ACER

Agency for the Cooperation of Energy Regulators

Energy and Inter-dependencies: how other non-energy Regulators plan to approach the CS challenge, and how other regulated markets may react to a CS attack on the energy systems
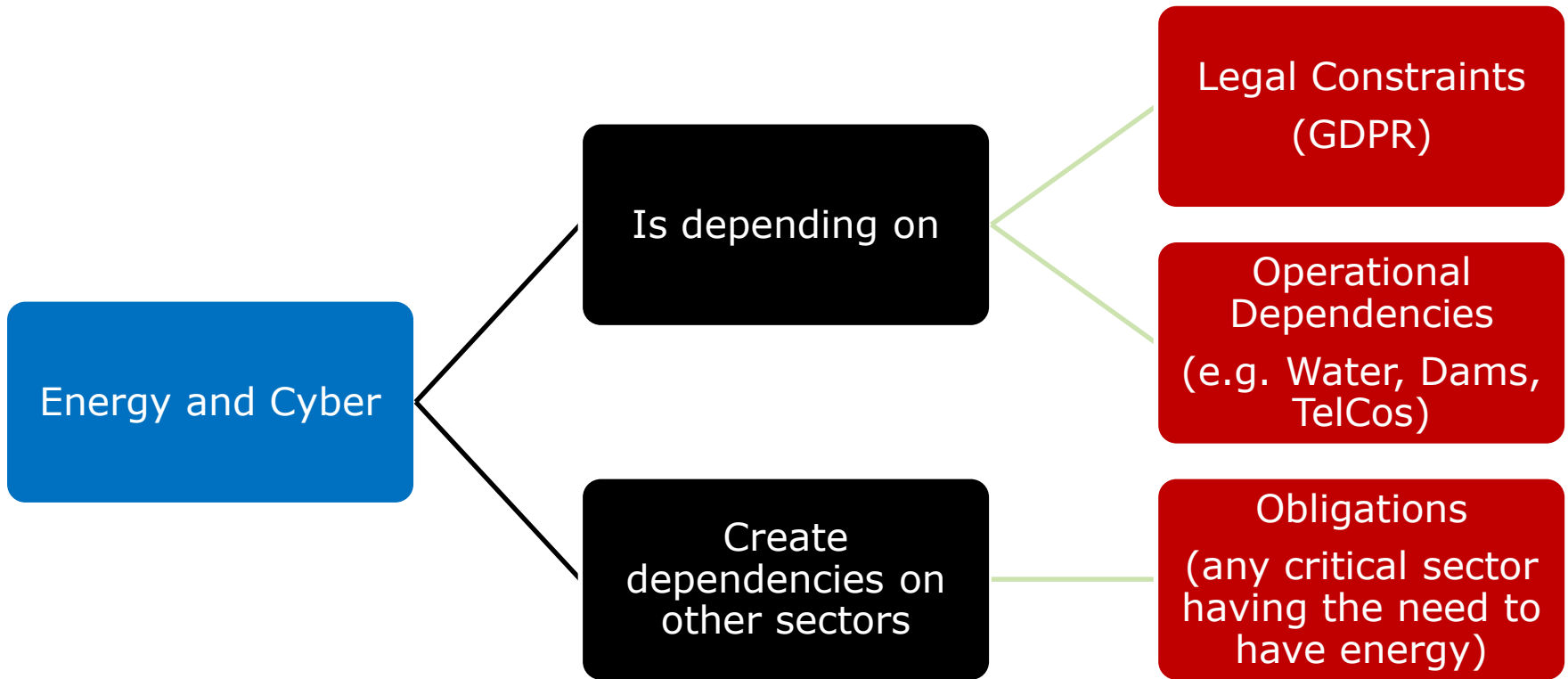
Prepared by: Stefano Bracco (Stefano.BRACCO@acer.europa.eu)
(Knowledge Manager and Security Officer at the Agency for the Cooperation of Energy Regulators)
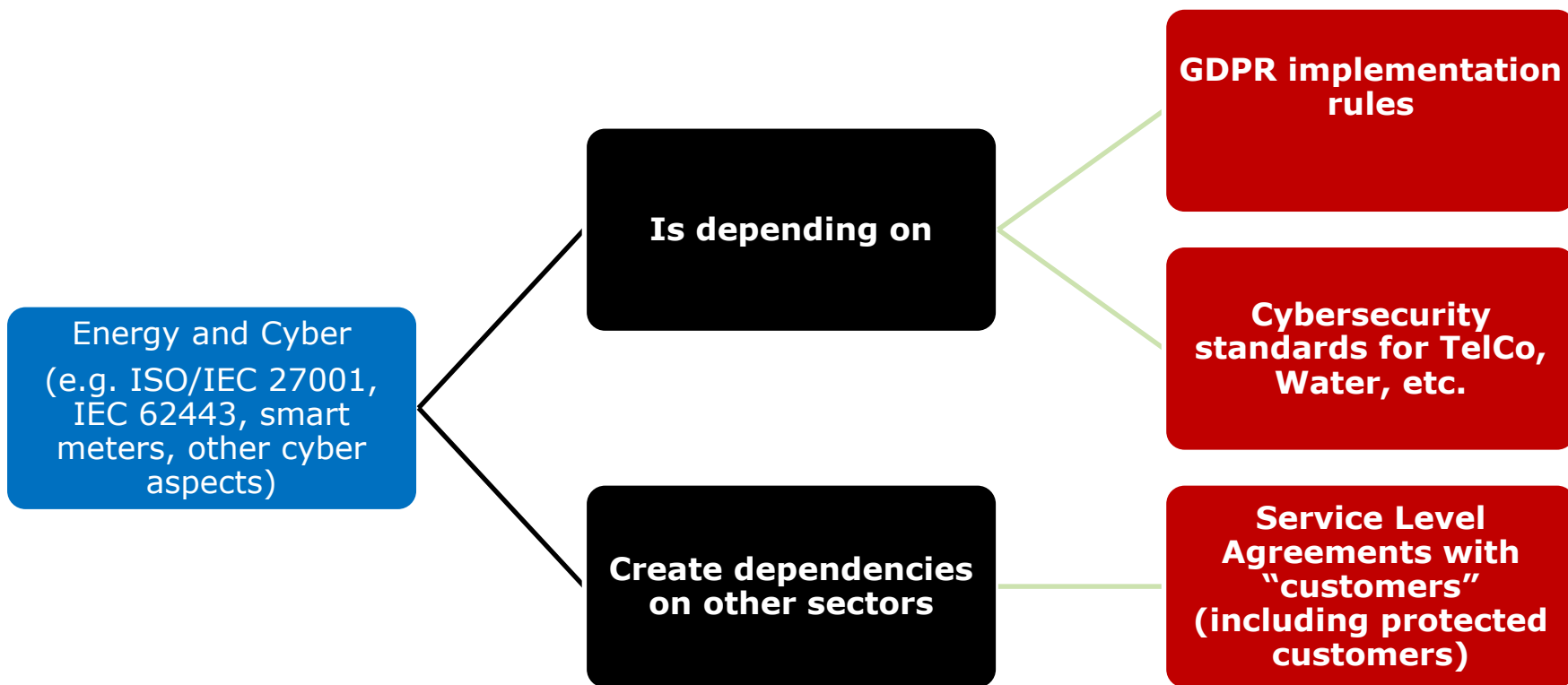
Brussels, 21 June 2019

**CEER Cybersecurity Workshop – Slot 3
Introduction**

Summary

❖ The issue of interdependencies
❖ Regulating in an world of interconnected sectors
❖ Cybersecurity scenarios and risk assessment

Energy and Cyber

- Is depending on
  - Legal Constraints (GDPR)
  - Operational Dependencies (e.g. Water, Dams, TelCos)
- Create dependencies on other sectors
  - Obligations (any critical sector having the need to have energy)

Energy and Cyber
(e.g. ISO/IEC 27001, IEC 62443, smart meters, other cyber aspects)

Is depending on

Create dependencies on other sectors

GDPR implementation rules

Cybersecurity standards for TelCo, Water, etc.

Service Level Agreements with "customers" (including protected customers)

- ❖ Shall regulation be allowed to enter into the boundaries of complex markets creating complexity and, somehow, vulnerabilities?
- ❖ Is <u>ALL</u> regulation embedded in current standards and rules (allowing regulators for a comfortable life)? If not, how to do this?
- ❖ Can a strategy cover consistently different needs of different sectors and different technical standards?
- ❖ Can we set rules (even cross-sector) which may help in alleviating the effect in the phase of response and recovery to an attack on the energy grid?
- ❖ Are markets able to alleviate or to solve cyber issues for different sectors limiting the need of strict cyber rules?

Thank you for your attention!

www.acer.europa.eu