RURA

Cyber Security and CIIP
- RWANDA -

Cyber Security and CIIP

Towards a primarily knowledge based economy by the year 2020

Aimable Karangwa

ICT Applications Expert

aimable.karangwa@rura.gov.rw

Rwanda Utilities Regulatory Agency

Phone: (250) 0835 2915

Fax: (250) 58 45 63

P.O Box 7289 KIGALI/RWANDA

WWW.rura.gov.rw

RURA

Agenda

- NICI Plan
- Challenges
- Strategies to overcome challenges
- Regulator Obligations

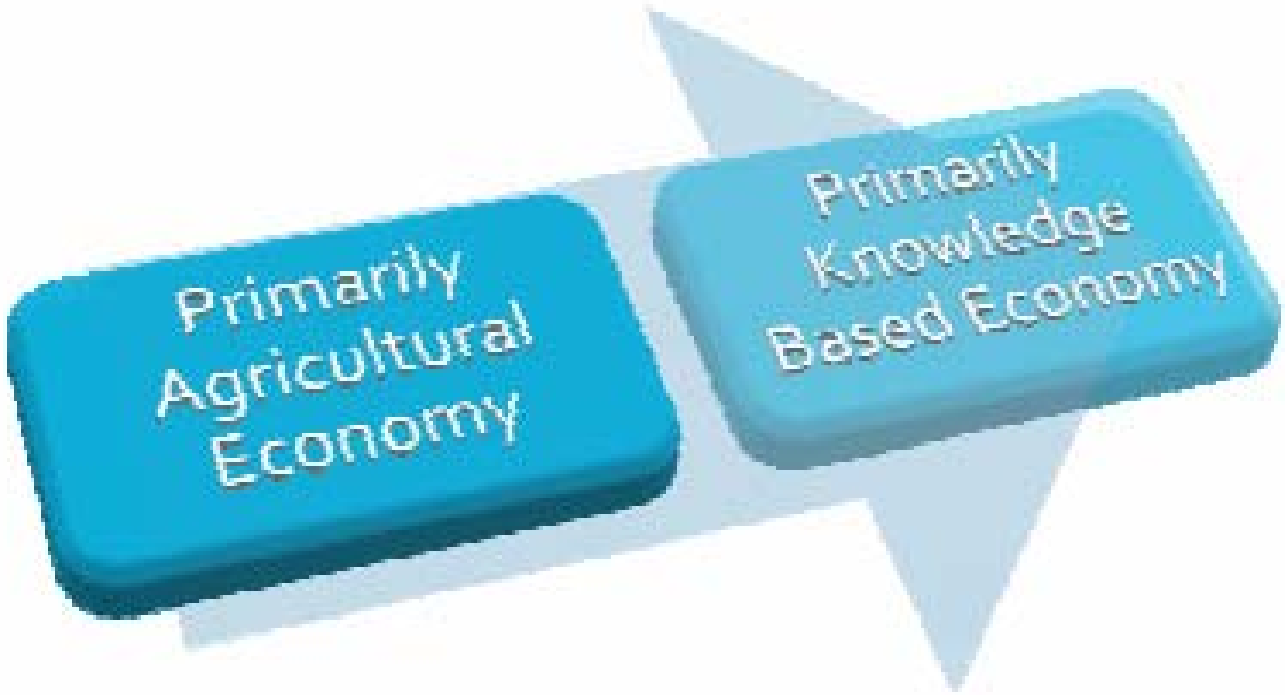
RURA

NICI Plan

- NICI Plan: National Information and Communication Infrastructure Policy and Plan.
- 1999 - 2020, 20 years journey to reduce poverty
- Objective: Move from a primarily agricultural economy to a primarily knowledge based economy by the year 2020.
- 2000: NICI Plan framework created to achieve this ambitious mission.

RURA

NICI Plan objective



RURA

NICI PLAN phases

RURA

Challenges

- 2006: <<Solution Building>> phase introduces new ICT applications and Cyber Security issues.
- Lack ICT applications policy and regulatory framework
- Lack of awareness of Cyber Security Issues.

RURA

Strategies to overcome Challenges

- 2001: Creation of RURA (Rwanda Utilities Regulatory Agency)
- With mission to regulate certain public utilities, namely:

  - Telecommunication
  - ICT,
  - Water
  - Gas
  - Transport
  - Electricity

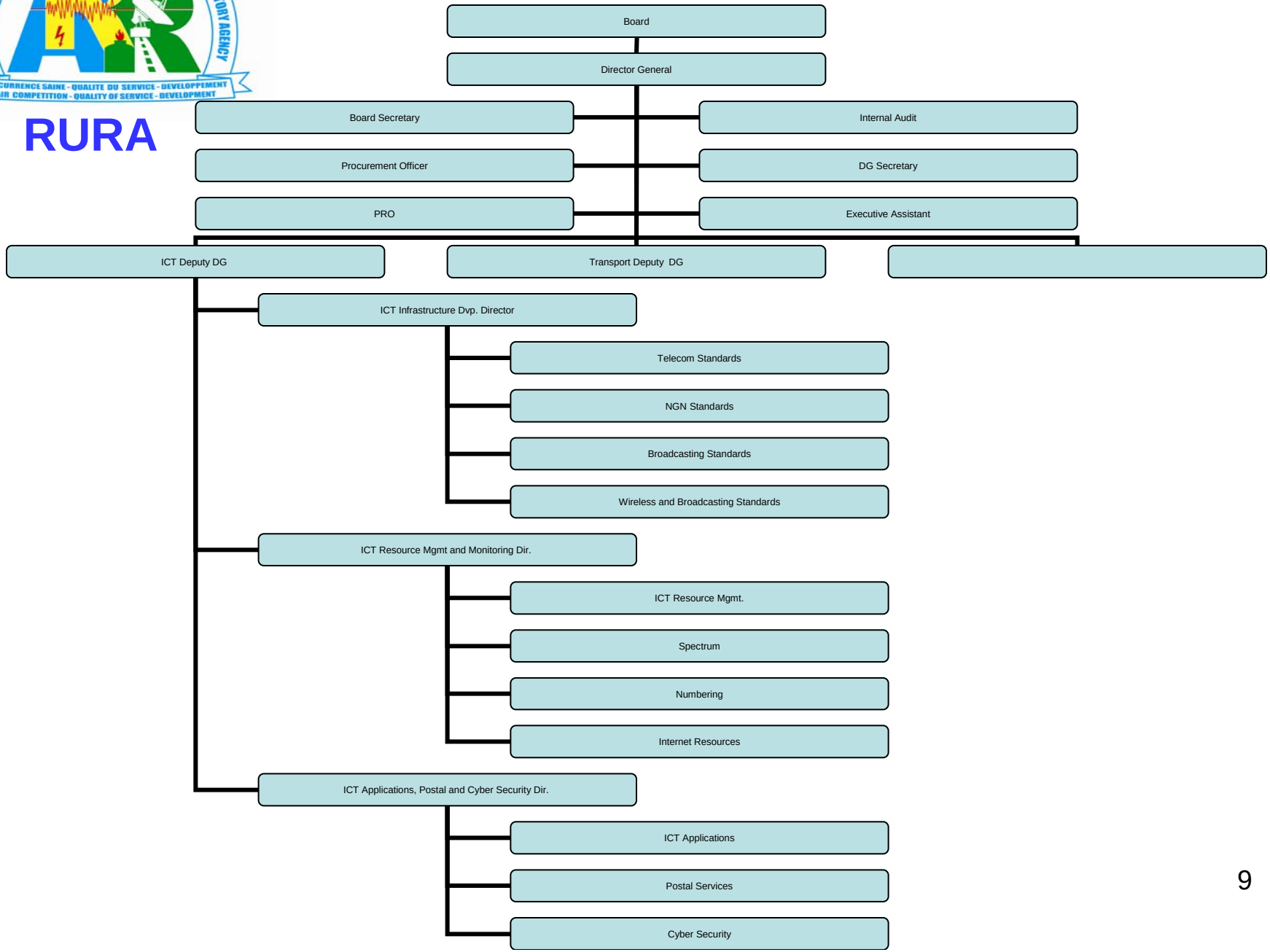
RURA

Strategies to overcome challenges

- Security is a principal Concern
- Adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of our national CII.
- Targeted stakeholders:
  - Policy Makers: Ministry of ICT
  - Licensing and Regulatory Framework: Regulator
  - Judiciary power professionals
  - Business owners & Managers
  - IT providers and professionals
  - End Users

RURA: Organization Structure

RURA



RURA

Cyber Security & CIIP: Obligations

Regulator:

- ❑ Define National Cyber Security strategies and guidelines (ITU standards)

Judiciary Power professionals:

- ❑ Define a legal framework enforceable at a national level but compatible with international level
- ❑ Develop measures to fight against cyber crime and collaborate at international levels

RURA

Cyber Security & CIIP: Obligations, contd.

Business owners & Managers

- ❑ Produce effective security processes
- ❑ Awareness of ICT related risks and security costs
- ❑ Collaborate with the Cyber Security regulator and technical professionals.

RURA

Cyber Security & CIIP: Obligations, contd.

IT providers and professionals

Analyze, design, develop and implement efficient security tools and measures of protection that are:

- Cost effective
- user friendly
- Transparent
- Auditable
- Third party controllable

RURA

Cyber Security & CIIP: Obligations, contd.

End-Users

Awareness among all users

- Adoption of a security behaviour for ICTs

  Help the end user to understand the threats (virus, spam, identity theft, data protection, privacy…):

  - Raise awareness of Cyber Cafe managers and school managers
  - To make them define practical recommendations for the safe use of ICT and communicate them to people they interact with.

RURA

Cyber Security & CIIP: Obligations, contd.

End-Users

- Facilitate definition and deployment of national cyber security strategies and international cooperation:
  - Create local know how based on well recognized standards and answer specific local needs by integrating local cultural values in national standards derived from international standards and recognized best practices.

RURA

Cyber Security & CIIP: Obligations, contd.

End-Users

- Vehicle a common understanding of what Cyber Security means to all.
- Educational events in partnership with local actors (schools, private or public institutions etc…)

RURA

Thanks for your attention