Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)

CONTRIBUTION TO THE 2019 GLOBAL SYMPOSIUM FOR REGULATORS (GSR-19)

1. What are the core design principles for collaborative regulation?

In view of the increasing technological developments which affect different parts of the economy, everyone everywhere is now linked by technology. Security boundaries have become blurred. There is need for regulatory collaboration between the ICT sector, sector-specific regulators as well as regulators from other countries. Managing cooperation has become more important than managing competition. It has become more important to consider shared interests in addition to self-interests. There is therefore need for a globally consistent approach to regulation. Alignment of national and international regulation is therefore a must.

The following principles are key for collaborative regulation:

- Co-regulation – avoid conflicting regulations
- Self- regulation – be responsive and flexible
- International coordination - harmonization of regulatory instruments; cross border agreements; Partnerships are necessary for success; working with global community will assist in embracing global standards
- Co-operation between various sectors and policy makers
- Regular multi-stakeholder engagement - engage all players so as to take everyone on board. Both leadership engagement and community engagement are key.
- Consumer education is necessary to bridge the information asymmetry gap
- Trust and transparency – this is necessary in order for everyone involved to have confidence in the system. Users need assurance that their data is protected and the principle of privacy is upheld. Therefore relevant legislation, including cyber security should be put in place.
- Identification and rectification of legislative bottlenecks in converging sectors by the co-regulators
- Operational framework for collaboration (Memorandums of Understanding)

2. What benchmarks for regulatory excellence and market performance can form the basis for digital infrastructure regulation?

Today's networks are basically built on people's devices. As a result, people need to have confidence in the system. The following can assist in forming the basis for digital infrastructure regulation:

- Customer or user satisfaction – The infrastructure should be user friendly. Information about the infrastructure and service must be available to users. Smart networks are necessary for efficient services.
- Cross border mobility is key to enable users to get quality service
- Encouragement of uptake and deployment of infrastructure
- Digital skills- The skills capacity of citizens to effectively utilise digital infrastructure and services as measured by the digital skills index.
- Cybersecurity- The promulgation of relevant cybersecurity legislations and the commitment of the country to cybersecurity at global level as measured by the cybersecurity index. The capacity of users to successfully implement relevant security measures and report security breaches is important.
- Innovation- Commitment to digital innovation and successes thereof as measured using the Global Innovation Index.
- Digital Connectivity- The deployment of digital infrastructure and its quality
- Access and Use of Digital Public Services- The digital public services dimension measures the digitization of public services.

3. What new regulatory tools and approaches are at hand for enabling digital experimentation?

The world is continuing to experiment, innovate and come up with new solutions for the ICT sector. Digital experimentation is disruptive. The experiments give rise to more exposure to breach and illegal access to systems. Security is compromised as a result. The experiments can give rise to data breaches, hacked interfaces, broken authentication, system vulnerabilities, permanent data losses and many other attacks and abuses. Protection is therefore needed. The following tools and approaches enable digital experimentation:

- Embrace innovation
- Adapt to the changing technologies at a fast pace and avoid being risk averse
- Take speedy decisions and actions
- Respond rapidly and systematically to security threats
- Have precise security policies and services
- Train staff in order for them not to be left behind and to avoid surprises
- Ensure that non-technical staff embrace technology while technical staff demystify their area so that there is common understanding. Cross-functional skills within the regulator are necessary.

- Put in place relevant infrastructure like CIRT to enable instant response to security threats
- Put in place flexible frameworks