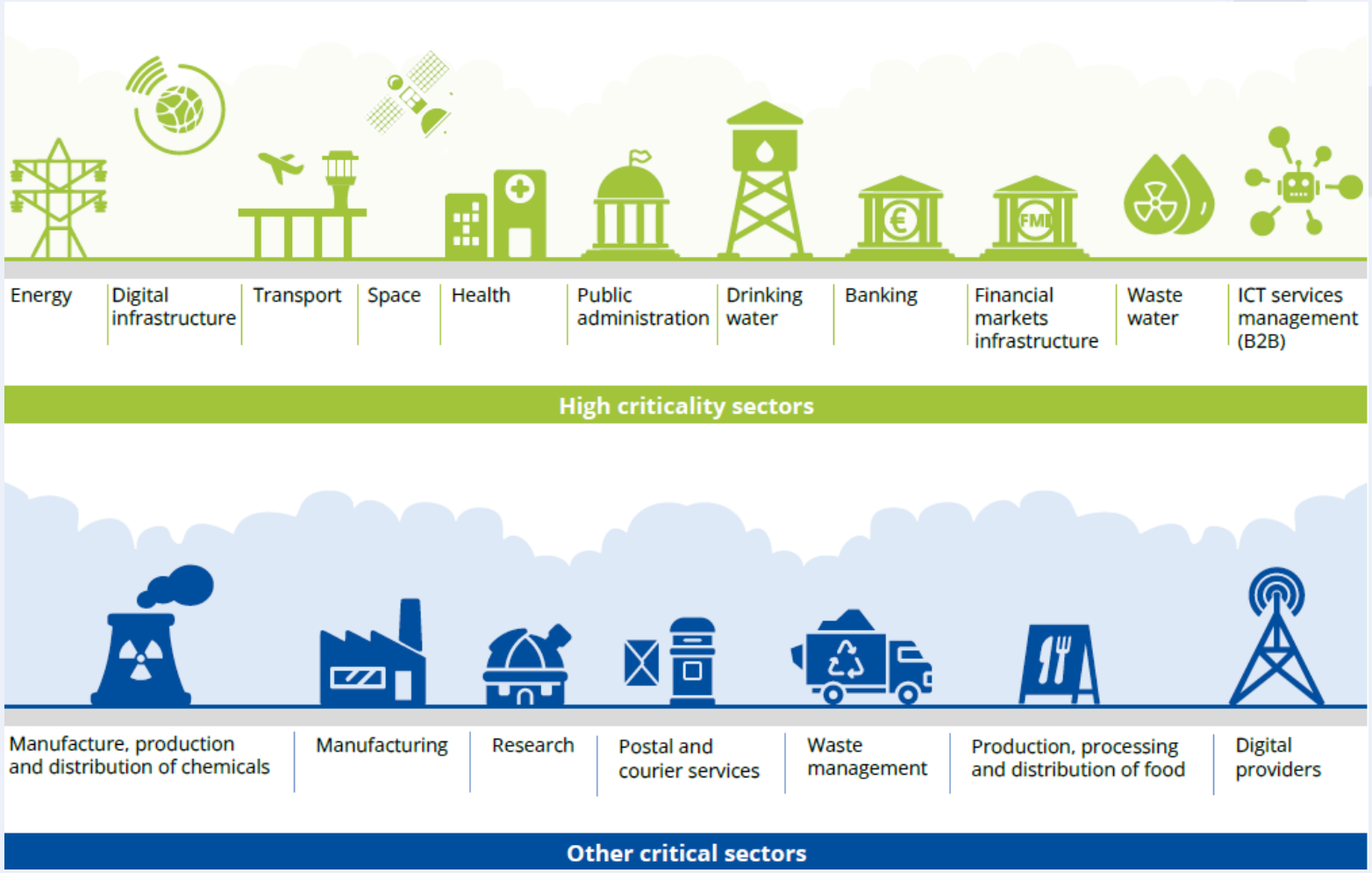
EUROSAI
IT Working Group

Auditing the Resilience of Critical Information Infrastructure in Europe

EUROSAI WGAFADC meeting

May 21, 2025

State of play in Europe regarding CII the scope



EUROSAI IT Working Group

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

State of play in Europe regarding CII key cyber risks

EUROSAI IT Working Group

- **Ransomware**
  - for instance, Lockbit
- **Supply chain attacks**
  - for instance, Solarwinds
- **Russia's war of aggression**
  - for instance, wipers, subsea cables
- **Industrial and state espionage**
  - for instance, NXP, ASML
- **Foreign interference**
  - for instance, EU elections
- **ICT supply chain risks**
  - for instance, 5G
- **Emerging threats (IoT, AI)**
  - for instance, deepfake social engineering

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

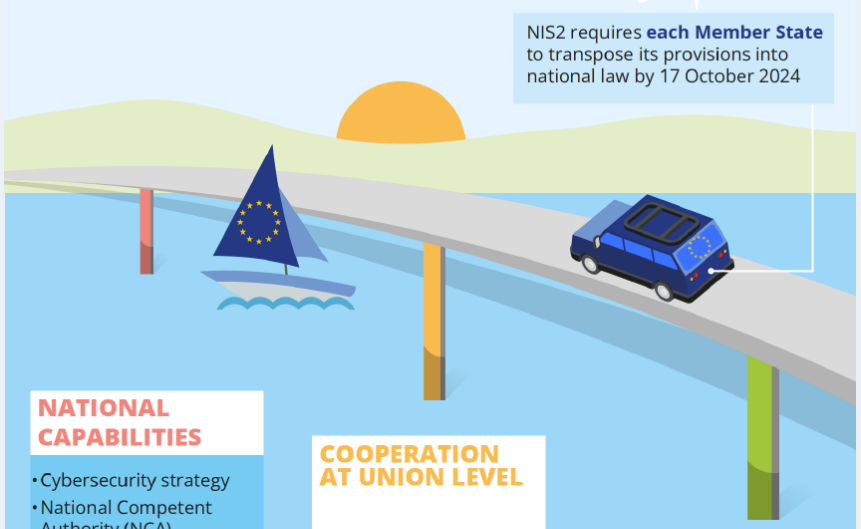
State of play in Europe regarding CII
NIS2 is reshaping the picture

EUROSAI IT Working Group

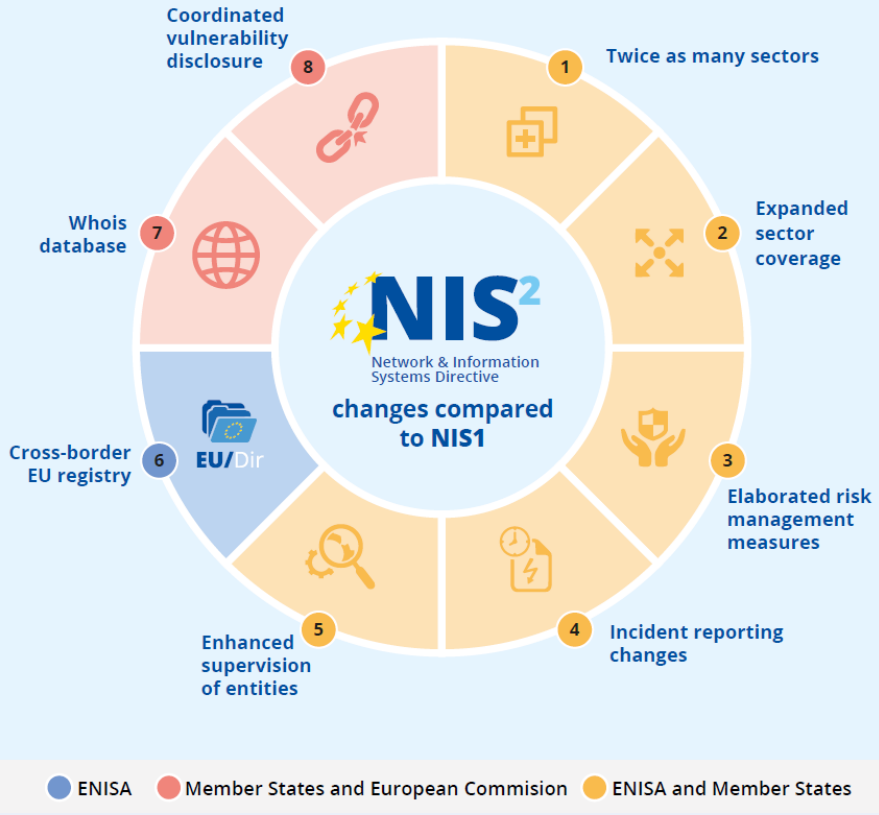
WHAT YOU NEED TO KNOW

The NIS2 directive is a flagship EU-wide legislation on cybersecurity.

Its aim is to ensure a high common level of cybersecurity across the Union on the basis of three pillars:

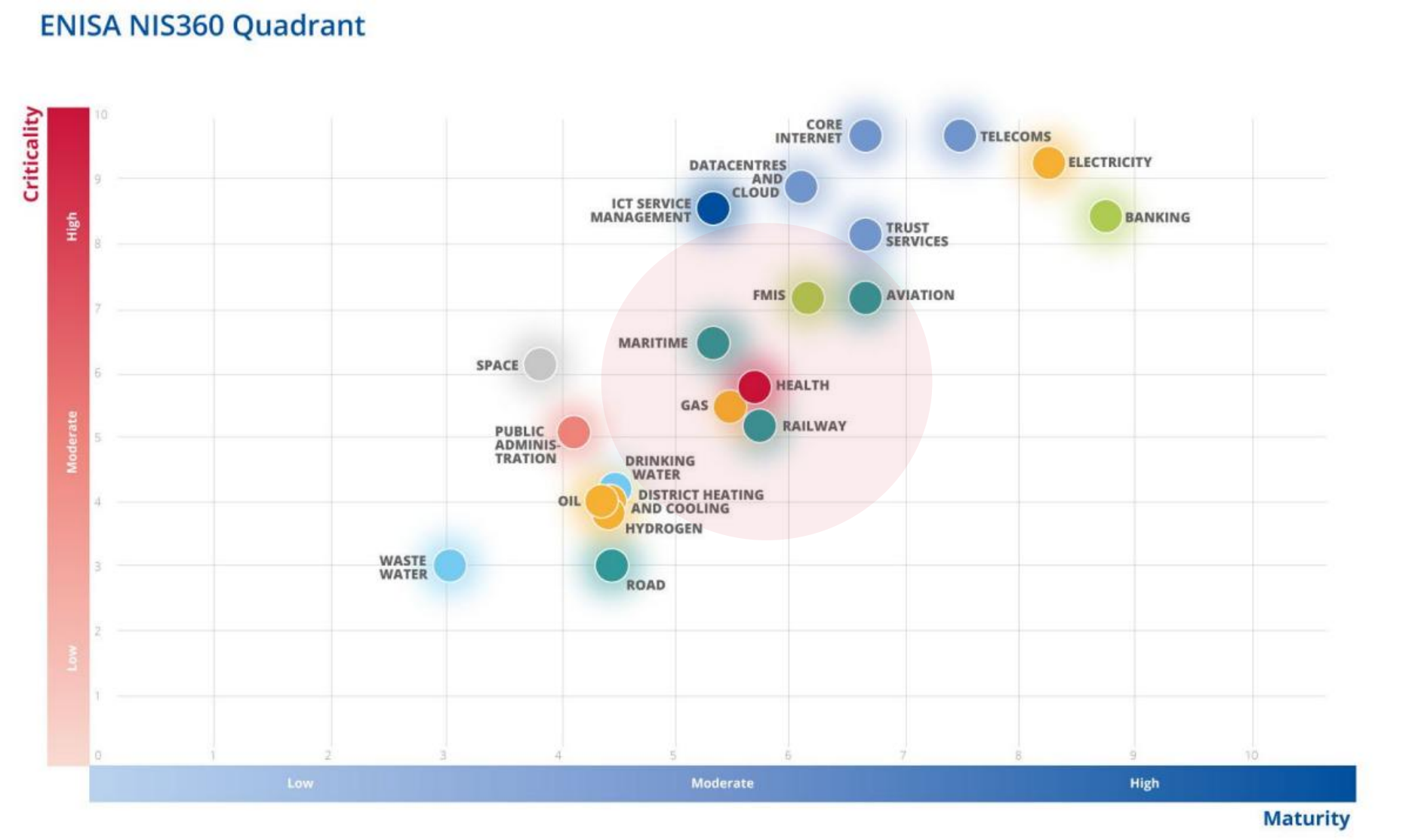


FROM NIS1 TO NIS2: WHAT'S NEW



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

State of play in Europe regarding CII criticality vs maturity



Auditing CII in Europe
some overall remarks

EUROSAI IT Working Group

- Different mandate of SAI-s (for example, in Germany BSI, Federal Office for Information Security, is performing CII audits and also provides assistance to CII operators).
- Focussing on single area – like business continuity management in CII providers in Slovenia – on long-term basis, develops internal SAI capacity and raises awareness in the society (instead of targeting wide range of topics).
- SAI's maturity assessment based on strong framework might be a valuable tool for long-term audit, providing a unified approach and creating basis for follow-up work.
- While it's natural to focus on large CII operators, it's equally important to look at government entities developing and managing CII (for example, interoperability issues and wider coordination in the government).

Auditing CII in Europe
main findings

- Incomplete identification and assessment of IS risks, missing or insufficient mapping of measures to identified risks, no systematic implementation (Slovenia* and Germany).
- Insufficient competence, training and awareness raising, inadequate document control, conflict of interest and low level of reliability checks (Finland, Germany).
- No systematic business impact analysis, limited focus on alert and report chains (Slovenia* and Germany).
- No Business Continuity Management System (Slovenia*).
- No centralized asset inventory, missing linkage between assets and risk management (Germany).

** looking specifically at water utility companies*

Auditing CII in Europe
critical success factors

- Only holistic approach can have lasting impact across all organizational levels (Germany).
- Well-thought-out organizational policies, clear definition of roles and reliable, well-informed employees (Germany, Switzerland).
- Implementing and incorporating updates and life-cycle of system into maintenance contracts (Switzerland).
- Establishing proper access control system (Switzerland).
- Practicing response plans and emergency organizations (Switzerland).
- Binding and cross-sectional guidelines (Switzerland).
- Ensure communication and information flow in the event of an accident (Switzerland).
- Monitoring and controlling resilience measures (Switzerland).
- Maturity level of information security and business continuity is lowest in health and transport&traffic sectors (Germany, ENISA).

Thank you for your attention!

ITWG secretariat itwg@riigikontroll.ee

https://eurosai-it.org