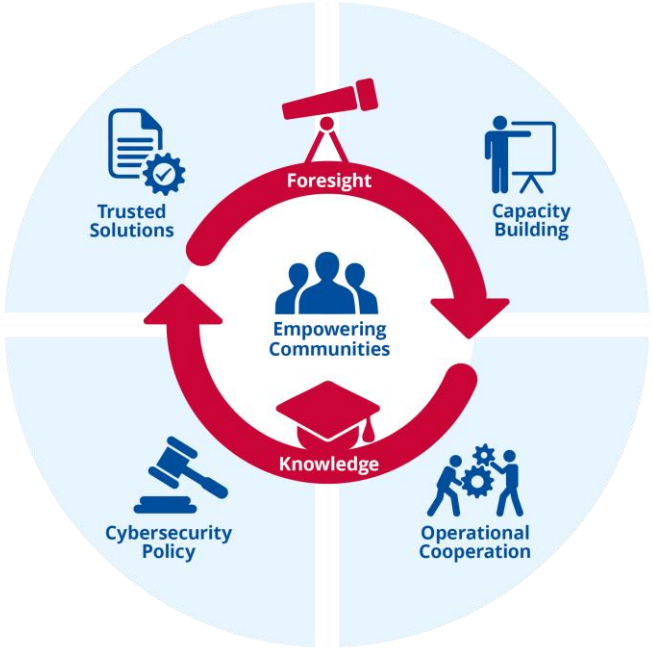
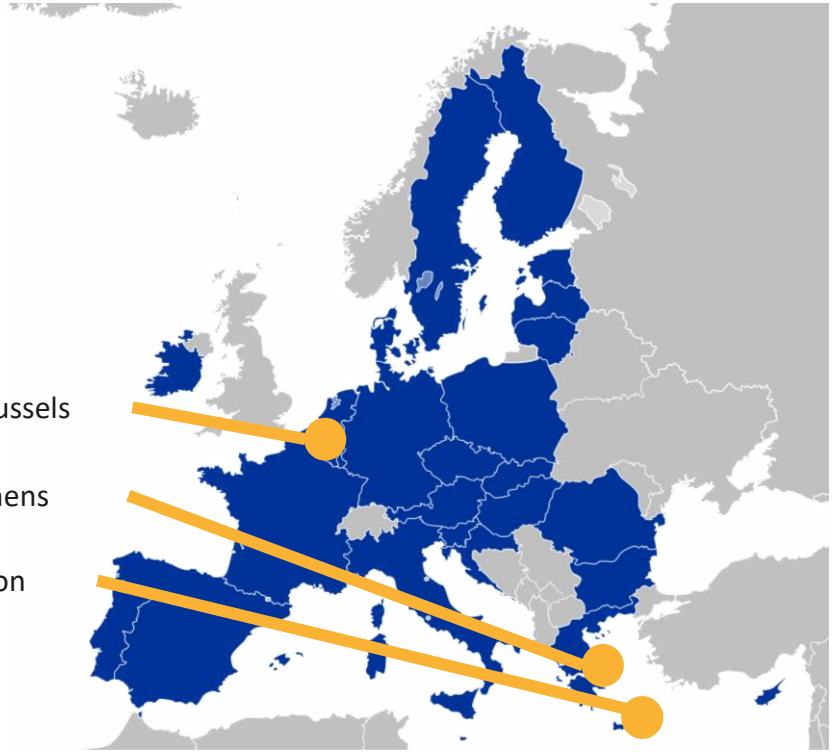
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA POWERING THE NIS2 IMPLEMENTATION

Hans de Vries
Chief Cybersecurity and Operational Officer
ENISA, the EU Agency for Cybersecurity

ABOUT ENISA – THE EU AGENCY FOR CYBERSECURITY





~100 staff - Cybersecurity work done by 4 units:

- **Operational collaboration unit:** CSIRTs network, Cyclone, Situational awareness
- **Capacity building unit:** Cyber exercises, challenges, trainings
- **Policy unit:** NIS2, 5G, eIDAS, resilience of critical sectors
- **Certification and standardization:** EU certification schemes and CRA (EUCC, EUCS)

EU POLICIES FOR CYBER RESILIENCE

Many EU policies coming into force – NIS2, DORA, AI act, Digital Services Act, Digital Markets act, etc.
ENISA's main focus is on:

NIS2 directive (resilience of critical sectors)

EU Certification (CSA)/Digital products (CRA)

Cyber solidarity act (cyber reserve, hubs, stress tests)

ENISA leading
(driving the community)

Financial sector resilience (DORA)

Electricity network code

Critical entities directive (CER)

ENISA advising
(alignment with NIS2)

MAIN CYBER THREATS FOR THE UNION

- DDoS attacks
- Ransomware
- Supply chain attacks
- Russia's war of aggression against Ukraine
- Industrial and state espionage
- Foreign interference
- Supply chain risks
- Emerging threats (IoT, AI), future issues (PQC)

Finland warns of hostile activities by Russia

Nordea has come under "unprecedented" denial-of-service attacks

NoName Cyberattacks Escalate, Targeting Diverse Sectors in Finland

Ireland's Health Services hit with $20 million ransomware demand

A Year After the SolarWinds Hack, Supply Chain Threats Still Loom

The Russia-led campaign was a wake-up call to the industry, but there's no one solution to the threat.

Exclusive: US sees increasing risk of Russian 'sabotage' of key undersea cables by secretive military unit

A year of wipers: How the Kremlin-backed Sandworm has attacked Ukraine during the war

Chinese Hackers Suspected Of Airbus Cyberattacks—A350 Among Targets

Europe's election campaigns are under the constant threat of foreign interference

Eleven EU countries took 5G security measures to ban Huawei, ZTE

Mysterious Cyber Attack Took Down 600,000+ Routers in the U.S.

The threat posed by code-cracking quantum computers

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

NIS2 DIRECTIVE

To achieve a high common level of cybersecurity across the EU

1. National capabilities

- National authority
- National Strategy
- National CSIRT
- National Crisis management framework

2. EU collaboration

- NIS Cooperation group
- EU CSIRT network
- EU Cyclone

3. Supervision of critical sectors

- Management responsibility
- Security measures
- Incident reporting

NIS2 changes

- Twice as many sectors
- More companies within a sector
- **Management responsibility**
- All hazard, including physical
- **Supply chain security**
- Cloud and datacenters essential
- **Managed service providers**
- Telecoms and trust under NIS2

New mechanisms in NIS2:

- National cyber crisis management
- EU Cyber crisis mgmt. (Cyclone)
- National vulnerability disclosure policies
- EU Vulnerability database (EUVD)
- EU Digital infrastructure registry (EUDIR)
- WHOIS requirements
- Union evaluations of supply chain risks
- Cybersecurity state of the union report

NIS2 MAIN FOCUS

NIS Directive is about resilience (CIIP!)

- Focus on
    - Outages, large attacks, major incidents (DDoS attacks, ransomware, etc)
    - Redundancy, failover, backups, scaling, capacity
    - Handle crisis situations, recovery, business continuity
    - Detection and response
- “Keep the ICT in the critical sectors working”

Resilience is a “partnership” between national authorities and the owners/operators of critical infrastructure

- “The stick is out there (ransomware), we will focus on the carrot”
- “With ISO27K1 you should be OK”

NIS2 = DIRECTIVE ++

It is a Directive!!!

- Each country decides on sectors in scope, and entities in scope (the minimum is set by the NIS2)
- National and sectorial security requirements come from your national agency/authority
- NIS2 entities in scope to be registered nationally, in a register

Some examples of EU harmonization built into NIS2

- Strategic cooperation in the NIS Cooperation group
  - Strategic cooperation: 5G toolbox, requested by Commission, developed by (and for) EU Member States
  - Technical guideline: National Coordinated Vulnerability Disclosure (CVD) policies (“working with ethical hackers”)
- Operational and technical collaboration in Cyclone and the EU CSIRT network
- EU Harmonization for the digital infrastructure sector
  - EU implementing rules for NIS2 security measures and NIS2 incident reporting
  - One-stop shop principle, main establishment, mutual assistance between NIS authorities
  - EU Registry for digital infrastructure entities (EUDIR)
- Union coordinated supply chain risk assessments
  - Following the EU 5G toolbox process
  - Nevers process, Cyber risk posture process, and more are coming

SUPERVISION UNDER THE NIS2

NIS2 Supervision

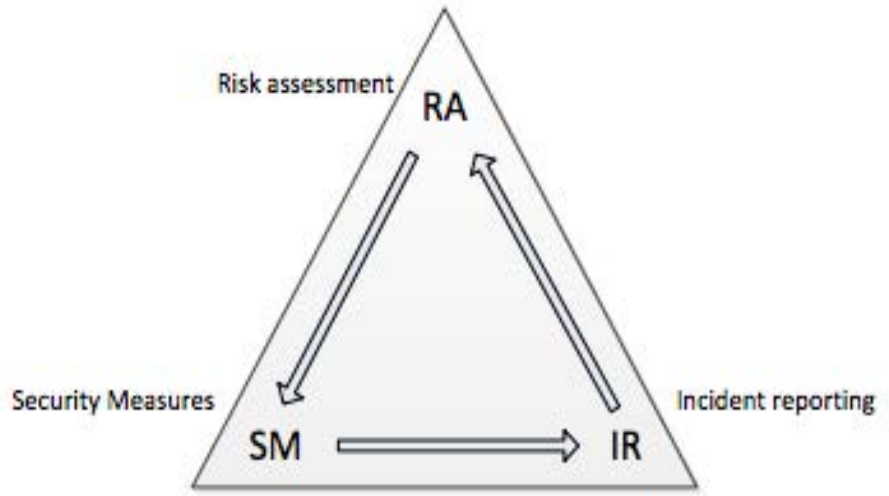
- Security measures, risk-based, all-hazard approach, i.e. anything impacting the ICT
- Incident reporting, when there is significant impact, in 3 steps
- Management to be held responsible for cybersecurity

NIS2 distinguishes essential and important entities

- Essential entities – ex-ante and ex-post supervision
- Important entities – ex-post supervision

Supervision typically includes

- Legal cybersecurity requirements imposed by a NIS authority
- Advice, guidance and support for entities in scope, issued by the authority
- Ex-ante supervision and ex-post supervision (after an incident), carried out by the authority



Triangle to be implemented by the operators/providers under NIS

(and supervised by the NIS authorities)

ENISA NIS2 STRATEGY

To address the NIS2 challenges

- New NIS2 tasks and changes of existing NIS1 tasks
- More sectors, more companies within each sector
- New threats, geopolitics (Russia, e.g.), supply chain (5G e.g.)
- Align with sectorial policy initiatives (DORA, network code, …)

ENISA made a 3 year NIS strategy (2023-2025) focused on:

- Supporting MS with horizontal tasks
- Providing sectorial stakeholders with sector-specific good practices
- Streamlining ENISA support for NIS sectors (across the ENISA units)
- Including a **NIS360** to prioritize NIS sectors

Some details about our NIS2 work

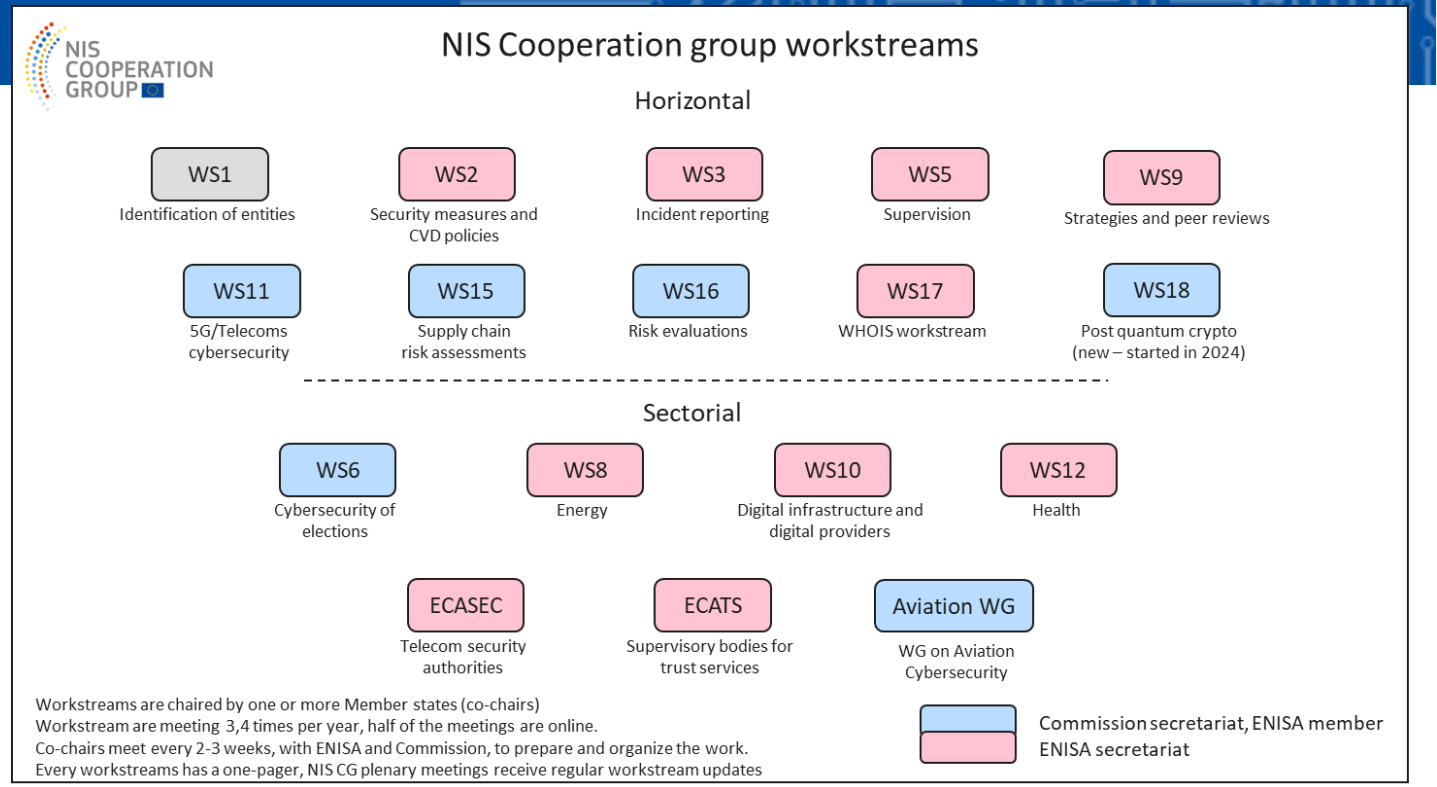
1. SUPPORTING NIS CG AND IMPLEMENTING NIS2 TASKS

Driving EU cybersecurity collaboration

- **NIS Cooperation group** has grown to **16 active groups**
  - **~700 experts** in the community now (~50 in 2017)
- **EU Cyclone** is up and running
- **EU CSIRT network** working since 2016

Supporting MS with NIS2 implementation

- **NIS2 Security measures framework**
- **NIS2 Incident reporting thresholds and template**
- **National CVD policy guideline**
- NISCG guideline on **NIS2 WHOIS provisions**



New ENISA NIS2 tasks

- **EUDIR** - NIS2 EU registry for digital infra
- **EUVDB** – ENISA is CVE Numbering Authority, EU CSIRT network now has CVD procedures
- **EU Cybersecurity state of the union report** – Based on EU wide Cybersecurity index

2. SUPPORTING UNION RISK EVALUATIONS/TOOLBOXES

Supporting the 5G toolbox process

- 5G toolbox strategic and technical measures
- 5G progress reports
- ENISA 5G Matrix, Open RAN security analysis

5G Security Controls Matrix powered by ENISA

https://www.enisa.europa.eu/publications/5g-security-controls-matrix

Supporting the Nevers process

- Nevers risk assessment and recommendation published (2/2024)
    - New threats (UA/RU, submarine cables, satcom), based on 5G toolbox model ENISA-CNECT-MS
- Nevers action plan to follow up on recommendation, Subsea cable recommendation to MS

Nevers union risk assessment: Report on the cybersecurity and resiliency of the EU communications infrastructures and networks | Shaping Europe's digital future (europa.eu)

Union coordinated supply chain risk assessments

- New mechanism in the NIS2, but already used (see above)
- ICT Supply chain toolbox being developed - for use in new areas/sectors
- Union risk assessment methodology being drafted – new sectors/areas in focus

3. SUPPORTING THE NIS SECTORS

ENISA NIS packages for NIS sectors

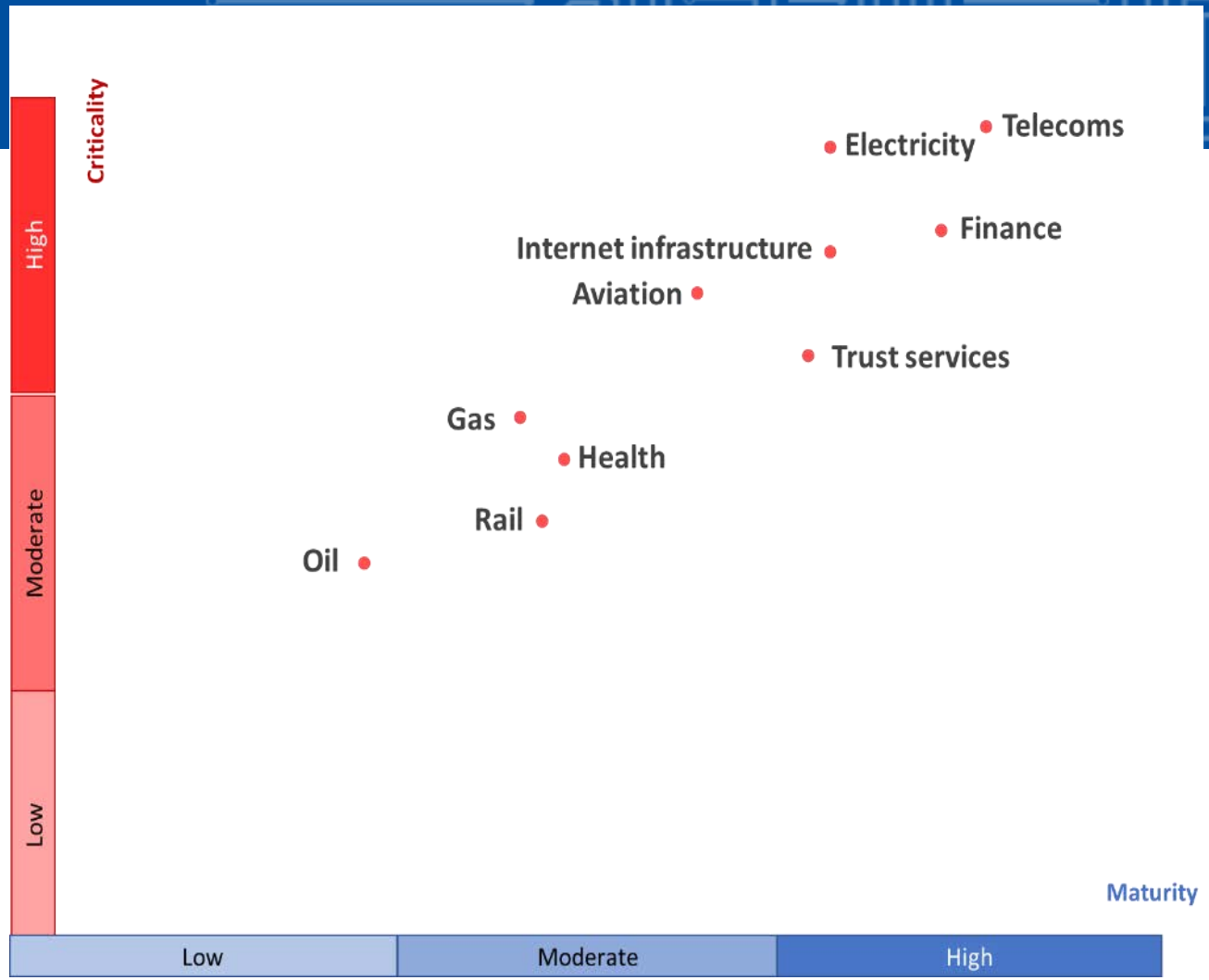
- For now we **focus on 6 main sectors**, and are engaged with 3 other sectors
- We are **streamlining sectorial work** across the ENISA units
    - Cyber Europe, Awareness raising campaigns
- We work with **sectorial groups of national authorities in the EU**
    - Telecom security (ECASEC), Energy cybersecurity (WS8), Health cybersecurity (WS12)
- The sectorial groups **support also the horizontal NIS2 work**
    - NIS2 taskforces in sectorial groups
    - Bringing technical/sectorial expertise in NIS2 horizontal tasks
- We facilitate public-private **dialogue between NIS authorities and industry**
    - Examples: ENISA Telecom security forum, ENISA eHealth conference, …
- **We promote alignment and consistency** between NIS2 and sectorial initiatives and lex specialis

Sustain	• **Energy-electricity** • **Telecoms** • **Core internet and cloud** • **Trust**
Build	• **Health** • **Rail**
Involve	• **Finance** • **Space** • **Aviation**
Prepare	• Public administrations

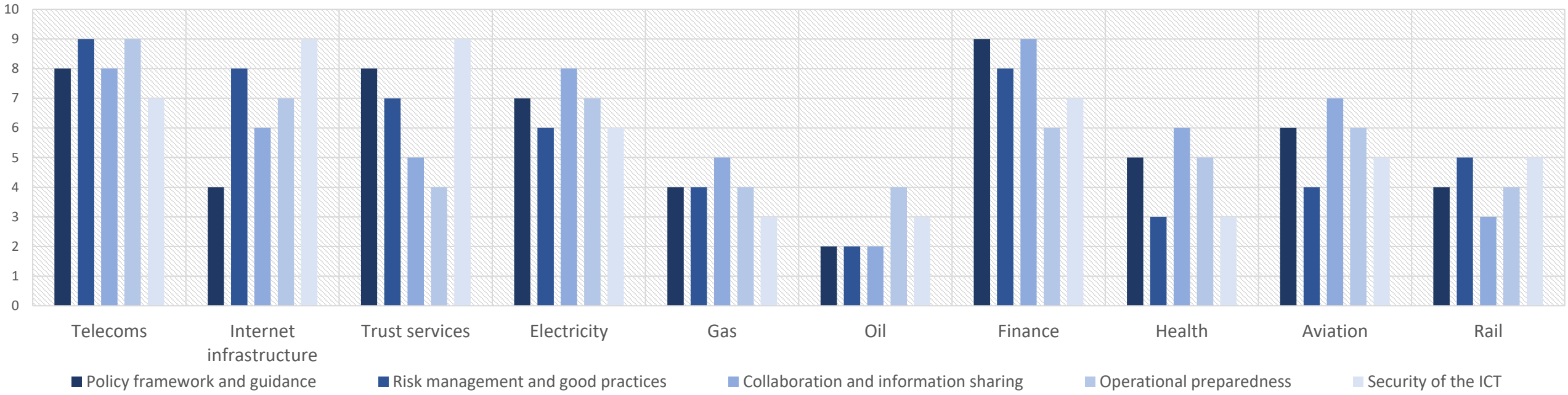
ENISA NIS360 is a our methodology to assess/prioritize sectors across the board

ENISA NIS 360

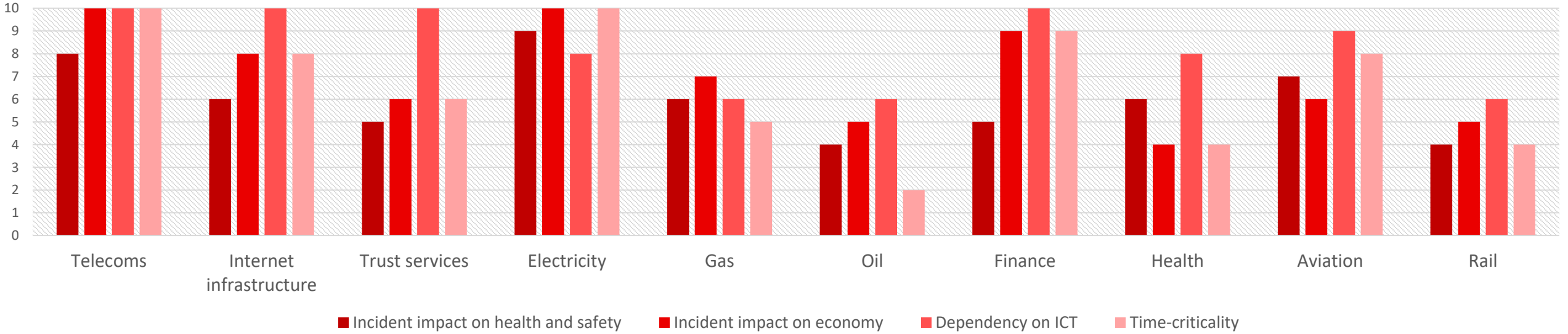
- In 2023 report a first round
  - 10 NIS1 subsectors assessed
  - Working with the national authorities
  - Not public, but shared TLP GREEN (**ask us for a copy**)
- NIS360 outcomes
  - Telecoms, finance, electricity most mature
  - Telecoms, electricity, finance the most critical
  - Oil, Gas, Rail, Health the least mature
  - Internet infrastructure almost as critical as finance
- In 2024 we are making a 2nd edition
  - Many more sectors, including the main NIS2 sectors
  - New methodology which uses also data from industry



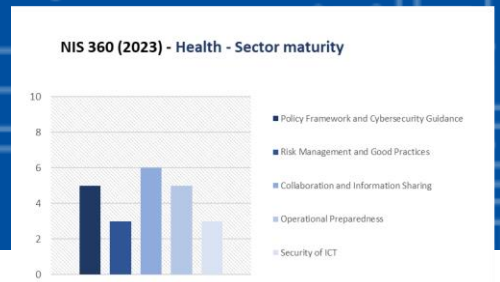
ENISA NIS 360 – 2023 - Maturity dimensions across NIS1 sectors

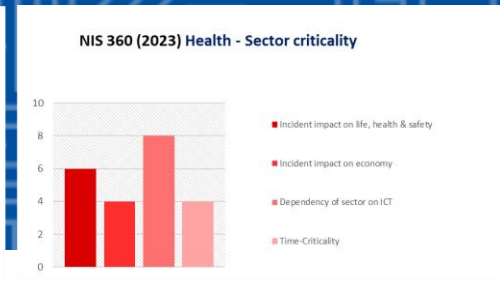


ENISA NIS 360 – 2023 - Criticality dimensions across NIS1 sectors



EXAMPLE: NIS360 FOR HEALTH





- Facts
  - Policy: NIS Directive, MDR, EU Health data space
  - CIRAS: 26% of all incidents are in health,
  - 39% of health incidents impact medical records,
  - 4% impact medical devices,
  - >50% health incidents are ransomware.
  - Average IT spending is 3rd highest,
  - Declaring mature detection and response
- Criticality
- MODERATE, incidents and cyber attacks don't block critical operations

- Maturity

+ Policy framework is established for year, interplay EECC-NIS2 to be better understood

+ Operators do risk management and adopt good practices

+ Collaboration and information sharing takes place, telecom operators participate in ISACs

- 3rd party risks, supply chain risks to be addressed

- Operational preparedness and crisis management can be improved

- Priorities for improvement
  - Policy: Interplay NIS2 MDR (and CRA and AI act)
  - Union risk evaluations Critical assets to be identified, threat taxonomies
  - Information sharing and collaboration: Better sharing with all stakeholders

WHAT'S NEXT FOR NIS2

NIS2 implementing rules for digital infrastructure

- Publication in October 2024, comes into force on 7 November
- See: https://digital-strategy.ec.europa.eu/en/news/new-rules-boost-cybersecurity-eus-critical-entities-and-networks

ENISA technical guidance on NIS2 reporting (one template) and measures (mapped to standards)

- Publication and consultation from 7 November 2024 – On the ENISA website for industry consultation! Have your say!

Transposition and implementation by the 27 EU Member States is ongoing

- Registration of entities under the NIS2 – 1000s or 10.000s of companies – in 2025
- Incident reporting starts – significant impact, but also voluntary reporting, e.g. about near-misses (create culture, trust!)
- Supervision of security measures start – get to know each other (partner with big ones, guide smaller ones, help the sector!)

Can we make it easier and simpler, especially for smaller companies? NIS-to-know, European NIS FAQ!

Can we harmonize more? Supervision approaches, reporting templates, security requirements?

Q&A

YOUR INPUT, IDEAS, SUGGESTIONS VERY WELCOME

Email us or connect on Linkedin

ENISA-NIS-Directive@enisa.europa.eu - HansLourens.DeVries@enisa.europa.eu