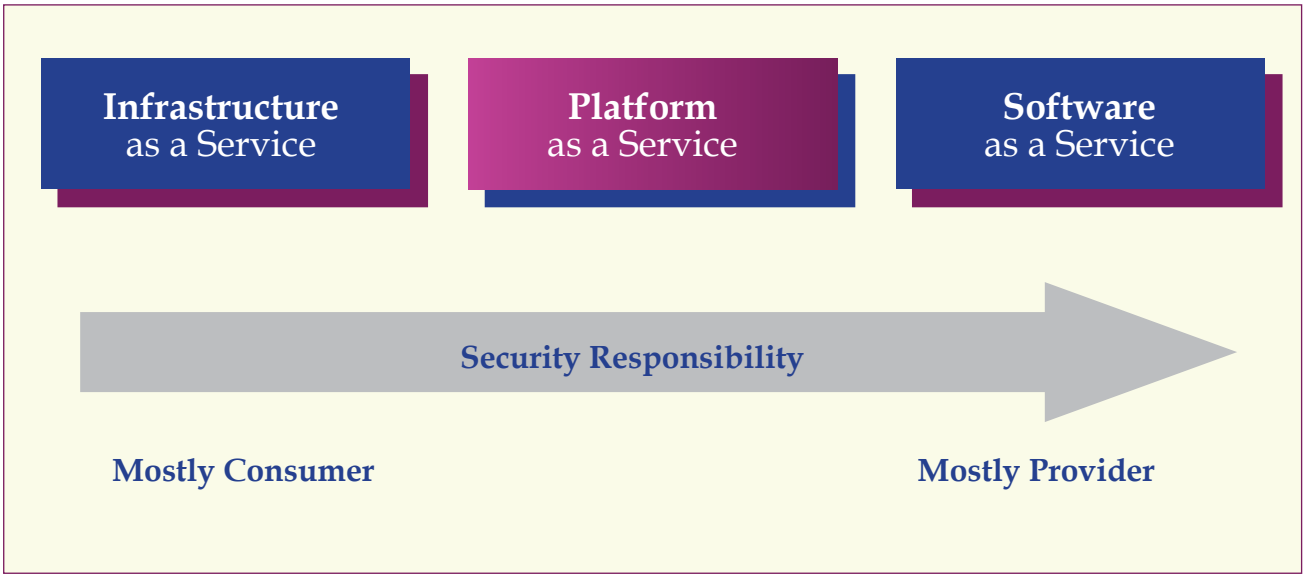
5.4 Compliance and Audit Management in Cloud Environment

Information technology in the cloud is increasingly subject to a plethora of policies and regulations from governments, industry groups, business relationships, and other stakeholders. Compliance management is a tool of governance; it is how an organization assesses, remediates, and proves it is meeting these internal and external obligations. But cloud compliance issues aren't merely limited to pass through audits; the nature of cloud also creates additional differentiators.



Proper organizational governance naturally includes audit and assurance. Audits must be independently conducted and should be robustly designed to adopt best practice, deploy appropriate resources, and tested protocols and standards. Before delving into cloud implications, an organization should define the scope of audit management related to information security.

Cloud Security and Compliance Scope and Responsibilities



6. Conclusion

Cloud Computing is the natural evolution of traditional data centers, it is distinguished by exposing resources (computation, data/storage, and applications) as standards-based Web services and following a "utility" pricing model where customers are charged based on their utilization of computational resources, storage, and transfer of data. They offer subscription-based access to infrastructure, platforms, and applications that are popularly referred to as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). While these emerging services have increased interoperability and usability and reduced the cost of computation, application hosting, and content storage and delivery by several orders of magnitude, there is significant complexity involved in ensuring that applications and services can scale as needed to achieve consistent and reliable operation under peak loads.

Cloud Computing can provide an opportunity to professional accountants to automate their process and deliver client services in an efficient, error-free and faster way. ICAEW's document "The Future of the Profession" states that new ways of doing business, shaped by technology and shifting regulatory environments, mean accountants in business and practice are facing tough challenges and exciting opportunities. Further, it mentions skills required of accountants in the future are tech-savvy thinkers, strong communicators, flexible thinkers, strategic thinkers and good networkers.

IFAC in article "The What, Why, and How of Cloud Computing for SMPs" states following potential benefits for Small and Medium Practitioners for moving to the cloud -

- It can help SMPs upgrade their service level by getting real time information allowing for an instant picture of business performance and tailored advisory services to their clients.
- The nature of services SMPs provide to their clients is changing. Accountants will be ideally placed to interpret information and Big Data and use it to help design analytics (including key performance indicators or dashboards) corresponding to the client's specific business needs.
- SMPs will be able to offer their services at a lower cost. Administrative and in-house IT support costs will decrease as online services are updated and backed-up automatically via online accounting software, customers and vendors can enter their data directly into the system, which will minimize the time spent dealing with clients' administration and data entry.
- It will improve flexibility as access to information will no longer depend on location. SMPs will be able to service their clients from any location, and it will also allow for a more flexible working environment—remote working will become much easier.
- It offers smaller companies access to services and tools, such as Big Data analytic tools. Also, SMPs using online applications can employ "chunkification", which means choosing an application's key features that a business really needs and then linking them to other "chunks" offering other key functionalities.
- As more and more clients use cloud technology, embracing the change will not only keep SMPs relevant, but it also may bring new international clients and business partners and attract young talent.

7. References

1. ICAI Concept paper on "Embracing Robotic Process Automation-Opportunities and Challenges for Accountancy Profession" (2018).
2. Cloud Security Framework for Indian Banking sector - IDRBT
3. Gartner's study on Cloud Computing future (www.gartner.com)
4. Forbes Study on Cloud Computing growth in India (www.forbes.com)
5. Cloud Security Alliance – Security Guidance for critical Areas of Focus in cloud computing 4.0 (www.cloudsecurityalliance.org)
6. Cloud Control Matrix v3.0.1 Released by Cloud Security Alliance
7. NIST Cloud Computing Security Reference Architecture(special publication 500-299)
8. ICAEW – The Future of the Profession; https://economia.icaew.com/features/october-2017/the-future-of-the-profession (www.icaew.com)
9. IFAC "The What, Why and How of Cloud Computing for SMPs" (www.ifac.org)

Composition of Digital Accounting and Assurance Board 2019-20

Council Members

Chairman

CA. Manu Agrawal

Vice-Chairman

CA. Dayaniwas Sharma

CA. Prafulla Premsukh Chhajed
President (Ex-officio)

CA. Atul Kumar Gupta
Vice-President (Ex-officio)

CA. Anil Satyanarayan Bhandari

CA. Tarun Jamnadas Ghia

CA. Nihar Niranjan Jambusaria

CA. Dheeraj Kumar Khandelwal

CA. Aniket Sunil Talati

CA. Rajendra Kumar P

CA. M P Vijay Kumar

CA. Sushil Kumar Goyal

CA. Pramod Kumar Boob

CA. Hans Raj Chugh

CA. Sanjeev Kumar Singhal

CA. Rajesh Sharma

CA. Prakash Sharma

Shri Sunil Kanoria

Co-opted Members

CA. Cotha S Srinivas

CA. Shrikant Maheshwari

CA. M R Vikram

CA. Punit Mehta

CA. Sunil Chandiramani

CA. Rajkumar Kothari

Special Invitees

CA. Hemant Joshi

CA. Arun Ahuja

CA. Mohan Lal Kukreja

CA. Nitesh Gupta

CA. Tushar Mehta

Secretary, DAAB

CA. Jyoti Singh

Digital Accounting and Assurance Board

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

ICAI Bhawan, Hostel Block, 7th Floor
A-29, Sector-62, Noida - 2013 09 INDIA

Tel (Direct) +91-120-3045 961 / 992 / 963
www.icai.org