Linux Academy
Study Guide

Cloud Essentials

Contents

Cloud computing is an Internet-based computing solution that delivers *IT as a service*: Hardware and software with shared resources, configured to work together, providing applications their collective computing power with the illusion of running on a single system.

Imagine a massive bunch of computers linked through high-speed networks where large numbers of discrete organizations can store their applications and data on a pay-as-you-go model.

Three Types of Cloud Computing

Public Cloud

Based on the standard cloud computing model, in which resources, such as infrastructure (including servers, storage, and applications) are made available to the general public over the Internet, by a cloud service provider.

Examples of public clouds are Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Google AppEngine and Windows Azure Services.

Private Cloud

Infrastructure that is used only for a single organization, whether handled internally or by a third-party, and hosted internally or externally. The private cloud is a new method of computing, in which corporate IT infrastructure is present as an ubiquitous, easily-accessible and reliable utility service. Business and application owners, who want to use a new business service, can use the infrastructure as a standard service without understanding the complexities of servers, storage, and networks. A private cloud, or a virtual private cloud, is a type of cloud computing infrastructure created for in-house data center use.

Hybrid Cloud

A cloud computing environment comprised of at least one private cloud and at least one public cloud. With this model, an organization typically manages applications with sensitive data in-house, but may choose to store archived or non-sensitive data with a cloud provider.

Why Cloud Computing?

There are several benefits to cloud computing:

- Rapid provisioning/deployment
- Reduced cost
- Unlimited storage

- Access to skilled resources
- Better use of in-house personnel
- Scalability
- High availability and redundancy

Cloud computing offers massive computing power, unlimited (but not free!) storage, significant improvement in utilization of hardware, and human resources at low costs.

There have been several concerns voiced about cloud computing. These concerns are mostly in the areas of security and privacy. Cloud computing providers know this, and understand that without stringent security and privacy measures, this model cannot survive.

At the same time, be aware that cloud computing shares characteristics with the following fundamentals:

- Autonomic computing
- Client-server models
- Grid computing
- Mainframe computers
- Utility computing
- Peer-to-peer

Cloud Client

A cloud client consists of computer hardware/software that depends on cloud computing for application delivery, and is, in essence, useless without it.

A cloud client is the definitive client computing solution that is used to restore the outdated computing model of insecure, unreliable, environmentally-unfriendly and exclusive PCs.

Characteristics of Cloud Computing

- **`On demand self-services`** • Computer services such as email, applications, network, or server service can be delivered without needing human interaction with each service provider.
- **`Broad network access`** • Cloud capabilities are accessible over the network and accessed via standard mechanisms that support the use of heterogeneous thin or thick client platforms such as mobile phones, laptops, and PDAs.
- **`Resource pooling`** • The computing resources of the providers are pooled together and use the multiple-tenant model, with different virtual and physical resources dynamically assigned and reassigned depending on the consumer demand for serving multiple consumers.

- **`Rapid elasticity`** • The ability for computing resources to scale out (add resources) and in (remove resources) quickly based on the needs of the services and demands.

- **`Measures service`** • The resource usage of cloud computing can be measured, controlled, and reported and provides transparency for the provider and consumer of the utilized service. Cloud computing services make use of a metering capability that controls and optimizes the use of resources.

Cloud Computing Compared to Virtualization

Generally, **cloud computing** is a service that can dynamically expand or contract computation or storage capabilities on an as-needed basis. It is used by organizations who want to minimize costs and have access to programs and applications that are not physically installed on the company's servers.

Virtualization is a type of technology used to help those companies and users who want to utilize their computers, applications, storage devices, and servers more efficiently. Virtualization is a technology that enables you to run multiple OSes concurrently on a single physical host, where each of the OSes runs as a self-contained computer.

Virtualization is the creation of a virtual (rather than physical) version of something; this could be an OS, a server, a storage device, or even a network resource.

The goal of virtualization is usually a more effective use of resources. It simplifies provisioning while adding flexibility at the same time.

Cloud computing and virtualization are two different technologies that are often, incorrectly, used interchangeably. They are similar in that both help deliver optimized resources, on-demand utilization, flexibility and scalability, at low costs. However, there are several key differences:

- Virtualization is a technology, whereas cloud computing is more of a business model that leverages a variety of technology in innovative ways.

- Virtualization is actually one of the technologies that can be used to implement cloud computing.

Virtualization has been around longer than cloud computing and began its early days within the boundaries of an organization's firewall, although it has since been utilized in hosted environments.

In essence, virtualization is an enabler for cloud computing technology.

Cloud computing specifies a new supplement, consumption, and delivery model for IT services, depending on Internet protocols, and can be utilized better if desktop virtualization is done first, as much of cloud computing requires multiple virtual servers and storage devices. But understand that virtualization is also crucial because it enables customers to run multiple OSes concurrently on a single physical server, where each of the operating systems runs as a self-contained computer.

Virtualization has physical access to the virtual servers. On the other hand, cloud computing makes use of those resources but does not have physical access to them.

Benefits of Virtualization

- Allows workload-balancing and the avoids downtime, because most virtualization technology supports virtual machine live migration from one host to another.
- Provides dynamic fault tolerance against software failures (through rapid bootstrapping or rebooting).
- Provides hardware fault tolerance (through migration of a virtual machine to different hardware).
- Provides the ability to securely separate virtual operating systems.
- Provides the ability to support legacy software as well as new OS instances on the same computer.
- Virtualization also has benefits when working on development (including the development of OS); running the new system as a guest avoids the need to reboot the physical computer whenever a bug occurs.
- Server virtualization is an effective tool for disaster recovery planning.
- Minimizes hardware downtime and recovers data quickly; during the implementation of server virtualization, an organization should consider the following:
  - » Data backups
  - » Recovery of data
  - » Restoration performance
  - » RTOs/RPOs

Workspace Virtualization

Workspace virtualization is a method of distributing applications to client computers by utilizing application virtualization; it can combine some major applications together into one inclusive, complete workspace.

At a minimum, the workspace consists of everything above the OS kernel, such as applications, data, settings, and any other non-privileged operating system subsystems required to provide a functional desktop computing environment.

Virtual Machine (VM)

A virtual machine (VM) is a software implementation of a computer that executes programs like a real machine.

Virtual machines are separated into two major categories, based on their use and degree of correspondence to any real machine.

A system VM provides a complete system platform that supports the execution of a complete operating

system.

An essential characteristic of a virtual machine is that the software running inside is limited to the resources and abstractions provided by the virtual machine.

Multiple virtual machines with different operating systems can co-exist on the same computer.

Examples of Cloud Computing

- Google App Engine – application hosting
- Amazon EC2 – virtual IT
- Microsoft Office 365

Cloud Storage

Cloud storage is a model of networked, online storage where data is stored on virtualized pools of storage, which are generally hosted by third parties.

Hosting companies operate large data centers and people who require their data to be hosted buy or lease storage capacity from these companies and use it for their storage needs.

The data center operators virtualize the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects.

Cloud storage has the same characteristics as cloud computing regarding agility, scalability, elasticity and multi-tenancy.

Cloud storage is:

- Made up of many distributed resources, but still acts as one.
- Highly fault tolerant through redundancy and distribution of data.
- Highly durable through the creation of versioned copies.
- Typically eventually consistent with regards to data replicas.

Cloud storage advantages:

- Companies only pay for the storage they use.
- Companies do not need to install physical storage devices in their own data centers or offices.
- Storage maintenance tasks, such as backup, data replication, and purchasing additional storage devices are offloaded to the responsibility of a service provider.

- Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a web service interface.

Potential concerns:

- Performance may be lower than local storage, depending on how much a customer is willing to spend for WAN bandwidth.
- Reliability and availability depend on WAN availability.
- Users with specific records-keeping requirements, such as public agencies that must retain electronic records according to statute, may encounter complications with using cloud computing and storage.

Security Rundown

Security Advantages with Cloud Computing

- Advanced honeypot capabilities
- Provides rapid reconstitution of services
- Provides real-time detection of system tampering
- Provides on-demand security controls
- An unbiased party holds the data
- Provides simplification of compliance analysis
- Provides fault tolerance and reliability
- Provides greater resiliency

Security Disadvantages with Cloud Computing

- A data center may crash all the virtual machines; this can be prevented by backing up your data and utilizing failover and clustering.
- When the main parent server is hacked, cloud computing is not suitable to employ.
- Cloud computing is sometimes not secured.
- Cloud computing sometimes cannot be logged if the environment is not secured.
- Cloud computing still has to exist on the physical server.
- Extra cost of data transfer fees.
- Users do not have control over remote servers, their particular software, or their security issues.

- For users, it is very difficult to migrate massive amounts of data from the provider.

Organizations that May Not Benefit from the Cloud

Cloud computing offers several cost-effective solutions to today's highly competitive businesses, regardless of organization size. The ability to activate and retire resources as needed, dynamically update infrastructure elements and move workloads to improve efficiency without having to worry about creating new infrastructures for each new application, all at an affordable price, supported by specialists at no additional cost. Who wouldn't want these advantages?

If yours is an organization with legacy apps looking for instant scalability from a cloud solution, consider this:

Even if an organization decides that the advantages offered by cloud computing are too good to ignore and decide to run their applications on a cloud (public or private), it does not necessarily mean that their applications **can** run on the cloud. For example, just because an organization is running applications on Microsoft Windows Azure or employing virtualization expert, does not mean those applications can scale. To take advantage of the scalability, agility, and reliability of the cloud, applications must be built on a cloud-enabled platform.

If you cannot afford to spend resources to do this, and the key benefit you are looking for is immediate scalability, consider your options: If you are a large organization considering the cloud from a cost savings perspective, keep in mind that while public cloud has a low initial cost, there is an ongoing cost as well. Depending on your usage of the cloud, you may or may not see cost-savings. Also, keep in mind that you will keep paying the costs, without adding an asset to your books or depreciating your facilities investments.

Organizations that need stringent governance around their IT resources may also not find the cloud to be a good fit for all their computing needs.

Cloud Services from a Business Perspective

Scalability

Cloud computing allows for immediate scaling at any time, without long-term commitment. More CPU, more memory, more storage the horsepower when you need it.

Security

Security is one of the biggest concerns of this computing model. With security becoming a core factor for organizations determining a cloud provider, many cloud vendors are emphasizing security from the get-go. The large scale of cloud helps providers hire skilled professionals to input the latest and best in measures

and governance around the security, privacy, and confidentiality of your infrastructure and services.

Hardware Independence

Cloud computing is hardware agnostic, providing a convenient way of accessing computing services, independent of the hardware you use. This model provides a high degree of flexibility and openness versus being boxed into specific hardware platforms that may not adapt to changes over time.

Variable Costs

One of the factors that appeals to consumers of cloud computing services is the benefit of variable costs. With a variable cost basis, organizations can take more risks. If cloud computing doesn't work out, they can close the relationship/unsubscribe from the service at any time. It's a lot less risky than investing in capital and acquiring infrastructure or licenses and having to keep them when they are no longer needed.

Time to Market

Most businesses are faced with enormous pressure to accelerate time-to-market for new products and services while controlling costs. In many organizations, IT staff are so busy maintaining critical production systems that setting up development, test, and QA servers fall behind. Cloud computing provides a rapid deployment model that enables applications to be set up in record time at a low cost. It makes resource provisioning dynamic and a self-service system, where application development teams can now provision their own servers; even if the infrastructure team does it for them, it can still be done at a fraction of the time and cost of traditional models.

Distribution over the Internet

The Internet is one of the most reliable components of computing infrastructure. Your Internet provider may occasionally have hiccups, but when compared to the rates of failures for disk drives, memory, cooling units, backup power, etc., in your internal data center, the uptime for the Internet is considerably higher. In addition to uptime, the method of providing the computing resources via the Internet is, by itself, a major time- and costs-saving benefit.

Private and Public Clouds from a Technical Perspective

Private Cloud

- A private cloud is an infrastructure that is used only for a single organization, whether handled internally or by a third-party, and hosted internally or externally.
- The private cloud is a new method of computing, in which corporate IT infrastructure is present as an ubiquitous, easily accessible, and reliable utility service.

Business and application owners, who want to use a new business service, can use the infrastructure as a standard service, without understanding the complexities of servers, storage, and networks.

Examples:

- VMware vCloud suite
- OpenStack

Advantages of the Private Cloud

- Self-service provisioning of infrastructure capacity is only feasible up to a point.
- Cloud vendor can provide a fully-managed service.
- Some cost savings are possible from economies of scale from providers for a large enterprise-wide solution.
- Private clouds can be used for particular operating systems and applications, and make use of cases that are unique to the client.
- Data and secure information are placed behind the corporate firewall.
- SLAs and contractual terms and conditions are negotiable between client and the cloud vendor for meeting the particular requirements.
- The client pays for resources as they are used and allows capacity fluctuations over time.

Public Cloud

A public cloud is based on the standard cloud computing model, in which resources, such as applications and storage, are made by a service provider and are available to the general public over the Internet. Public cloud services can be free or delivered on a pay-per-usage model. The public cloud can provide immediate cost savings to an organization.

Depending on the specific requirements of the organization, such as customized configuration requirements and service-level agreements (SLAs) regarding up-time requirements, a company should decide whether to move critical applications to a public cloud vendor.

Examples:

- Google App Engine
- Rackspace
- Amazon EC2
- Salesforce.com

Disadvantages of the Public Cloud

- The sharing of sensitive data takes place beyond the corporate firewall.
- Distance may create challenges with access performance and user application content.
- There are limited platform choices available. Support for operating system and application stacks may not meet the requirements of the client.
- A separate provider needs to be found (and paid for) to maintain the computing stack.

Advantages of the Public Cloud

- Up-front capital is not an investment in infrastructure.
- The client pays for resources as they are used and permits capacity fluctuations over time.
- There is a simple web interface for self-service provisioning of infrastructure capacity.
- There is a possibility of significant cost savings from provider's economies of scale.
- Operating costs for the cloud are absorbed in the usage-based pricing.
- Vendors are encouraged to deliver to contract.

Steps to Successful Adoption of Cloud Computing

- **`Identify your business drivers`** • Get educated, talk to vendors and key members of your IT staff
- **`Develop the strategy`** • Show how the cloud can align with business needs, and articulate a value proposition
- **`To cloud or not?`** • Assess your organizational readiness from financial, technical, business and governance perspectives
- **`Pilot it`** • Run a pilot with one or more scenarios where you anticipate benefits. Evaluate against clearly defined success criteria
- **`Gain stakeholder buy-in`** • Carefully analyze feedback from both IT staff, as well as users. Is cloud computing right for your organization? Is it worth it? Get buy-in
- **`Plan for an enterprise roll-out`** • If the pilot is successful

Cloud Deployment Models

Software as a Service

- The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure
- The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface.
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings

Software as a Service (SaaS) cloud implementation delivers software or, more generally described, an application to its end user. SaaS enables a service provider to make applications available over the Internet. This capability eliminates the need to install software on users' computers, and it can be helpful for mobile or transient workforces.

SaaS Benefits:

- **Inexpensive** • Little or no capital investment
- **Flexible** • Offered as an on-demand service; customize your contract
- **Stable** • SaaS applications are installed on reputed, protected, and redundant hardware
- **Rapid deployment** • Little to no time to provision and deploy
- **Accessible** • Only thing needed is internet access

Platform as a Service

- PaaS a way to rent hardware, operating systems, storage and network capacity over the Internet.
- The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Platform as a Service (PaaS) is the platform that delivers a solution stack as a service. It supports in the deployment of applications. It does not involve the cost and complexity of buying and managing the underlying hardware and software and even the provisioning hosting capabilities. It provides all the facilities that are required to support the complete life cycle of building and delivering web applications and services, which are completely accessible from the Internet.

Infrastructure as a Service

- The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications
- The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; possible limited control of select networking

components such as host firewalls.

Infrastructure as a Service (IaaS) enables users to rent equipment and run a data center. In an IaaS arrangement, clients are typically billed based on the resources they consume, much like a utility company bills one for the amount of electricity one uses. Examples of IaaS include Rackspace's CloudServers offering, where a client rents a virtual server running an operating system of his/her choice. He/she then installs the applications according to the requirements of that virtual server. Major examples of IaaS are: Amazon Elastic Compute Cloud (EC2), Eucalyptus, GoGrid, FlexiScale, Linode, RackSpace Cloud, Terremark (Verizon Cloud)

Standardization

Cloud computing is growing very fast, and adoption of cloud computing has led to a strong push from IT organizations of all sizes, especially from major companies, to develop standards that address issues such as security and data portability in the cloud, but the rush for standards has multiple organizations trying to define standards. Where there is no defined standard as yet, one day we will have a convergence, which will likely benefit all concerned.

Security Basics

Cloud Computing providers are aware that concerns around security and privacy are of major concern to both adopters of cloud computing, as well as those holding back. They understand that without stringent security and privacy measures, this model cannot survive. Without reliable security, their businesses will collapse, so security and privacy are high priorities for all cloud computing entities.

Many people do not realize that many reputable cloud service providers rely on strict privacy policies, as well on sophisticated security measures, such as proven cryptographic methods to authenticate users. Often, cloud Computing vendors offer greater data security and confidentiality than companies that choose to store their data in-house. Always remember that organizations can do their part to enhance security, as well; organizations have the choice of encrypting their data before it ever gets to a cloud service.

Things to consider when negotiating contracts with cloud vendors:

- Get more information about exception monitoring systems
- Be aware of updates and make sure that staff doesn't suddenly gain access privileges they're not supposed to have
- Ask where the data is kept and inquire the details of data protection laws
- Encrypt the data at the source
- Seek an independent security audit of the host
- Find out which third parties the company deals with and whether they can access your data
- Be careful to develop good policies around passwords: How they are created, protected, and changed.

- Look into availability guarantees and penalties
- Option to include your own security policies

Risk-Related Issues Associated with Cloud Computing

- **`Regulatory compliance`** • Requires that the infrastructure obeys the rules that are specified either by regulatory bodies or corporate rules. While more operational than technical, it is difficult to design and operate the cloud computing infrastructure according to such compliance requirements.
- **`User privileges`** • A user should keep this in mind that, while assigning privileges to users, they must be given least privileges, because if the user has escalated privileges, they could access data and harm it.
- **`Data integration`** • Data-hosting companies can place more than one company's data on a server, as web-hosting companies place more than one company's website on a server to earn the profit. Encryption should be used to protect the data to prevent this from being problematic. Remember that the data remains as safe as the data it is integrated with.

Criteria When Piloting Cloud Services

- Understand and identify business goals for cloud computing
- Identify a group to pilot, or develop a prototype for the investigation
- Develop and communicate detailed requirements
- Manage the pilot/prototype and assess and communicate those results

Skills for Adopting Cloud Computing

Any company that wants to adopt cloud computing must consider upfront investment, running operating cost, and the time to market. Although businesses are pushing ahead with cloud computing, many of their IT departments, particularly in the areas of application development and security, have not been trained to work with cloud computing.Educating staff on the key principles of virtualization and cloud computing will ensure that your employees have the right skill set and competencies to enable the organization to make a successful transition to the cloud.

Success Factors for the Cloud

- Provides an increase in speed to market and new services
- Lowers the asset investment threshold
- Lowers switching costs via self-service
- Lowers the innovation access barrier
- Increases growth potential
- Increases speed and transformation rate of change

- Decreases access to services barriers

Organizational Assessment

An organizational assessment is necessary to have a better understanding of the current state of an organization.

The following steps are taken for an effective organization assessment:

- Articulate and emphasize the reason for change.
- Find the current state of an organization.
- Recognize the gap between future and current state.
- Anticipate and assess barriers to change.
- Make action plan to remove barriers.

Migration to the Cloud

Application Migration Strategy

- **`Rehost`** • Rehosting an application to the cloud without making changes to its architecture or code.
- **`Refactor`** • Involves application code and configuration changes for connecting the application to new infrastructure services.
- **`Review`** • Modifying or extending the existing code base to support legacy modernization requirements, then use rehost or refactor options for deploying to the cloud.
- **`Rebuild`** • Involves rebuilding the application on a provider's application platform. It discards code for an existing application.
- **`Replace`** • Involves discarding of an existing application or set of applications and uses commercial software delivered as a service.

Migrate an Application to the Cloud

A few ways to migrate an application to the cloud:

- Rehost on infrastructure as a service (IaaS)
- Refactor for platform as a service (PaaS)
- Revise for IaaS or PaaS
- Rebuild on PaaS

- Replace with software as a service (SaaS)

Theoretical 7-step model of migration to the cloud:

1. Conduct cloud migration assessments.
2. Isolate the dependencies.
3. Map the messaging and environment.
4. Re-architect and implement the lost functionalities.
5. Leverage cloud functionalities and features.
6. Test the migration.
7. Iterate and optimize.

Migrating an application to the cloud can be a challenge to organization with:

- IT policy formulation
- Organizational politics and culture
- Recognizing the system dependencies and how the migration to cloud will affect these dependencies and the work processes in place
- Security, compliance, and SLAs management

Cloud Bursting

Cloud bursting is an application deployment model. In cloud bursting, an application runs in a private cloud or data center and bursts into a public cloud when there is a spike in the demand for computing capacity. Cloud bursting is beneficial for high performance, non-critical applications that handle non-sensitive information.

It is possible to deploy an application and then burst it to the cloud to meet peak demands, or to move the application to the public cloud to free up local resources for business-critical applications.

An organization should consider security and regulatory compliance requirements when considering cloud busting.

Impact and Changes of Cloud Computing on IT Service Management

It is necessary to understand the cloud service life cycle to understand the impact and changes of cloud computing on IT service management in a typical organization. Service principles are important to provide measurable value to business objectives and outcomes underlined in ITIL service management. Service strategy is at the core of the cloud service life cycle. It is the fundamental phase used to define service principles.

Service design, transition, and operation are the revolving life cycle stages, while the continuous service improvement stage is used to anchor these revolving life cycle stages.

Phases of the cloud service life cycle:

1. Service design
2. Service strategy
3. Service transition
4. Service operation
5. Continuous service improvement

Service Catalog

A service catalog helps the customers of cloud service providers understand the services available from the provider, their options, the function of value of each option, and the cost and quality of each service. Service catalogs help customers perform a cost-benefit analysis by being transparent.

Implementing a service catalog is essential for cloud computing success.

Your service catalog should include:

- Service identification
- Service bundling
- Service level
- Metadata
- Integration of provisioning services
- Integration of metered services
- Security services

Implementing a service catalog has multiple benefits. Not only does it provide information about services to the consumer, but it also allows the cloud provider to be a business partner rather than just a technology provider. And a partner who can understand both business and technology can go a long way in providing just the right solution for a customer and improve customer satisfaction.

Incident management is used to restore normal operations as quickly as possible. The Incident management process is followed by the service desk function (operator) to resolve incidents as and when they occur. The priority of an incident primarily depends on the impact and urgency of the situation. Usually, the lower the priority value, the more urgent an issue. So, for example, out of a rating of 1-5, 1 is likely to be the highest priority.

Access management gives the right to authorized users to use the service, block the unauthorized users, and ensure that the policies and actions specified in security management and availability management are appropriately executed.

Cloud Services and Access Methods

- **`Identity management`** • Identity management: The user's identity is unique and is handled via identity management systems, such as Lightweight Directory Access Protocol (LDAP), or LDAP over Secure Sockets Layer (SSL)
- **`Access`** • The level and extent of service functionality or data that a user is permitted to use
- **`Rights`** • Also known as privileges. They refer to the actual settings, which are used to provide access to a service or group of services.

Objectives of Continuous Service Improvement Phase

- Review, analyze, and make suggestions on improvement opportunities in each life cycle phase.
- Review and analyze service-level achievements.
- Review and improve the effectiveness of IT delivery.
- Recognize and use best practices to improve IT service quality and increase the efficiency and effectiveness of enabling ITSM processes.
- Make sure that applicable quality management methods support continual improvement activities.

Service Level Agreements (SLA)

A Service Level Agreement (SLA) is a part of a service contract where the level of service is formally defined. In practice, the term SLA is sometimes used to refer to the contracted delivery time (of the service) or performance.

A Service Level Agreement (SLA) is a negotiated agreement between two parties where one is the customer, and the other is the service provider. This can be a legally binding, formal or informal, 'contract'. Contracts between the Service Provider and other third parties are often (incorrectly) called SLAs, as the level of service has been set by the (principal) customer there can be no 'agreement' between third parties (these

agreements are simply a 'contract'). Operating Level Agreements or OLA(s), however, may be used by internal groups to support SLA(s).

Security Perspectives

Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Security Issues Associated with the Cloud

There are several security issues/concerns associated with cloud computing, but these issues fall into two broad categories:

- Security issues faced by cloud providers (organizations providing Software, Platform, or Infrastructure as Service via the cloud)
- Security issues faced by their customers.

In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the customer must ensure that the provider has taken the proper security measures to protect their information via audits and governance.

Compliance

Numerous regulations pertain to the storage and use of data, including Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act, among others. Many of these regulations require regular reporting and audit trails. Cloud providers must enable their customers to comply appropriately with these regulations.

Business Continuity and Data Recovery

Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data lost will be recovered. These plans are shared with and reviewed by their customers.

Legal and Contractual Issues in the Cloud

Aside from the security and compliance issues enumerated above, cloud providers and their customers will negotiate terms around liability (stipulating how incidents involving data loss or compromise will be resolved, for example), intellectual property, and end-of-service (when data and applications are ultimately returned to the customer.

Public Records

Legal issues may also include records-keeping requirements in the public sector, where many agencies are required by law to retain and make available electronic records when requested. This may be determined by legislation, or the law may require agencies to conform to the rules and practices set by a records-keeping agency. Public agencies using cloud computing and storage must take these concerns into account.

Direct Cost & Cost Allocations

Cost allocation is a technique to conclude the cost of services provided to customers of that service. It does not verify the cost of the service but moderately determines what the service costs to offer. It is important to verify the cost allocation of the services that the FAA is used to provide, to decide a permissible fee/charge/tax for those services and their charges.

Incorporated in cost allocation are:

- Direct cost
- Indirect cost
- Incremental costs

Direct Costs

Direct costs are also known as separable costs. These are the costs that are associated with a single type of service and are connected to one type of output or customer, such as a sector-to-sector hand-off.

Indirect Costs

Direct costs are those that can be assigned to a particular process, product, or service. Lets say a company wanted to implement a document imaging system: The cost of scanners would be considered a direct cost. Indirect costs support multiple processes, products, or services. Continuing with the same example, if the imaging system's storage was on the storage area network (SAN), along with files, email, and databases, the cost of the SAN would be indirect.

Incremental Costs

Incremental costs modify with the level of output productivity produced. Incremental costs measure alters in output, e.g., differences in staffing levels or staffing costs at a competence that is based on traffic count.

The cloud computing economic model is widely expected to bring significant rewards. Several organizations have already reported reaping cost benefits in several ways, by reducing capital investment, rapid time-to-market, virtualization, and others.

However, this is not always the case. For example, many organizations admit that when there is no chargeback,

little attention is paid to the creation of new servers or deletion of unwanted servers. Uncontrolled sprawl and not reclaiming unwanted services can add hefty charges to your cloud bills.

Cost Allocation

Cost allocation is a technique to conclude the cost of services provided to customers of that service. It does not verify the cost of the service, but moderately determines what the service costs to offer. It is important to verify the cost allocation of the services that the FAA is used to provide to decide a permissible fee/charge/ tax for those services and their charges.

Strategic Flexibility

Rights and responsibilities of cloud service consumers according to Gartner Global IT Council:

1. The right to maintain ownership, use, and control of one's own self-data.
2. The right to service-level agreements that address liabilities, remediation, and business outcomes.
3. The right to notice and make a selection about modifications that affect the service consumer's business processes.
4. The right to know the technical limitations or requirements of the service upfront.
5. The right to know the legal requirements of jurisdictions in which the provider operates.
6. The right to know what security processes the provider follows.
7. The responsibility to understand and adhere to software license requirements.

Cloud computing, virtual business services or third-party provisioning of critical services, are included in today's directory of business-enabling tools. They are helpful in enabling small scale businesses to offer services once available only to customers of large organizations.

The three general factors associated with cloud computing "flexibility":

- **Location** • Clients can access a cloud system from any Internet-enabled location, such as a desktop, laptop or mobile device. This can comprise of customers, clients, and other business partners, under suitable security.
- **Hardware** • There is no requirement to buy server side equipment with cloud applications, and it's much simpler to request supplementary cloud capacity than to procure additional on-premise hardware. Cloud systems and applications benefit from economies of scale, normally using virtualization, which translates into lower costs to users.
- **User Numbers** • With cloud systems and its applications, it is comparatively quick, simple and cheap to add additional users when needed. This allows a lower entry level, and flexibility for the future requirements and modifications.