6.1 QoS Terminology:

The IEEE has defined quality as being" the degree to which a system, a component or a process meets specific customers' needs requirements and expectations" 47].

The International Standards Organization (ISO) defines quality as "the amount of features and characteristics of a process or service that bears the ability to meet the specific needs or implied". IEEE in association with ISO defined quality as the ability of products or services to fulfill their function [48].

Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance [49].

Quality of Service (QoS):"Totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service [50]."

Cloud quality (QoS) ensures the operational uptime delivered (service reliability) is that which is promised, through effective utilization of redundant resources. Service availability and scalability is achieved through data replication, distribution and load balancing to give consumers the appearance of a seamless and transparent experience. These properties offer considerable technical performance improvements, through more efficient resource utilization and significant cost efficiencies by lowering cost impact of over or under provisioning, lowering entry cost structure and reducing the time taken to realize value [51].

6.2 Quality of Service: Principles

- **Knowledge about consumers or clients and their needs:** Providers must take effort to continuously learn who the clients are and what they expect [52].
- **Delivering products quality and services**: define quality products and services, and put them in standards and service level agreements to provide clear expectations and consistency in delivery [53].
- **Correct deviations from customer expectations**: Having a philosophy, values and standards does nothing if there is no accountability for their adherence. All

employees have to become responsible for: knowing the expectations for service delivery and getting the training and decision making to meet the performance expectations [53].

- **Strengthen customer loyalty and service**: quickly respond to resolve customer complaints, successfully resolving a customer issue is the fastest way to build customer loyalty. Once all the employees know and understand this truth, they will come to learn that problems with customers result in a great opportunity to build brand and company loyalty, resulting in more customers and more sales [53].
- **Maximize satisfaction and retention**: Gaining feedback at various moments of the customer experience and make sure the "customer" is front and center in strategic objectives – organizational or departmental. **[53]**

6.3 Quality of Service: Standards and Measurements

Regulators face the challenge of ensuring that service quality for core services does not deteriorate, so without appropriate quality regulation, price regulation may give CSPs unintended and distorted incentives for infrastructure investments and service delivery [31].

6.3.1 Quality-of-Service Measures

The development of meaningful measures is the foundation for all QoS frameworks. However, there are certain preconditions for establishing measures. Regulators should determine their objectives, including the quality level required, in the context of competing objectives. Because collecting and processing information is a complicated undertaking that requires extensive planning, regulators must also consider the coordination needed to develop the parameters and incentives as well as the best means of obtaining information [31].

6.3.2 Minimum service standards

- **Quality of service applies to** technical, commercial and commodity standards. Utility regulators generally have more direct oversight with respect to technical and commercial standards. Technical standards apply to reliability issues, such as the number and duration of service interruptions. Commercial standards apply to the direct transactions between the CSP and the end user. Such standards are expressed in terms of measures and represent the minimum performance level that regulators expect from CSPs. These

standards may be authorized through regulatory agency orders, licensing provisions, or legislation. Minimum standards should be set at appropriate levels before monitoring and enforcement occurs [31].

- Subjective-through customer satisfaction surveys and subjective good- fits the QoS definition but time consuming [54].
- **Service levels**

  Service levels are an important way of ensuring that a provider meets the level of service expected by the agency. This is particularly important where the cloud computing service is critical either to the functioning of an agency or to the agency's clients [55].

- **Response times**

  Where an interruption to all or part of the service does occur, it will be important to contractually tie the provider to investigate and, where it is in the domain of the provider, resolve the interruption as soon as possible. An agency may wish to categorize response times based on the severity of the fault [55].

- **Flexibility of service**

  One of the key advantages of a cloud computing services model is that it should offer flexibility of service with the ability to easily scale up or down the required level of service depending on agency needs. It is therefore important for an agency to consider its requirements in this regard [55].

- **Business continuity and disaster recovery**

  Business continuity and disaster recovery will often be a critical consideration in cloud computing service agreements given the reliance that an agency may have on obtaining uninterrupted access to that service [55]. Threats to business continuity in this context can include:

  - Interruption to communications networks
  - Hardware or software failure
  - Power failure
  - Disaster (fire, storm, riot etc) that disables access to the service

Agencies should therefore consider including protections in their agreement with the provider where necessary to ensure access to the service is not disrupted [55].

6.4 Approaches to Regulation for Quality of Service

6.4.1 Encouragement

Raising awareness and encourage the public sector to adopt cloud computing services: should follow and encourage cloud computing services, opportunities and savings offered by the governments in the world effectively. This would raise awareness of the possibilities to provide economic opportunities and provide great value for the citizens, consumers and businesses. [56]

6.4.2 Enforcement

One of the main attributes of effective regulation is the power to enforce compliance with sector policy, laws and regulatory decisions, including dispute resolution decisions. Today, very few regulators do not have enforcement power [10]. The differences in market and regulatory maturity, as well as legal and judicial practices, affect the enforcement practices and procedures of individual countries. However, it is generally agreed that an effective enforcement system is essential in any economy in order to give effect to those rules necessary for maintaining order in the sector, maintaining and facilitating stability, growth and development of the sector, deterring wrongdoing, protecting consumers, and maximizing social and corporate welfare. In summary, an effective enforcement system should be:

(a) *fast* – enforcement decisions must be made quickly, decisively, and clearly to reduce uncertainty in the market and deter future violations;

(b) *Firm* - penalties must be severe enough to deter violations;

(c) *fair* – the enforcement system should be perceived as fair and transparent, and decisions for enforcement action must be based on objective facts and evidence and made publicly available; and

(d) *Flexible* – the regulator should have other means aside from formal litigation or regulatory adjudication, such as alternative dispute resolution, to resolve complaints and disputes, as well as a wide variety of enforcement tools to ensure that the severity of the punishment matches the severity of the violation [10].

Additionally, in order for the regulator to enforce its rules effectively, an enforcement regime should include the following minimum attributes:

(a) Adequate resources for carrying out enforcement activities;

(b) An efficient mechanism for dealing with complaints of non-compliance with rules and regulations;

(c) A regulator with the authority to conduct investigations and enforce laws, rules, regulations, and decisions;

(d) Transparent procedures for investigations, judgment criteria, sanctions and appeals, as well as options for dispute resolution; and

(e) An appeal mechanism to appeal a decision to a higher level, whether within the regulatory body or to the court system. [32]

6.4.3 Integration with regulation & licensing

A key aspect of regulation is the determination of the market structure, and in particular, the number of service providers (SPs) licensed to provide cloud services. A prime reason for licensing new CSPs is to increase competition. Licensing can significantly increase confidence in the regulatory system. Regulatory certainty is a critical element of the licensing processes where the aim is to attract new CSPs [57].

The integration states that quality of service must be configurable, predictable and maintainable over all architectural layers to meet end-to-end quality of service. Flows traverse resource QoS modules, each QoS module traversed must provide QoS configurability (based on a QoS specification), resource guarantees (provided by QoS control mechanisms) and maintenance (based on monitoring mechanisms) of on-going flows [58].

6.5 Quality of Service - Regulatory Roles and Responsibilities

Often, a regulator's responsibility is to establish quality of service (QoS) guidelines or parameters, as well as the methods and procedures for monitoring operators' performance against these established parameters. The fundamental objective in establishing QoS targets and reporting is to ensure that the general public (*i.e.*, the consumer) is served and, at the same time, that the operator is not impeded from carrying out day-to-day operating routines as a result of excessive reporting requirements. The level of regulatory intervention with respect to QoS is often

dependent on the degree of competitiveness that is present in the market. Generally, the regulator takes a more hands-off the approach with respect to QoS monitoring and reporting requirements if a market is highly competitive. Nonetheless, the reporting and the report analysis process should not be too onerous for either the operator or the regulator irrespective of market conditions. In addition, it also should be developed in consultation between the operators and the regulator to establish realistic benchmarks and make the process manageable and useful in identifying areas where the consumer is receiving inadequate service levels [41].

Although different approaches have been adopted in various jurisdictions, the regulatory goal should be to ensure:

(i) the delivery of acceptable service for the cloud user; and

(ii) Those consumers are aware of the variations in performance from various service providers/operators thereby allowing them to make an educated choice regarding their preferred service provider. QoS indicators are one of the most effective regulatory tools in this regard. [41]

Ultimately, consumer should reap the benefits from the enforcement of QoS regulations. In certain instances, for example, operators opt to run the risk of incurring a penalty as opposed to investing to improve the QoS. In such cases, the imposition of monetary fines does not result in any direct benefit to consumers. On the other hand, consumers may benefit directly when the penalty for violating QoS standards is, for example, to provide consumers with services free of charge; to give the consumer retroactive rebates as compensation for the poor QoS; or to move them up to the top of a waiting list for the provision of services [41].

Regulators are recommended to ensure that cloud service providers provide customers with greater transparency about their traffic management practices, and ensure the publication of comparable information on the availability. Service providers should specify transparent and clear terms and conditions in contracts signed with customers [41].

6.5.1 QoS Audit:

- Request third-party audits and/or certifications related to infrastructure and security, including penetration testing and vulnerability assessments. In addition, any reports produced from these audits and certifications will be provided to the government for review.

- Perform an onsite inspection of the cloud vendor's infrastructure and security practices on a specified basis.
- Review the infrastructure and security specifications in written format if it so chooses.
- Audit the performance records of the cloud provider, as well as access to daily and weekly service quality statistics. [59]

6.5.2 Cloud service provider features

- software as a service – applications are delivered over the internet;
- significant cost savings because resources in massive warehouse-sized data centers are pooled at scale, built from low-cost commodity chips and disks, and share the overhead of cooling, refrigeration, physical security, and backup power;
- Presented as a utility with a matching business model, namely pay-per-use;
- A new data-parallel programming framework. [60]

6.6 Price Regulation:

The main aim of price regulation is to ensure that consumers are protected from excessive prices from services rendered to them; Price regulation brings about equality among service providers and avoidance of anti-competition practices" [32].

6.7 Service Level Agreements (SLAs)

The use of cloud services includes the deployment of a defined service model and should always be underwritten by comprehensive service level agreements (SLAs). The secure delivery of any cloud service is dependent on the CSP's personnel, processes, and technologies, while the secure usage of cloud services remains the responsibility of the client [61].

Typically, cloud-hosting agreements are concerned with "up-time" and high availability, with little or no mention or assurance of security. However, the client is ultimately responsible for ensuring the service they're using meets their security requirements and compliance obligations [61].

SLAs and other written agreements between the Cloud Service Provider (CSP) and client should clearly identify the delineation of responsibilities between parties, including responsibilities for implementing and managing different security controls.

These SLAs and agreements should be established as a prerequisite to any cloud service implementation [61].

Failure to develop and agree upon appropriate SLAs may result in issues for the client if the cloud service does not meet the needs and demands of their business. SLAs should be established and agreed as part of any contract and service negotiations. Performance, availability, integrity, and confidentiality should be considered and SLAs agreed for each service managed and/or operated by the CSP. Written agreements should also cover activities and assurances to be provided by both parties upon termination of the service provision [61].

Cloud service providers tries to produce maximum number of services by using less resource but still meeting service level agreements and QoS standards [43].

SLA defines, limits and usages and responsibilities of cloud service user and cloud service provider. SLA further gives certainty, which cloud service provider will comply with the rules about data storage; these rules are local government jurisdiction under cloud computing services [62]. SLA also defines security requirements who and what need to control, in case of any disaster, there must be disaster recovery process defined in SLA and cloud service provider and user both agreed on this specific SLA. SLA also gives terms and conditions for cloud service provider in case if cloud service is failed to keep alive. SLAs can resolve and gives control over privacy and data security [43].

Cloud service provider should provide cloud computing service by signing Service Level Agreements (SLAs) with customer. Cloud service user may have SLA with cloud service provider defining in SLA about memory usage and throughout in given time, CPU usage and how much bandwidth user got. Provisioning of recourses must meet SLAs, in case failed to meet SLA and QoS, cloud service provider may have penalties. Same as if cloud service user over use resource by crossing SLA, it would give loss to cloud service provider. So SLA is bond and agreement between cloud service provider and cloud service user. Still there are barriers creating conflicts to define and sign and meet SLA specifically to security and privacy. Due to unpredictable customer demand, power and software and hardware failure, conflicts are raised that might affect cloud service quality and reliability [43].

Data ownership, data transfer, cloud service performance, reliability, security and privacy are main issues need to define clear roadmap to create trusted bond between

cloud computing service provider and cloud service user. SLAs are the component empowering cloud computing to bridge this bond [43].

Cloud computing service users demand high performance service that requires lot of resource form cloud data center resource pool. Cloud service provisioning in cloud based technology is totally depending upon Service Level Agreements (SLAs). SLA is contract between customer and cloud service provider that defines requirements of services specified as quality of service (QoS). SLA contains, functional and non functional both kind of requirements as well as defining pricing and service time line commitments, pricing and penalties. Cloud service provider ensures to meet SLA, by doing continuous monitoring of recourses and agreed terms and conditions in SLA. There are some gaps in monitoring technology, sometime monitoring is don't at higher level and lower level is ignored, resulting as breaking agreements of SLA and QoS [43].

In any case, it is certain that SLA (Service Level Agreement) can be designed to include acceptable terms and conditions and standards to deliver services. For example one of SLA for any cloud computing service, start and end time bounds and a simple description of cloud resource and services requirements. SLA (Service Level Agreement) is one instrument which can be used to reserve resources in advance. The time requirements and dependencies can be modeled in the SLA to guarantee the resource availability [43].

6.7.1 SLA must include:

- Clear definition of services and,
- Customer duties and,
- Uptime, Performance and response time, Error correction time, and Infrastructure and security [59].
- ***Data Breaches:*** The contract should specify the cloud vendor's obligations in the event of data breach or unauthorized access. It is important to include reporting/notification requirements related to the breach within a specified timeline, as well as details about the breach such as its nature, the data compromised, the involved parties, mitigation efforts, and corrective actions to be taken by the vendor. The contract should also specify indemnification in the event of the breach, as the data breach relates to specific legal, regulatory, and operating agreement provisions. In other words, the cloud provider should be responsible for

all damages, fines, etc. including litigation costs related to a breach. Many cloud providers avoid putting this type of language in their contracts, which makes the government liable for costs associated with breaches [59].

- **Data Storage Location**: The legal system cannot keep pace with technology and, currently, most courts are holding that the legal jurisdiction over a contract dispute involving data takes place in the state where the data physically resides. it is important to consider the inclusion of statements about the physical storage location [59]
- **Service Pricing**

  Pricing plays a key role in the marketplace, which has been well studied in economics [62]. The contract should include specific price caps to eliminate ballooning costs after the initial investment. Monitoring the pricing will be incumbent on the government and can be facilitated through regular review of government contracts with the cloud provider, as well as communication among peer governments. Review of pricing for non-governmental entities will be difficult.

- **Remediation/Penalties**

  Remedies for violation of the SLA should include corrections and/or penalties. Both corrections and penalties should be specific (such as "Service credit will be rendered when SLA is not met by XX Vendor. The service credit will be applied as liquidated damages against the following quarter of service costs." It is important to document how the credit will be provided and when it will be provided. Ideally, the financial penalty should be 10-20 percent of the contract, per Gartner, in order to motivate the vendor to avoid violations. These penalties should be related to SLA performance, while fines and costs associated with data breaches should be covered under the Data Assurances section of the contract [59].

- **Disaster Recovery/Business Continuity**

  The contract should specify minimum disaster recovery and business continuity requirements and ensure that the cloud provider meets the minimums through inspection of documentation, etc. Furthermore, the contract should specify

penalties for failures in complying with the minimum requirements, as discovered through onsite inspections, audits, or actual disasters [59].

- **Termination**

  The contract should state that the government can terminate the contract "at any time without having to show cause and without additional fees or penalties." The contract should require the cloud provider to provide advance notice at a set time, e.g., 60 days before service discontinuation. As previously noted, the contract should specify how data will be retrieved/ returned upon termination by either party [59].

6.7.2 Providing QoS

Many ways to provide QoS!

- Scheduling, admission control, traffic control, dynamic resource provisioning
- Regulate (adopt & control) the data injection rate into computing resource [62].

Chapter conclusion

- Regulator should ensure the CSP are in the safe side of providing services and comply with SLA, the pricing models are compatible with services.

- Price Schedule setting by the CSP compatible with the services. The role of regulator is to control and monitor these scheduling, the regulator involved in setting the prices when there are one service provider and also there are excessive, manipulation in prices. Regulator submits CSPs to the market and open competition.