3.1 What is Regulation?

A ***regulation*** is a rule or law designed to control or govern conduct. In statist mechanisms it can also be extended to monitoring and enforcement of rules as established by primary and/or delegated legislation. ***Regulation*** creates, limits, or constrains a right, creates or limits a duty, or allocates a responsibility [9].

3.2 Source and role of regulation

What can be the source of power to achieve any kind of measures decided? First of all, there are questions: who can be the regulator, what are the remedies to be applied, is there any possibility to enforce the rules? [10].

There are *industrial based global communities* to regulate themselves:

- The most powerful organizations are the global business communities, like standardization bodies, or common voluntary industrial platforms. They may build up internal rule of behavior.
- The other regulators can be Global International Organizations, like Word Trade Organization (WTO), International Telecommunication Union (ITU), Organization for Economic Co-operation and Development (OECD) … which are based on a written constitution, and under the membership there is a possibility to achieve written multilateral agreements. These agreements go into the law-force through member states, and the governments will have the power to enforce the rule.
- There are also Communities of States like European Union, which has a strong internal regulation system. US Federal regulation has even more means to regulate the internal market, which is one of the largest.
- There are also regional agreements in a networked industry e.g Africans or Arabs [10].

As we see, regulation is based on *voluntary partnership* as a basis. This partnership is mostly built up by the incumbent industrial players or governmental parties. The common interest is, to extend business, achieve social benefits, and avoid common risks.

Other type is the *government based regulation*, which is part of the country governance. The role and scope of the government based regulation depends on the administrative culture of the country: idea of the role of government in general, habit to fulfill the legal orders, and imposition of penalties. The government may also - as a punishment - exclude the market player from the limited resources like frequency band or other ones.

The *self regulation of the smaller organizations* is part of the cohesion they build up among themselves. The rules should serve the common goals and interests to gain business or social benefits or prevent some risks and losses [10].

3.2.1 NTC Sudan Responsibilities [11]:

- To issue licenses to import and market Premises Equipment.
- To examine and release Customer Premises Equipment.
- To ensure the implementation of applicable specifications into telecom structures (towers, optic cables, etc.).
- To issue equipment type approval.
- To set and measure service quality indicators.
- To handle customer protection issues and relevant dispute resolution and consultation.
- To participate in relevant national committees and international events.
- To respond rapidly to complaints and inquiries.

3.2.2 Why regulate?

- Regulatory intervention: is necessary to ensure the successful transition of a monopolistic telecommunications market to a competitive one [12],
- To safeguard consumer interests,
- To maintain an effective competitive marketplace,
- To foster the long-term development of the ICT sector.

Effective regulation has resulted in many benefits, such as [12]:

- Greater economic
- Technological growth,
- Increased investment in the sector,
- Better quality of service,

- Lower prices.
- Higher penetration rates.

Greater need for regulation as regulator must implement tools to address new competitive market (e.g. rules regarding potential anti-competitive practices, licensing framework, universal service, tariffing) [12].

3.2.3 Goals of Regulation

- Avoid market failure.
- Ensure consumer interests are protected.
- Safeguards to create effective competition.
- Prevent anti-competitive practices.
- End goals:
    - Effective and robust competition.
    - Protect consumers.
    - Widespread access to networks and services [12]

3.3 Approaches to Regulation

3.3.1 Why We Need Regulation in the ICT Sector

There is need for regulatory framework to [13]:

(a) Support ICT development, investment and application;

(b) Promote competition in the industry where appropriate;

(c) Ensure affordability and access to ICT nationally;

(d) Address issues of privacy, e-security, and ICT legislation, cyber crimes, ethical and moral conduct, copyrights, intellectual property rights and piracy;

(e) Support research and development in ICT; and

(f) Develop an institutional framework for policy development and review.

3.3.2 What are the basic principles of regulation and regulatory concepts?

- **Efficiency and economy:** we need to use our resources in the most efficient and economical way.
- **Proportionality:** we must ensure that any burden or restriction that we impose on a person or activity is proportionate to the benefits we expect as a result.

- **Sustainable growth:** we must ensure there is a desire for sustainable growth in the economy in the medium or long term.
- **Consumer responsibility:** consumers should take responsibility for their decisions.
- **Senior management responsibility:** a firm's senior management is responsible for the firm's activities and for ensuring that its business complies with regulatory requirements.
- **Recognizing the differences in the businesses carried on by different regulated persons:** where appropriate, we exercise our functions in a way that recognizes differences in the nature of, and objectives of, businesses carried on by different persons subject to requirements imposed by or under Financial Services and Markets Authority (FSMA).
- **Openness and disclosure:** we should publish relevant market information about regulated persons or require them to publish it (with appropriate safeguards).
- **Transparency:** we should exercise our functions as transparently as possible. It is important that we provide appropriate information on our regulatory decisions, and that we are open and accessible to the regulated community and the general public **[**14**]**.

The level of regulatory intervention will vary from country to country, and will depend on various factors, including the level of market maturity, the legal and regulatory framework and the regulatory issues arising from new technologies and services [3].

Regulatory Science deals with problems that are thought of not belonging to the normal spectrum of scientific work. *Regulatory concept* is borrowed from the use of boundary concepts in science studies [15].

3.3.3 Evaluation of how the types and styles of regulation are applied in Sudan

In Sudan there is no specific regulations for cloud computing are applied yet probably because the domain of cloud computing services still is new. Cloud computing is an ICT area which falls between NTC and the National Information Centre (NIC). Probably that explains why its regulation has not been addressed to-date.

3.3.4 The link between policy and regulation in the ICT sector

Under the governance system, adopts policies that define the expected outcomes of the district's work and provide a framework within which the district operates. Policies are divided into four categories [16]:

- **Board Culture:** These policies define how the board governs itself and the district.
- **Board and Superintendent Relationship:** These policies define the board's relationship with and delegation of authority to the superintendent.
- **Superintendent Expectations:** These policies define the limits of the superintendent's decision-making authority to select resources, teachers, and educational programs that he or she believes best serve student-learning needs. SEs give the superintendent wide latitude to make decisions to meet the board's expectations.
- **Results Policies:** These are the academic goals that the board expects students to achieve [16].

Regulations are the procedures that define how the district will fulfill the goals defined in board policy. They also may clarify policy or state law [16].

Both regulation and policy may include exhibits that usually explain in detail how regulation and policy are fulfilled [16].

3.3.5 The importance of transparency regulatory to economic growth

– **Transparency**

Transparency relates to regulatory decisions being reached in a way that is revealed to the interested parties. We should exercise our functions as transparently as possible. It is important that we provide appropriate information on our regulatory decisions, and that we are open and accessible to the regulated community and the general public [14].

– **The Benefits of Transparent Regulation**

I. ***Efficiency and Effectiveness*** – Open processes enhance consensus and create confidence in the regulator. Increased public participation promotes diverse ideas in decision-making and increases support for rules and policies, making implementation easier. In addition, transparency can lead to greater efficiency by ensuring that duplication of functions is avoided [14].

II. ***Certainty and Reliability*** – Regulatory credibility and legitimacy builds stability, essential for attracting investment. This is particularly important in newly liberalized markets, where potential entrants need to trust that their investments are protected from arbitrary action and that further commercial development will not be thwarted by sudden changes to "the rules of the game." [14]

III. ***Accountability and Independence*** – Openness promotes accountability and legitimacy, reinforcing regulatory independence and reducing political and industry interference. Stakeholders will have confidence that their views will be heard, without bias, by the regulator. Where regulatory actions are exposed to public view, regulators are more likely to engage in careful and reflective decision-making [14].

IV. ***Continuity*** – A stable set of rules governing transparency will transcend political changes and outlast political appointments, ensuring a continuous regulatory record regardless of who is in charge of the regulatory agency or which political party is in office [14].

Effective regulation requires the implementation of a supporting legal and regulatory framework to create an environment that promotes public confidence and ensures stability, transparency, competition, investment, innovation, and growth in the sector.

3.3.6 Recommendation improvements in regulatory environment to enable greater socio-economic development

> *A driving force for improving ICT sustainability* A diverse legislative framework can affect many aspects of the design, manufacture, procurement, operation, use and disposal of ICT products and services. Indeed, the need to comply with relevant legislation and standards is a major driving force for suppliers and consumers to improve ICT sustainability. [14]

To decide whether a system of economic regulation is "good", or in need of reform, it is necessary to identify the criteria for assessing regulatory quality. Regulation quality can be judged in terms of two main criteria – the quality of the outcomes and the processes of regulation [14].

The outcome of a regulatory system can be assessed against the yardsticks of effectiveness and efficiency. Effective regulation achieves the social welfare goals set down by the government for the regulatory authority. Efficient regulation achieves the social welfare goals at minimum economic costs. The economic costs of regulation can take two broad forms [14]:

> (1) The costs of directly administering the regulatory system, which are internalized within government and reflected in the budget appropriations of the regulatory bodies; and
>
> (2) The compliance costs of regulations, which are external to the regulatory agency and fall on consumers and producers in terms of the economic costs of conforming with the regulations and of avoiding and evading them.

3.4 Regulatory means for Cloud Computing

How the regulator should intervene in the service providing process, in order to inform the possible customers before, and defend them after joining to a certain cloud? From regulatory side to help the safety and security of the cloud computing service provider there are some possibilities [10]:

- *Enforce the transparency of the service* this can be made by independent auditing expert mechanism, and the result can be published.
- *Control terms of delivery*: customer need some help to understand the terms of delivery, it should be provided by the service provider, and the control mechanism can monitor it randomly.
- *Build up customer defense institutions*: Customer should get procedures in case of injustice and unfairness and get compensation to it, by a court, by a tribune or by an agency.
- *Prevent the monopolization of the market:* The market should be open to new entrants and new innovation technologies; because the incumbent providers intend to exclude newcomers [10].

Regulating the cloud is not simply a matter of creating a set of rules, handing them down to everyone who uses the cloud, and moving on to the next issue. The reality is, regulating the cloud, or more properly, regulating entities using the cloud. Currently there is no existing regulation, but there should be. In addition, Building consumer trust and confidence in cloud is a key [17].

Trust is a vital enabler of commercial interaction on the internet, and will become even more important as Cloud computing become ubiquitous [18].

Effective regulation has proven to result in greater economic growth, increased investment, lower prices, and better quality of service, higher penetration, and more rapid technological innovation in the sector [2].

Regulation aimed to help the safety and security of the cloud computing services from vulnerabilities of cloud, loss or theft, and lead service providers to minimize risks associated with uptime requirements, disaster recovery and protection of sensitive data [19].

3.5 Regulatory issues:

In the cloud there are a number of issues that need to be regulated. Potential physical location of data centers cloud anywhere, with geography-blind distribution of applications and data.

As a practical commercial, national regulations should be able to influence the actual deployment of cloud services in countries around the globe. Without concrete guarantees on the privacy of data held by cloud providers, the diffusion of cloud

services may be hampered by the perceived risk in entrusting sensitive data to external cloud services [19].

Strongly related to the notion of service level agreements and policy, in that of governance how to manage sets of virtual resources at the infrastructure level, applications may consist of many virtual networks. Managing these virtual missions, or virtual data centers, requires policy and enforcement from both the provider and consumer [19].

In a private cloud, the infrastructure for implementing the cloud is controlled completely by the enterprise. Typically, private clouds are implemented in the enterprise's data center and managed by internal resources. Private clouds maintain all corporate data in resources under the control of the legal and contractual umbrella of the organization. This eliminates the regulatory, legal and security concerns associated with information being processed on third party computing resources.

In the public cloud, however, external organizations provide the infrastructure and managing required to implement the cloud. Public clouds have the disadvantage of hosting data in an offsite organization. In addition, as most public clouds leverage worldwide networks of data centers, it is difficult to document the physical location of data at any particular moment. These issues result in potential regulatory compliance issues which preclude the use of public clouds for certain organizations or business applications [19].

According to Enki, et.al, the identified regulatory issues in the cloud one of the service level agreements(SLA), service and support and performance cloud computing services define an SLA as some guarantee of how much time the server, platform or application will be available. For example, a cloud provider will provide 99.99% uptime, or five minutes downtime a year, with availability not achieved. Since its infrastructure is not built to reach this uptime, it is effectively offering a 10%. Discount a service in exchange for the benefit of claiming that reliability. Another trick is to compute the SLA on an annualized basis. This means that customers are eligible for a service only offer one year has passed. The end-user should pay close attention to the details of the SLA being provided and weigh that against what business impact it will have if the service provider misses the committed SLA and regulatory authorities [19].

One of the greatest attractions of cloud computing is that it enables computing to be available to large community. In addition, the elimination of the responsibility for physical hardware removes the need for data center administration staff. As a result, there is an increasing number of people responsible for production computing who do not have systems administration backgrounds, which creates demand for comprehensive cloud vendor support offerings and there by greatly inconveniencing the customer. Round the like support staff costs a great deal [19].

The cloud is a pervasive federated network in which unregulated personal area network and local area networks will interoperate with traditionally regulated electronic communication services. Regulators need to carefully monitor challenges posed by these networks, taking action as necessary to regulate for technical interoperability, consumer protection, support for competition and the appearance of opportunities for the exploitation of market power [19].

3.6 Regulatory Mechanisms: licensing and monitoring

Regulatory mechanisms need be sought to bring down the cost of entry into the business and reduce the cost to the end consumer.

3.6.1 Law

The legal and regulatory landscape around cloud computing is by no means static. There are new laws being proposed that could change the responsibilities of both cloud computing tenants and providers.

This creates practical challenges in understanding how laws apply to the different parties under various scenarios. Regardless of which computing model that use, cloud or otherwise, the need to consider the legal issues, specifically those around any data that might collect, store and process. There will likely be state, national or international laws will need to consider ensuring that are in legal compliance.

If the tenant or cloud customer operates in the other country, they're subject to numerous regulatory requirements. These include Control Objectives for Information and related Technology and Safety Act. These laws might relate to where the data is stored or transferred, as well as how well this data is protected from a confidentiality aspect.

When using a cloud infrastructure sourced from a cloud services provider, there must impose all legal or regulatory requirements that apply to the services on the supplier

as well. This is cloud customer responsibility, not the provider's. Taking the Health Insurance Portability and Accountability Act **HIPAA** regulations as an example, any subcontractors that employ (for example, a cloud services provider) must have a clause in the contract stipulating that the provider will use reasonable security controls and also comply with any data privacy provisions [20].

Contractual Issues: These are some of the issues that must consider at all stages of the contractual process:

- Initial due diligence
- Contract negotiation
- Implementation
- Termination (end of term or abnormal)
- Supplier transfer

✓ **Questions that should be considered prior to evaluating cloud services providers include:**

- Is this cloud service a true core business of the provider?
- How financially stable is the provider?
- Is the company outsourcing any aspect of the service to a third party, and if so, does the third party have the appropriate arrangements with the provider?
- Does the physical security of its datacenters meet the legal, regulatory and business needs?
- Are its business continuity and disaster recovery plans consistent with the business needs?
- What is its level of technical expertise within its operations team?
- How long has the company been offering the service, and does it have a track record with verifiable customers?
- Does the provider offer any indemnification? [20]

✓ **Illegal interception**

In Sudanese law there criminalizing assault on the integrity of data, systems and information networks in Informatics Crimes Act of 2007.

clause (6) of the Act to criminalize reality objection intentional messages without a permit from the Department of Public Prosecutions or the competent authority or the owner of the piece of information by eavesdropping or pick up or intercept messages through technical means in place of arrival, in origin or within the information

system. The aim of this material is to protect the right for transfer data in all forms of electronic transmission of data [21].

- ✓ **Law assault on the safety of systems and communications**

Clause (9.8) addressed the assault on the safety of information systems through the criminalization of sabotage system, or disability deliberate, the legitimate use of IT systems including communications systems [21].

- **Types of crimes in Offences Act Informatics 2007:**
  - Systems, media and information networks Crimes that located on the offenses and crimes media systems and information networks, the main threats for the security data and computers are crimes against confidentiality and integrity of the content and availability of data and information systems.

3.6.2 Tariff Regulation

Regulators must establish effective and transparent tariff regimes in order to contribute to the orderly evolution to competition in the cloud computing. As markets become more competitive, tariff regulation becomes a less important regulatory function. A fundamental reason for tariff regulation is to prevent the abuse of dominance. There are two market situations in which tariffs are required to address dominance: non-competitive or monopoly markets and competitive markets. For service markets in which a dominant operator does not face effective competition, the regulatory concern is that prices will be set substantially above cost so that the operator earns a monopoly level of profit. In this circumstance, regulators have historically used "rate of return" regulation, which establishes the maximum return on capital invested, or increasingly, regulators have imposed a price cap regime (with or without consideration of the rate of return), which provides some level of incentives for operators to function efficiently and reduce costs [3].

3.6.3 Licensing

In most countries, licensing is one of the primary functions of the regulator, although in certain countries, this responsibility falls under the jurisdiction of the sector ministry or is shared between the regulator and the ministry [22].

Through licensing, governments often implement policies aimed at opening the market, providing services to underserved areas, modernizing telecommunications infrastructure, and supporting ICT policies. Licensing responsibilities generally include: preparation and publication of model licenses; development of license application guidelines and evaluation criteria; establishment of license fees; and license renewals. Recently, regulators have begun to re-examine their licensing practices as a result of increasing technology convergence and are moving towards unified or converged licensing models [22].

As more regulators examine the need to adopt new licensing regimes in light of increasing liberalization and technological developments, it is critical to take into account and review the impact of the proposed new licensing regimes on the existing licensees and, in particular, any exclusivity provisions that were previously granted to incumbent operators. Usually, incumbent operators are concerned with issues such as license parity; therefore, regulators are often faced with the challenge of facilitating the market entry of new service providers while at the same time addressing the acquired rights of existing operators. In addition, when establishing license award processes in cases where a beauty contest (comparative evaluation) process is used to select and award the license to the best applicant, regulators should formulate objective and transparent evaluation criteria. Not only will transparent evaluation criteria be more attractive to potential new entrants, but these will also minimize the potential for unsuccessful applicants to appeal the license award [22].

- **Terms of the licensing:**
  1) **Privileged user access**: sensitive data processed outside the enterprise needs the assurance that they only accessible and propagated to privileged users
  2) **Regulatory compliance**: A customer needs to verify if a cloud provider has external audits and security certifications and if their infrastructure complies with some Regulatory security requirements.
  3) **Data location**: since a customer will not know where the data will be stored, it is important that the cloud provider commit to storing and processing and processing data in specific jurisdictions and to obey local privacy requirements on behalf of the customer.

4) **Data segregation**: one needs to ensure that one customer's data is fully segregated from another customer's data.
5) **Recovery**: it is important that the cloud provider has an efficient replication and recovery mechanism to restore data if a disaster occurs.
6) **Investigations support**: cloud services are especially difficult to investigate, if this is important for a customer, then such support needs to be ensured with a contractual commitment.
7) **Long-term viability**: the data should be viable even if the cloud provider is acquired by another company [23]

3.6.4 Penalties

Penalties are an enforcement tool widely used by government agencies as a means of encouraging compliance with regulatory requirements. Specifically, administrative penalties are financial penalties that can be imposed on those who fail to comply with a provision of a statute or regulation, with an order issued by a Ministry official or with the terms of an authorization issued under a statutory scheme. For minor to moderate violations, administrative penalties are a cost-effective, timelier, and more certain response to non-compliance than court imposed penalties [24].
Imposing sanctions for service providers in the absence of laws commitment, licensing regulatory requirements, and performance standards, service prices that incompatible with the services

3.6.5 Publicity

Preparing a marketing plan for the new cloud service providers (CSPs) that will be the essence of campaign for providing cloud services. Creating a comprehensive campaign that outlines the benefits and offers for customers will help to facilitate understanding of the CSPs products and, eventually simplify and encourage adoption [25].

A marketing plan outlines the CSPs will position and present its cloud offering. Its main components are: creating buyer personas, drafting a benefit statement, outlining CSPs approach and measuring the results. By these elements we can create an effective marketing plan for CSPs [25].

The regulator publicity that provided to the service providers gives them adequate support about the dependability and reliability. In addition, add a new acquisition of customers.

3.6.6 Enhanced regulation mechanisms

- Fair revenue sharing schemes between different actors,
- Enhanced QoS capabilities,
- Networks Neutrality,
- Consumer trust and confidence to create mass market demand [26]

3.7 The legal and regulatory levels

Cloud computing service users tend to ask questions regarding such legal issues as:

- In which country (or region) is the cloud computing service provider located?
- Is the infrastructure (i.e. are the data centers) located in that same country or region?
- Is the cloud computing service provider authorized to use an infrastructure located outside the country or region referred to in the contract?
- Where will the data be physically stored?
- Is the place of jurisdiction for the service contract the same as for protection of the data?
- Are any of the clouds computing services on offer outsourced either locally or elsewhere?
- What will happen to cloud-stored data upon expiry of the contract? [27]

Chapter conclusion

• Role of Cloud regulator & provider

Regulators responsibilities as follows:

- To encourage technological development and promote effective competition in the cloud computing
- A regulator should ensure the provision of services and to ensure these services are affordable and easily accessible.
- A regulators main duty is to attract investment into the cloud computing services sector in accordance with the principles and laws
- A regulator has a duty to ensure that the rights of the consumer are respected; it also has powers to implement policies that protect consumers from illegal market activities such as excessive market prices, low quality service and breach of contractual obligations
- A regulator should be able to settle disputes referred to it, make provision for alternative dispute techniques and ensure that clash of interest are settled amicably [28].

A goal of regulation is to have service quality properly aligned with customers rates, establishing a quality of service framework are a formidable task for regulators who try to integrate quality into incentive systems, regulators should:

- Determine appropriate regulatory priorities
- Coordinate oversight responsibilities for quality of service and quality of commodity programs.
- Define the appropriate quality standards desirable for each service
- Develop quality of service measures
- Identify a process for developing those measures
- Select the number of measures for the framework
- Select the types of measures for the framework
- Understand the biases in and contexts for the measures
- Determine the appropriate incentives for incorporating those measures
- Determine the most effective process for monitoring and reviewing the framework [29]

Provider responsibilities as follows:

- Responsible for making cloud services available to cloud consumers as per agreed upon SLA guarantees.
- The cloud provider is further tasked with any required management and administrative duties to ensure the on-going operation of the overall cloud infrastructure.