Cloud Computing

What is Cloud Computing?

Cloud computing is where the organization outsources data processing to computers owned by the vendor. Primarily the vendor hosts the equipment while the audited entities still has control over the application and the data. Outsourcing may also include utilizing the vendor's computers to store, backup, and provide online access to the organization data. The organization will need to have a robust access to the internet if they want their staff or users to have ready access to the data or even the application that process the data. In the current environment, the data or applications are also available from mobile platforms (laptops with Wi-Fi or cell/mobile cards, smart phones, and tablets).

Cloud computing much like outsourcing offers cost savings and the ability to share costs with other clients who each pay only part of the infrastructure costs. It enables delivering computing services via networks and has the potential to provide information technology (IT) services more quickly and at a lower cost. Cloud computing provides users with on-demand access to a shared and scalable pool of computing resources with minimal management effort or service provider interaction. It reportedly has several potential benefits, including faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robust collaboration capabilities.

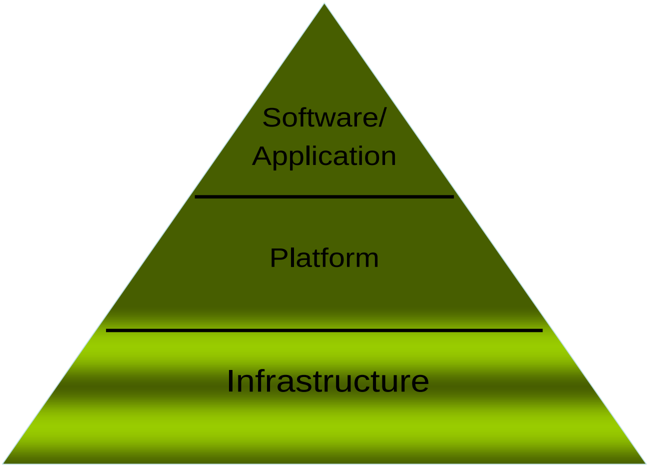
Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer. Cloud computing can potentially deliver several benefits over current systems, including faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robust collaboration capabilities. However, along with these benefits are the potential risks that any new form of computing services can bring, including information security breaches, infrastructure failure, and loss of data. Media reports have described security breaches of cloud infrastructure and reports by others have identified security as the major concern hindering federal agencies from adopting cloud computing services.

If an organization has contracted with a vendor to provide software as a service, i.e., where the application software and associated data are hosted on a server that is operated by a vendor at their or some other location then the agency is utilizing some aspects of cloud computing already. Additionally, agencies that utilize a vendor provided infrastructure (computing, storage, backup) or are getting infrastructure services from a vendor are too utilizing cloud computing.

An organization may choose to utilize either a public cloud or a private cloud. In a public cloud model, the vendor makes available infrastructure, applications, storage and other resources (support) to many customers. Generally customers access these services via the internet which is acquired separately. In the private cloud model the services and access are offered solely to a single customer and hosted either locally or in a remote, controlled, location. Generally the customer has a lot more control over the environment but also needs additional expertise to design and manage the environment and it requires careful planning to ensure that applicable security concerns are addressed.

Cloud Computing Models

There are generally three cloud computing models, infrastructure, platform, and software.



In the Infrastructure-as-a-Service (IaaS) model, users typically utilize the vendor's infrastructure to support their business operations. Infrastructure may include storage, hardware, servers, and networking components. These are accessed via the internet and customers use their own platform (Unix, Windows, environment, etc) and associated software. The service provider owns the infrastructure equipment and is responsible for housing, running, and maintaining it. The customer typically pays on a per-use basis.

In the Platform-as-a-Service (PaaS) model the vendor provides both the basic infrastructure and platform. Customers use their own software and applications and access them over the Internet. Just as in the IaaS model, PaaS facilitates deploying applications without the cost and complexity of buying and managing the underlying hardware and software (operating systems and other support software) where the applications are hosted.

In the Software-as-a-Service (SaaS) model, sometimes called “software on demand,” the vendor provides infrastructure, platform, and software/applications (office, database, etc.). The customer accesses the applications over the internet and pays depending on use, access, or number of access points (desktop, mobile, etc.).

Elements of cloud computing

Data and resources are always accessible

The vendor who is responsible for hosting the data and applications typically provides access to these over the internet. Users are able to access the data and applications either from their office via desktop computers or from remote locations using mobile computing platforms (tablet, Smartphone, web browser) at any time. If needed, they are able to update or store additional information which is also available to other users or team members who may be physically in a different location. For example an auditor may update a record of meeting to a document handling system utilizing their tablet and in a relatively short time span the same is available for review or sharing to other team members who can access the same from their office. In effect it allows multiple users to access the data at the same time without regard to physical locations of the different users.

Use of web technologies

Almost all smart phones, tablets and other means to access the web are able to leverage cloud computing resources. The applications make use of web technologies (browser or app) to access the cloud computing resources. These technologies support any level of security that might be required and allow sensitive data to be stored and retrieved based on the organization’s requirements.

Lower infrastructure costs

With cloud computing an organization does not need to purchase computing resources to host by itself the data and or applications. Most of the data and applications that access them reside on the computers owned and operated by the cloud computing vendor. The vendor is responsible for upgrades to the equipment, maintenance, backup and disaster recovery procedures. Additionally the vendor is also responsible for ensuring access to the data and applications based on the requirements of the organization. The organization does have to provide to their users a means to access the data and applications. These are typically via desktop or mobile computers with internet access. The costs associated with these are the responsibility of the organization; however, most organizations already have a robust office IT environment which can easily access the cloud computing resources.

Do not need much hardware on client side

The only hardware that is needed on the client side, i.e., the users of the data are either common desktop computers or if mobile access is required, smart phones, tablets, or other means to access the web (internet kiosks). Most organizations already have provided their staff with desktop computers and are in the process of moving towards smart phones that are fully able to access the cloud computing infrastructure.

Freedom from backup and local disaster recovery issues

The vendor who is hosting the cloud computing resources should ensure that the data is backed up and that a suitable disaster recovery plan is in place based on the requirements of the organization. Typically the vendor is hosting data and applications from many different clients and is able to share the cost of both the equipment and services (maintenance, disaster recovery planning and testing) across all of the clients. Organizations thus not only do not have to have their own disaster recovery plan for the hosted services but are getting these services for a lower cost than if they were to plan for these themselves. This is because of resource pooling1. The clients must still have, if the need exists, a robust and failsafe way to get to their data and applications of their internet service provider has a significant outage. Typically, mobile computing will suffice to ensure continuity till the ISP is back online.

Rapid Elasticity

As the needs of the organization grow or more computing or data storage is required, the vendor is rapidly able to respond by providing commensurate with demand. In some cases the vendor may automatically upgrade data and computing capabilities to meet demand and to ensure quality of service to the client. Examples include providing additional storage or allowing greater than maximum number of users to access the services while at the same time ensuring that the response time is within the required parameters.

[1] The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that 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 data enter). Examples of resources include storage, processing, memory, and network bandwidth.

Audit Concerns

When an organization chooses to utilize cloud computing, they need to be aware of risks that they may face with the service provider, the risk they face if they are unable to effectively oversee the service provider, and other risks related to management and security weaknesses in the service providers approach. As an auditor you will need to understand what the agency has done to mitigate the risks with cloud computing. When we as auditors are asked to appraise whether an entity or organization getting the benefits of cloud computing are managing the vendor to ensure that they get the required services we need to be aware of the risks that they may face.

The use of cloud computing services is not without risk for the audited entity or the user of the service. While there are benefits of cloud computing, this needs to be balanced with the degree of risk the audited entity is willing to accept. In the example above, it is highly unlikely that Google or Amazon would tailor their service for the user or the user. Thus if for example the level of security that Google typically provides with their email or other web services (Google Docs, cloud storage, etc.) are not sufficient then utilizing their service, while cost effective, may not be in the audited entity's best interest. If they still go ahead with the service, they may find that some of their communications might not be as secure as they expect. While this risk can be managed, the audited entity must make a conscious decision to do so and ensure that any additional controls they put on this service (by limiting or filtering content) are monitored and enforced.

Some of the common risks that the agency will need to mitigate are listed below. The auditor will need to ask the agency how they are mitigating these risks. See the hand book on questions that will assist you, the auditor in appraising whether the agency has addressed the risks.

Additionally, while this guide and handbook deal primarily with the use of cloud computing services for IT by the audited entity (or the internal IT organization), there may be cases where a non-IT contract (for example building maintenance, physical security, etc,) may utilize cloud computing IT services by a third party. The issue here for the audited entity is to determine what the prime contractor will retain in house (for example the direct labor provided for the effort) and what they will sub-contract to a third party via cloud computing (for example the management of schedules, logging, etc.). For the audited entity, it may be sufficient to lay out in the contract that they need to be provided logs, and other documentation about the level of service and issues regardless of where they are being processed or stored. This needs to be done at the start of the contract so that the prime contractor is aware of the requirements and can, if possible, request their cloud computing vendor to meet the requirement. Generally for

IT Audits most Supreme Audit Institutions (SAI) would not look at construction, facilities management, and other efforts unless specifically requested to do so. It should be noted that any additional requirement for data and other artifacts may increase the cost of the contract and the SAI or audited entity should be ready to accept the cost vs. the risk of not having some specific data element. They should also consider whether there are alternate means to get the data that may be at the cloud computing vendor or the third party.

Finally, the use of cloud computing does not exempt or free an audited entity from managing IT using best practices for IT Governance. Cloud computing cannot be undertaken prior to having an IT strategy or a plan and managing the effort much like any other investment with cost benefit trade-offs and periodic appraisal of the ability of the contractor or meet user requirements.

Cloud Computing Risks

Some of the risks that the audited entity will need to manage when they decide to utilize cloud computing includes:

1 Service Provider Risks

- Service providers may have limitations in their knowledge, skills, and quality of service
- Contracts could lock in an underperforming service provider
- Service provider could subcontract out selected services to a non-trusted party
- Service provider could be sold to a non-trusted party
- Service provider could file for bankruptcy

2 Technical Risks

- Lack of standards for services, fees, portability
- Lack of data protection (access, backup, secure, delete, archive)
- Reliability and performance across a globally accessible network may suffer, resulting in significant downtime and outages

3 External (Overseas) Risks

- Foreign regulations on information storage and transfer may limit what can be stored and how it can be processed
- Data may be used by law enforcement without your knowledge
- Privacy and security standards in flux
- Dispute because of the different legal jurisdiction

4 Management/Oversight Risks

- Loss of governance of data and data processing
- Limited view into physical, personnel, and information security controls
- Audit access: Auditors may not be able to access systems, applications and data in the cloud to check that they are there and working as intended.
- Investigation support: There could be limits on how much insight an organization has into problem situations (data breaches, performance shortfalls, etc.)
- Increased complexity in managing data mobility and ensuring data is returned to the owner if shared among different cloud services

5 Security / Connectivity / Privacy Risks

- Sensitive data could be mishandled or released.
- Physical Security: Who has access? Do personnel have requisite clearances? What are the controls over the infrastructure?
- Information Security: Is the service provider certified and accredited? Who validates this? Are data sufficiently segregated and encrypted? Does the service provider have a disaster recovery plan? Does Non disclosure agreement exist?
- Connectivity: Cloud computing is heavily dependent on Internet access, but agencies and service providers are unable to control or recover from the loss of Internet service
- Privacy Protections: Depending on laws, your right to privacy may be higher in your home or office than when stored on a 3rd party's web servers.

Most of the items that are critical to the customer must be put in a contract or a service level agreement. The Service Level Agreement (SLA) is the document where both parties (customer and vendor) agree to the level and quality of service. As an auditor we need to ask for the SLA or other document (contract or formal agreement) where these parameters are documented and ensure that the reporting from the vendor on various parameters is meeting the requirement or that the organization has taken necessary corrective action to address the deficiencies.

References:

NIST Special Publication (SP) 500-291, *NIST Cloud Computing Standards Roadmap*

NIST SP 500-292, *NIST Cloud Computing Reference Architecture*

NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*

Acronyms:

IaaS	Infrastructure-as-a-Service
IT I	Information Technology
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
SAI	Supreme Audit Institution
SLA	Service Level Agreement