

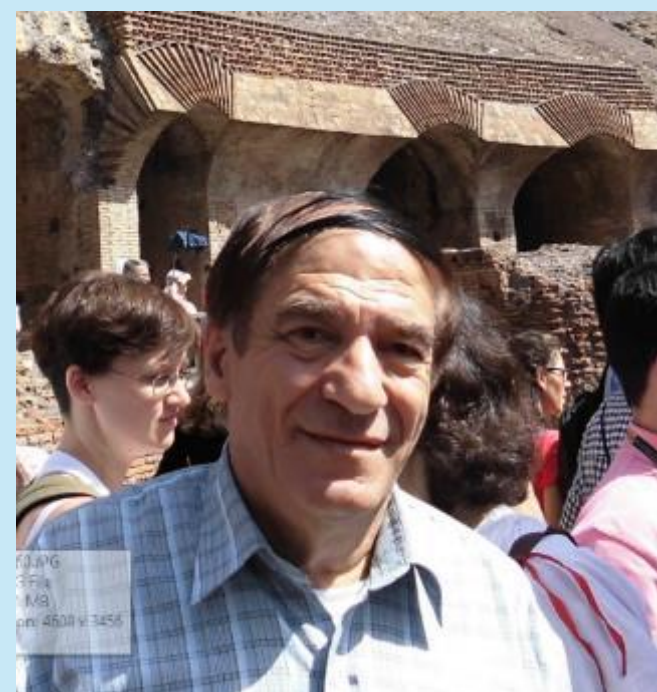


ITU Regional Development Forum for CIS (RDF-CIS) 2024,  
Astana, Kazakhstan, 26-27 March 2024



***RI CIS3:***

***Creating an enabling legal and regulatory  
environment to accelerate digital transformation.***



**Saleem Zoughbi**

**JANUARY 2024**

# Key policy objectives for the regulatory frameworks

---

**Encouraging** the expansion of broadband services.

---

**Lowering barriers** for investment in broadband networks and services.

---

**Encouraging public initiatives** that complement private initiatives when necessary.

---

Upholding a consistent and effective **policy framework** for all **market** actors.

---

**Ensuring independence** of regulators.

# Policy Directives need several changes

**increase competition and predictability** for investments;

**reduce regulation for co-investment** of rival operators in very high-capacity networks;

**improve coordination** and use of spectrum across the CIS region

**strengthen consumer protection**

**create a safer online environment.**

# Essential Directives for Regional Harmonization

(Framework Directive),

- establishes a **harmonized framework for the regulation** of electronic communications services and networks

(Authorization Directive)

- covers **authorization** of all electronic communications networks and services

(Access Directive),

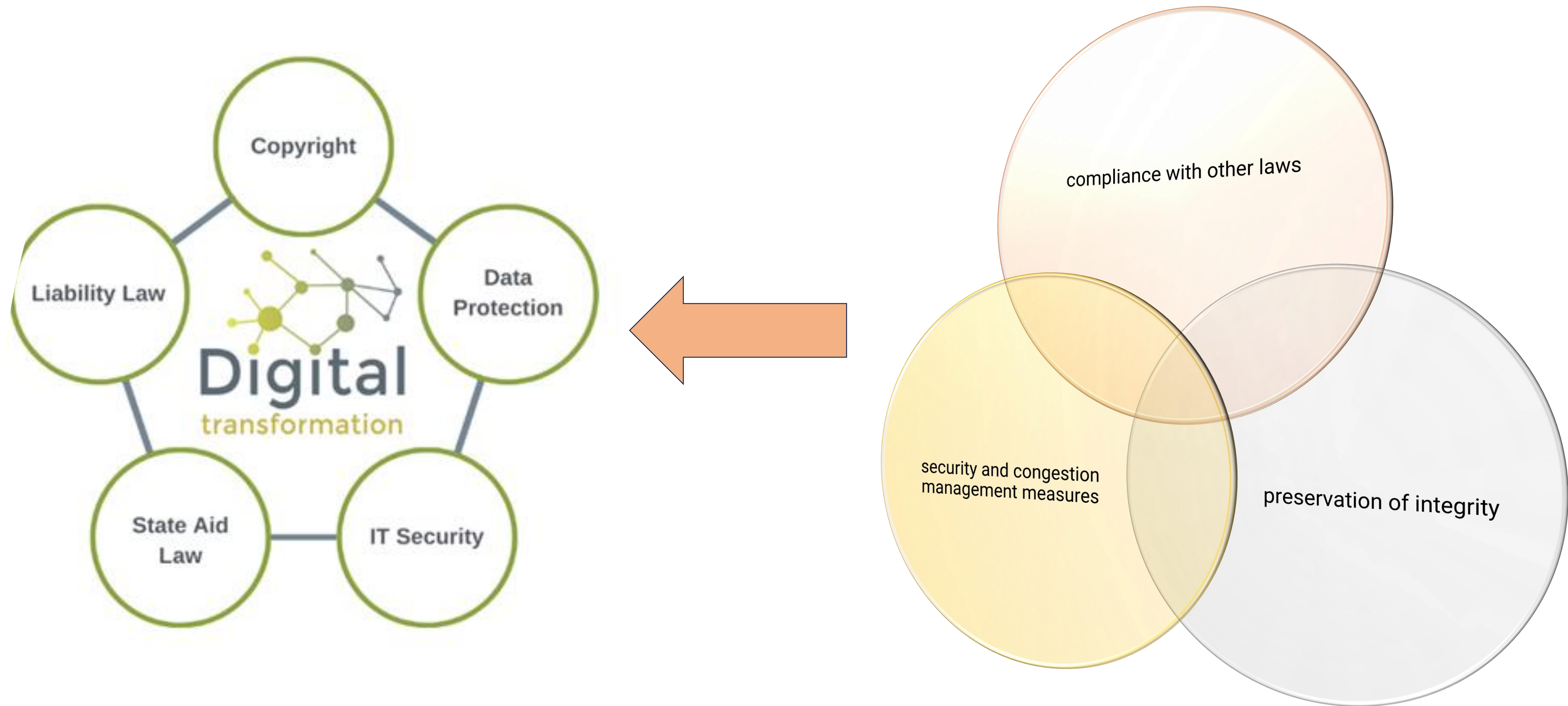
- **Sets objectives of a regulatory framework** to cover electronic communications networks and services

(Universal Directive)

- **Promotes universal service and users' rights** relating to electronic communications networks and services



# Major Concerns of HARMONIZATION



# Essential criteria for Legal Frameworks for CIS Region

1. the harmonization must meet the requirements of the content, applications or services for a specific level of quality;
2. the network capacity must be sufficient to provide these services in addition to any internet access services provided;
3. must not affect the availability of the general quality of the internet access services for end users.

# Takeaways

1. CIS countries cybersecurity exercises;
2. the development of national cybersecurity strategies;
3. Computer Emergency Response Team's (CSIRT) cooperation and capacity-building;
4. studies on data protection issues;
5. secure cloud adoption;
6. technology aimed at improving life and trust services.

