NOREA 23 September 2024

Network and Information Security directive 2 (NIS 2)

Naamgeving NIS 2 in Nederland:

“De Cyberbeveiligingswet”.

Jan Matto

forvis mazars

Network and Information Security Directive 2 (NIS 2:

Content

A) Setting the scene:

Systemic risks in relation to digitalization

➔ “cybersecurity & data protection” 🡰

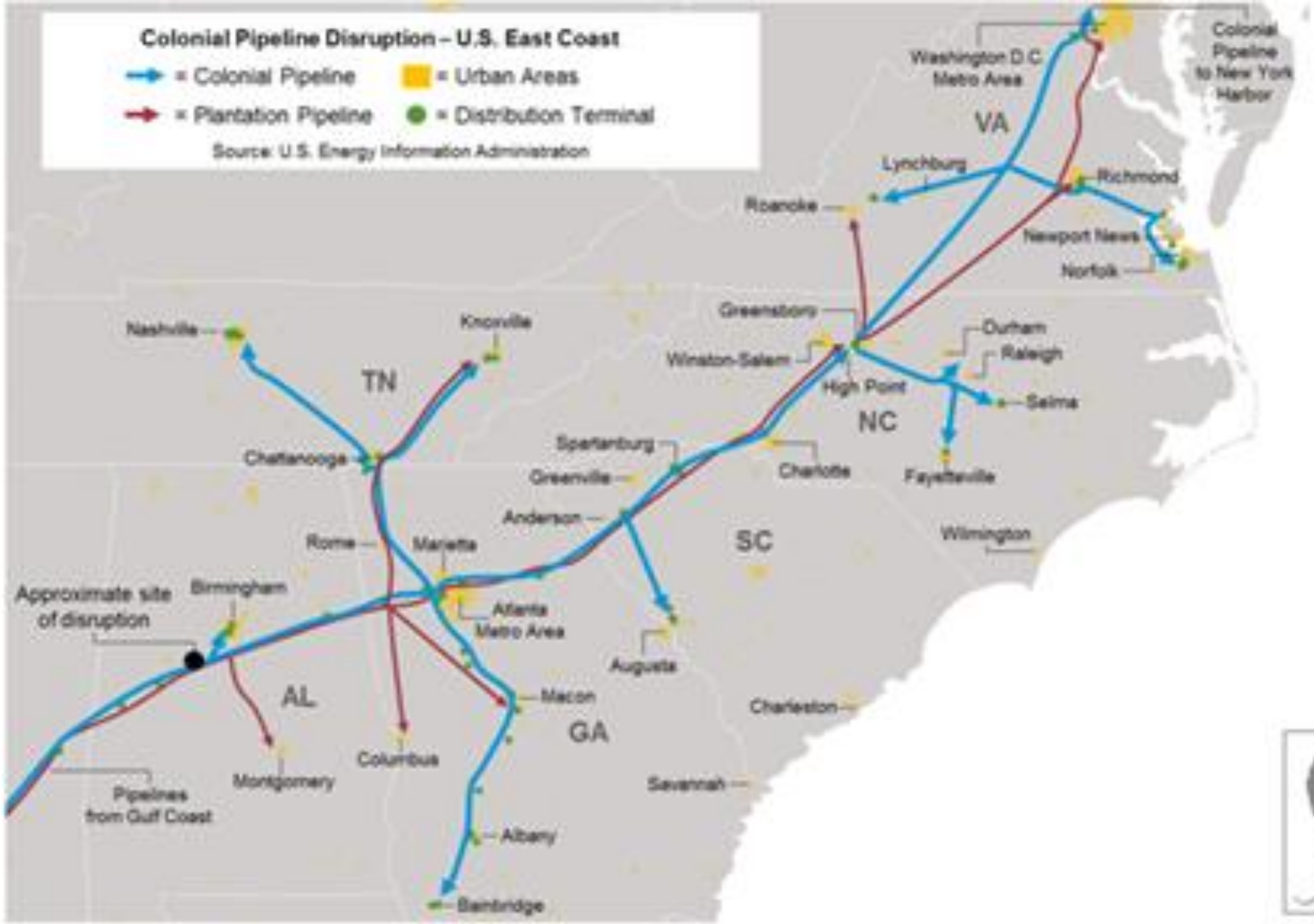
B) Reaction government, regulators, organizations

C) Key high lights NIS 2

D) Impact on the IT Audit profession

NIS 2: background and motivation

The Colonial Pipeline (May, 2021)


Colonial Pipeline Disruption – U.S. East Coast

Source: U.S. Energy Information Administration

NIS 2: background and motivation

What happened with the Colonial Pipeline? Timeline:

- May 6 2021, VPN access from an inactive account
  - Data is being extracted, 100 GB of data stolen in 2 hours.
  - Privilege escalation, Network pivoting and Lateral movement is done
- May 7 2021, ransomware is executed and spread.
  - Colonial pipe line is aware of the attack and shuts down the pipeline.
  - FBI starts investigation
  - The decision was made by the CEO after consultation with cybersecurity experts, US government authorities and insurance carrier to pay the ransom of 75 Bitcoin or 4.4 Million dollars
  - Darkside was to be found the culprit
- May 9, 2021, State of emergency was declared by the president.
  - 2 days after the pipeline went offline, major gas and oil shortages came about in the eastern states.
- May 12 2021, The colonial pipeline is restarted
  - 6 days after the hack the colonial pipeline was back online
- May 13, 2021 Colonial pipeline is fully operational

NIS 2: background and motivation

Colonial Pipeline ransomware attack: Aftermath

Financial Impact

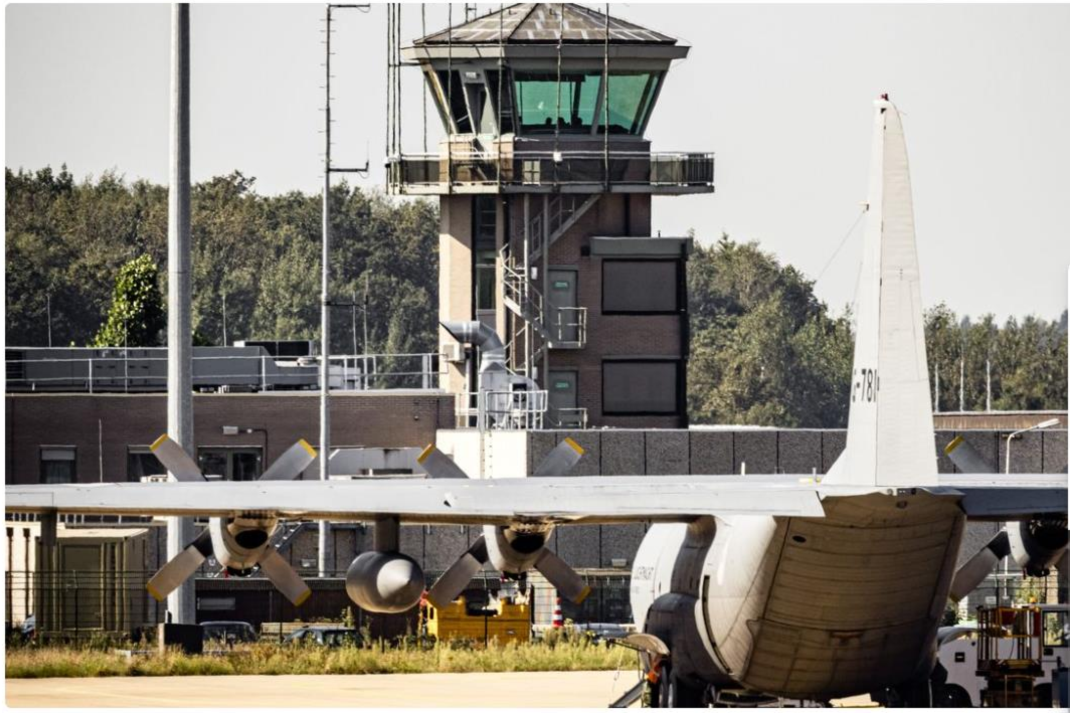
- Ransome of 75 bitcoin
  - Valued at 4.4 million dollars at the time
- In June 7 2021 67 bitcoins were seized from the original ransom payment
  - Valued at 2.3 million dollars at the time

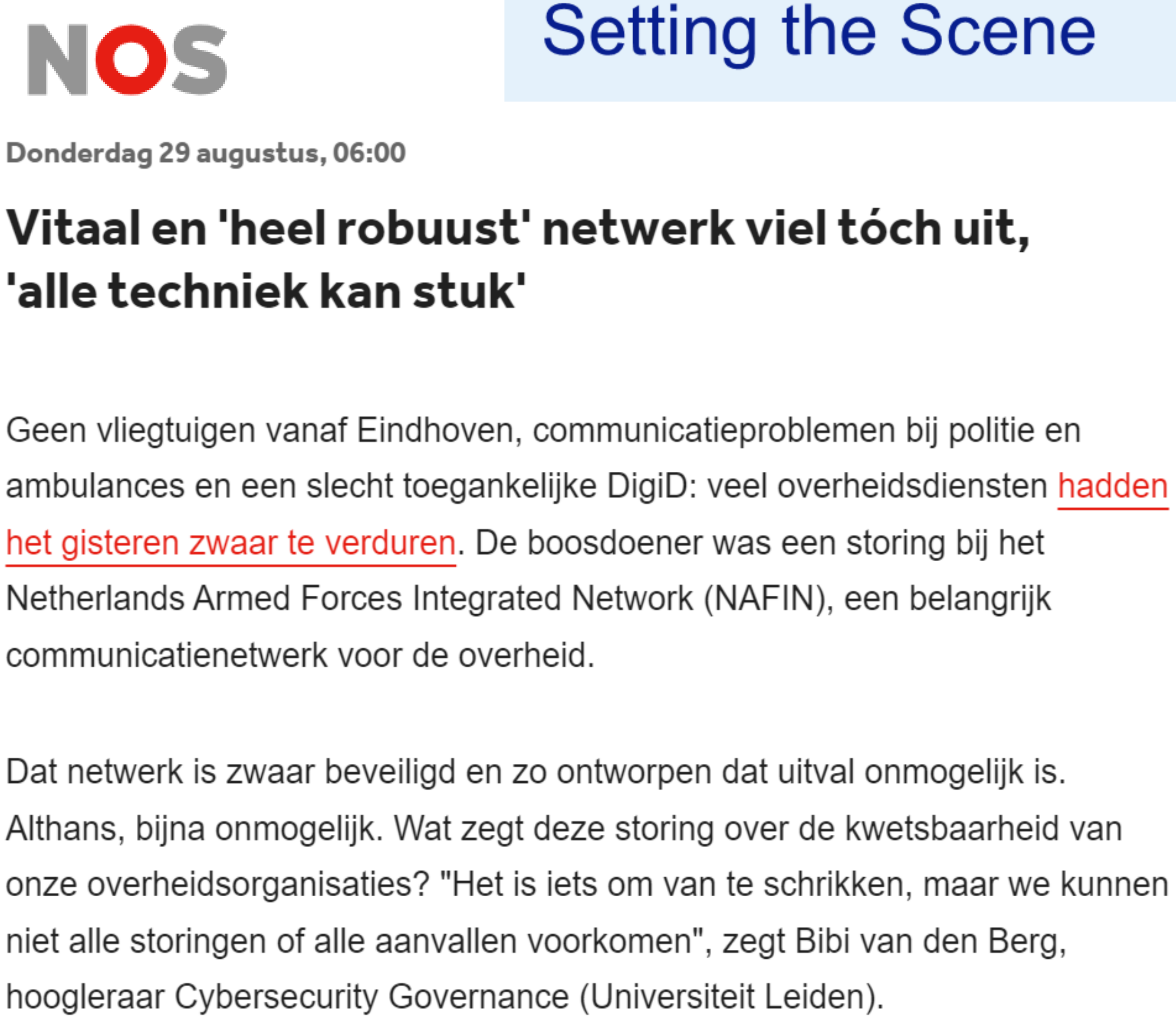
Other Impact

- State of emergency in 3 states.
- Transportation of aviation fuel was impacted
  - American Airlines had to put extra stops into some long haul routes
  - United Airlines and Southwest had to take extra fuel on flights
- A shortage of certified truck drivers that can drive tanker trucks we too few available
  - Many were laid of during covid
  - Had their license revoked
- Fears of inflation driven by spot energy price surges
- Millions of people without fuel in a car depended environment
  - Extreme gas prices due to panic buying

NAFIN Defensie netwerk

Setting the Scene





NOS

Donderdag 29 augustus, 06:00

Vitaal en 'heel robuust' netwerk viel tóch uit, 'alle techniek kan stuk'

Geen vliegtuigen vanaf Eindhoven, communicatieproblemen bij politie en ambulances en een slecht toegankelijke DigiD: veel overheidsdiensten hadden het gisteren zwaar te verduren. De boosdoener was een storing bij het Netherlands Armed Forces Integrated Network (NAFIN), een belangrijk communicatienetwerk voor de overheid.

Dat netwerk is zwaar beveiligd en zo ontworpen dat uitval onmogelijk is. Althans, bijna onmogelijk. Wat zegt deze storing over de kwetsbaarheid van onze overheidsorganisaties? "Het is iets om van te schrikken, maar we kunnen niet alle storingen of alle aanvallen voorkomen", zegt Bibi van den Berg, hoogleraar Cybersecurity Governance (Universiteit Leiden).

BRON:

Vitaal en 'heel robuust' netwerk viel tóch uit, 'alle techniek kan stuk' (nos.nl)

NIS 2: background and motivation

Other issues:

Management process versus IT reality

Compliance audit versus product audit

History versus actuality and future

- Cyber security / information security has a strong focus on management processes and allocation of responsibilities
- The idea of management system good, so system safe does not direct apply to digital infrastructures
- IT reality remains too underexposed
- Risks arise not only from “internal organization and systems” but also from new threats emerging outside the organization.
- Think of new vulnerabilities, new IT resources deployed at suppliers and customers, etc.
- In other words, monitoring risks is not only possible based on monitoring one's own organization and systems, but risks in the digital supply chain or “ecosystem” must also be monitored and evaluated on an ongoing basis.

NIS 2: background and motivation

Setting the Scene

To summarize a few observations and/or statements:

- A digital incident could affect the entire ecosystem of an organization
- Data breaches are cumulative in terms of risk impact
- The social and economic damage can be much more significant than the damage to an individual organization
- Risk management is (still) too focused on individual or own business operations
- Cloud computing and IT outsourcing imply a “loss of governance.”
- The emergence of “information chains makes it more difficult” to get a grip on risks for the responsible “end party.”
- Chain responsibilities are often not or insufficiently clear

The Internet of Everything

Network and Information Security Directive 2 (NIS 2:

Content

A) Setting the scene:

Why NIS 2

Systemic risks in relation to digitalization

➔ “cybersecurity & data protection” 🡐

B) Reaction government, regulators, organizations

C) Key high lights NIS 2

D) Impact on the IT Audit profession

NIS 2: background and motivation

Reaction government

- [ChatGPT (openai.com)]

Systemic risks are risks that have the potential to trigger a chain reaction of failures or disruptions that can ripple through an entire system, sector, society, causing widespread and often severe consequences in unexpected directions and levels.

Cyber systemic risks can manifest in several ways:

1. **Financial System**:
2. **Critical Infrastructure**:
3. **Supply Chain**:
4. **Data Breaches**:
5. **National Security**:.
6. **Public Trust**:
7. **Interconnectedness**:

Managing cyber systemic risks involves a combination of cybersecurity measures, risk assessment, contingency planning, and international cooperation. Governments, organizations, and individuals must work together to mitigate these risks and strengthen the resilience of digital systems to minimize the potential for systemic disruptions.

Risk dimensions in system theory

Reaction government

Definition of digital risks in perspective of digital systems

Depending of the system layer or level:

a) **System Risk** - risk in a specific system
Example a risk in a specific application or module in use
(local risk. Limited to the perimeter of the system object)

b) **Systematic Risk** – risk that is inherent to a specific type
of system (example a standard application, cloud service, …)

c) **Systemic Risks** – risks that disrupts a complete sector,
ecosystem, supply chain or society

Reaction government / regulators

NIS 2: background and motivation

Digital systemic risks?

- Digital Systemic Risks are on the agenda of the EU and regulators
- Concentration risks: disruptions on complete sectors / economy/ society
- Undermining of democratic processes, manipulation of data
- Disruptions of markets through large digital platforms and search engines
- Data monopolies disrupt free competition
- Distribution of illegal products / content / IE;
- Digitalisering and especially AI increases the risk of digital discrimination / exclusion
- Loss of governance, accountability and responsibility because of use of digtal technologies (Loss of digital or data sovereignty)

Network and Information Security Directive 2 (NIS 2:

Content

A) Setting the scene:

Why NIS 2

Systemic risks in relation to digitalization

➔ “cybersecurity & data protection” 🡨

B) Reaction government, regulators, organizations

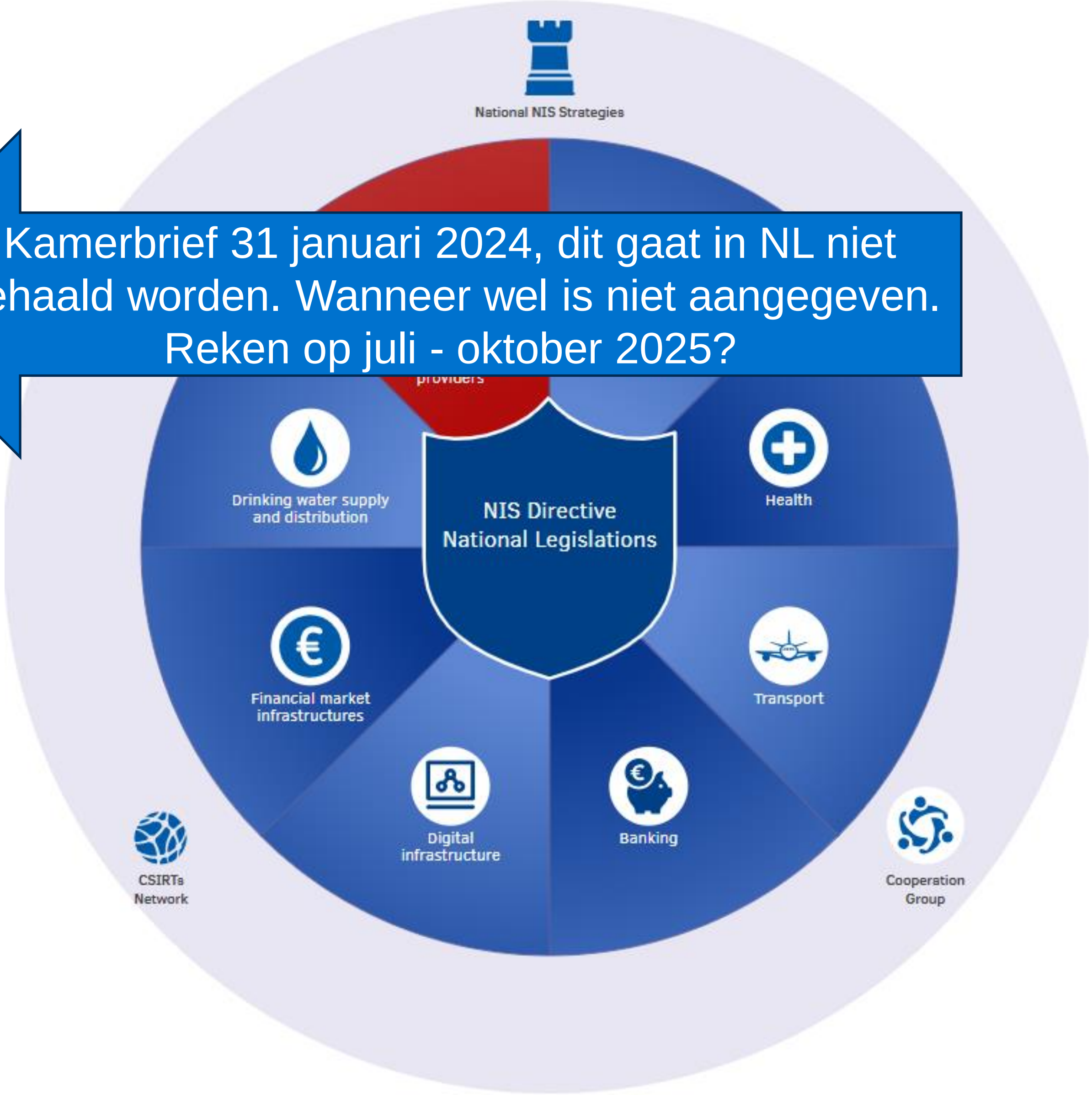
C) Key high lights NIS 2

D) Impact on the IT Audit profession

NIS 2: background and motivation

Context

- NIS 2 directive is the successor of the NIS 1 directive from 2016
  - Converted into national law by 17 October 2024
  - Apply from 18 October 2024
- Addressing following shortcomings of NIS 1:
  - Insufficient level of cyber resilience
  - Inconsistent resilience across Member States and Sectors
  - Insufficient common understanding of threats
  - No joint crisis response
- Including more sectors from 8 sectors to 18
- Closely linked with two other legislations:
  - Critical Entities Resilience (CER) Directive
    - Physical safety & security of vital processes
  - Digital Operational Resilience ACT (DORA) regulation
- Coordination Group of NIS 2 to align CER and DORA



Kamerbrief 31 januari 2024, dit gaat in NL niet gehaald worden. Wanneer wel is niet aangegeven. Reken op juli - oktober 2025?

NIS 2: background and motivation

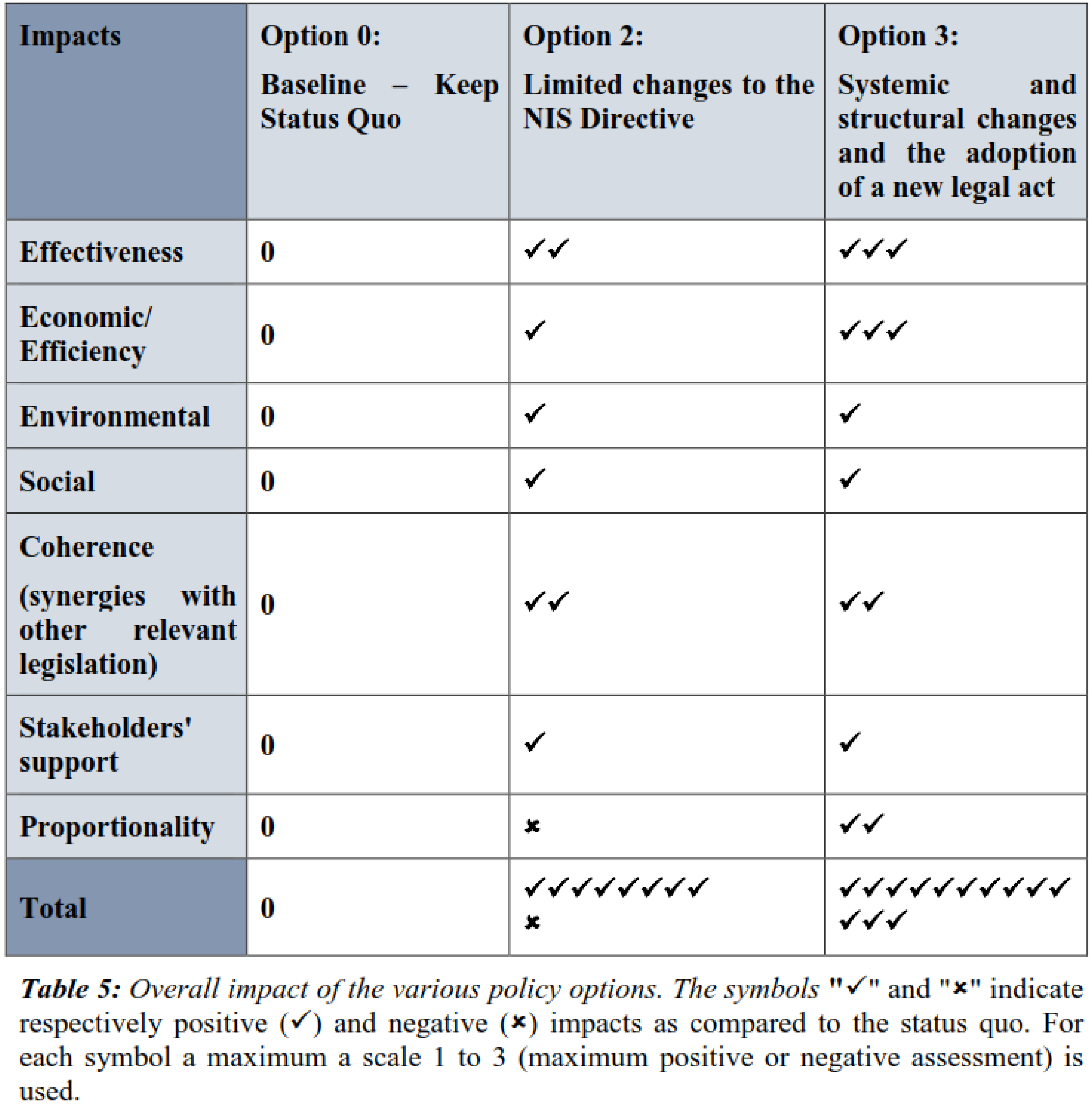
Policy choice EU

After Impact assessment for NIS 2:

- Option 3 preferred

A Directive was preferred:

- More cost efficient
- More implementation time
- Fine tuning and flexibility per Member State



Impacts	Option 0: Baseline – Keep Status Quo	Option 2: Limited changes to the NIS Directive	Option 3: Systemic and structural changes and the adoption of a new legal act
Effectiveness	0	✓✓	✓✓✓
Economic/ Efficiency	0	✓	✓✓✓
Environmental	0	✓	✓
Social	0	✓	✓
Coherence (synergies with other relevant legislation)	0	✓✓	✓✓
Stakeholders' support	0	✓	✓
Proportionality	0	×	✓✓
Total	0	✓✓✓✓✓✓✓✓ ×	✓✓✓✓✓✓✓✓✓✓ ✓✓✓

Table 5: *Overall impact of the various policy options. The symbols* "✓" and "×" indicate respectively positive (✓) and negative (×) impacts as compared to the status quo. For each symbol a maximum a scale 1 to 3 (maximum positive or negative assessment) is used.

High lights

NIS 2: Key Highlights

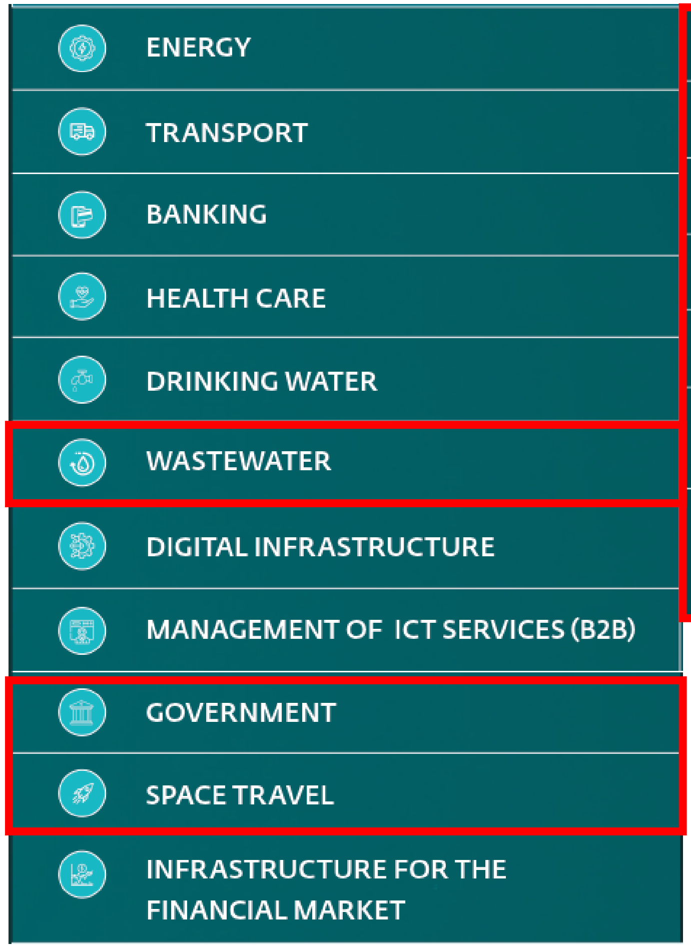
To summarize a few observations and/or statements:

- **New sectors** have been highlighted in red.
- Sets requirements for security organisations in
  - ‘Sectors of high criticality’ (appendix I)
  - ‘Other critical sectors’ (appendix II)

- **Scope has become broader** by introducing a 'size-cap' rule.
  - Organizations with more than 50 employees
  - More than €10 million turnover and €10 million balance sheet
  - Smaller organizations can be included by Member States

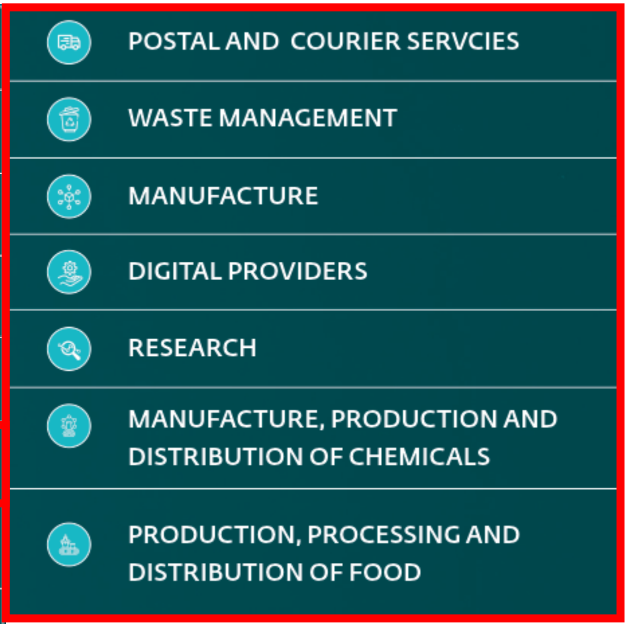
- **Categorisation of Essential and Important entities based on size and turnover/balance sheet**
- Bringing ideas such as the peer reviews for enhancing collaboration and knowledge sharing.

Sectors of high criticality



- ENERGY
- TRANSPORT
- BANKING
- HEALTH CARE
- DRINKING WATER
- WASTEWATER
- DIGITAL INFRASTRUCTURE
- MANAGEMENT OF ICT SERVICES (B2B)
- GOVERNMENT
- SPACE TRAVEL
- INFRASTRUCTURE FOR THE FINANCIAL MARKET

Other Critical Sectors



- POSTAL AND COURIER SERVCIES
- WASTE MANAGEMENT
- MANUFACTURE
- DIGITAL PROVIDERS
- RESEARCH
- MANUFACTURE, PRODUCTION AND DISTRIBUTION OF CHEMICALS
- PRODUCTION, PROCESSING AND DISTRIBUTION OF FOOD

RDI: NIS2 Zelfevaluatie NL (regelhulpenvoorbedrijven.nl)

High lights

NIS 2: Key Highlights

To summarize a few observations and/or statements:

Decision tree Essential or Important entity based on combination of specific sector and size entity:

Midsize

- Organizations with more than 50 employees, or
- More than €10 million turnover and €10 million balance sheet
- Smaller organizations can be included by Member States

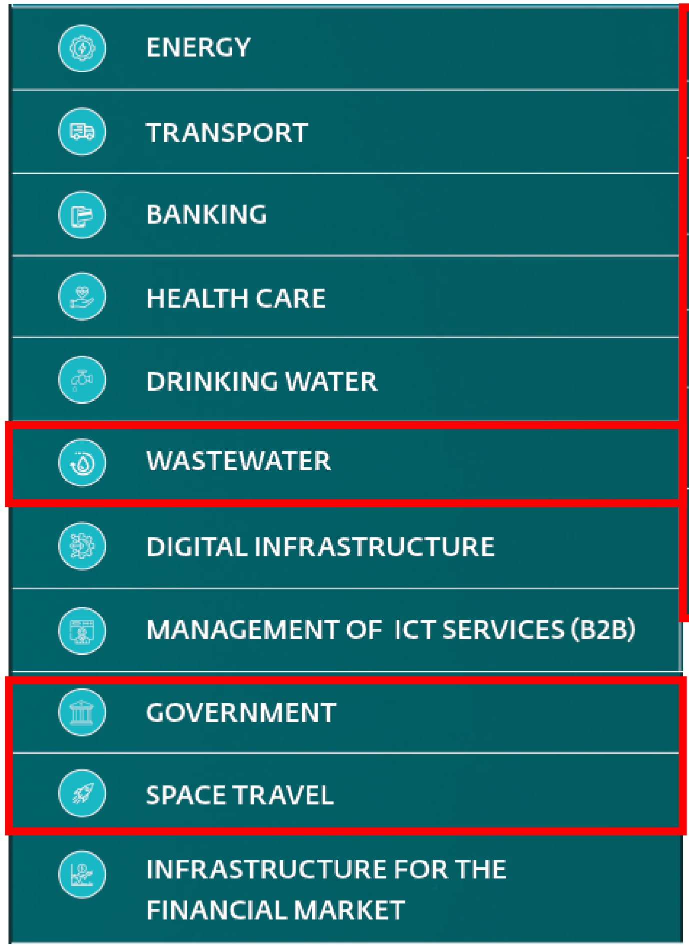
Large

- Organizations with more than 250 employees, or,
- More than €50 million turnover and €43 million balance sheet

Government, public services electronic communication network services, DNS service, domain registrars will always be regulated by NIS2 regardless their size.

RDI: [NIS2 Zelfevaluatie NL (regelhulpenvoorbedrijven.nl)](regelhulpenvoorbedrijven.nl)

Sectors of high criticality



ENERGY

TRANSPORT

BANKING

HEALTH CARE

DRINKING WATER

WASTEWATER

DIGITAL INFRASTRUCTURE

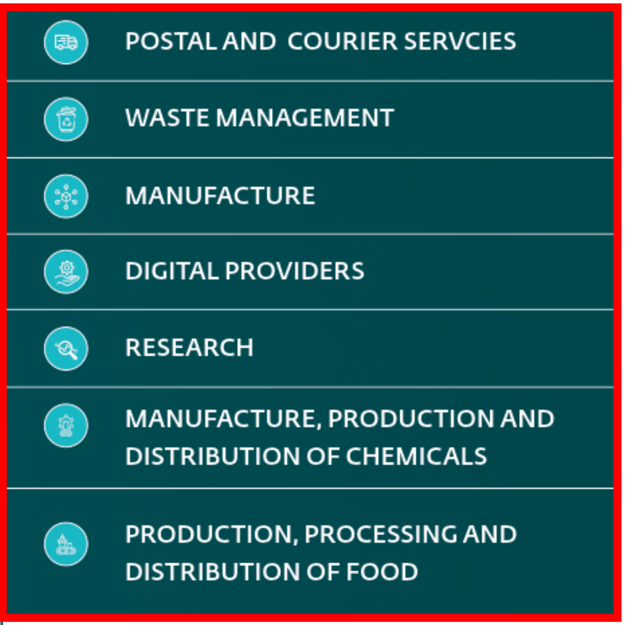
MANAGEMENT OF ICT SERVICES (B2B)

GOVERNMENT

SPACE TRAVEL

INFRASTRUCTURE FOR THE FINANCIAL MARKET

Other Critical Sectors



POSTAL AND COURIER SERVCIES

WASTE MANAGEMENT

MANUFACTURE

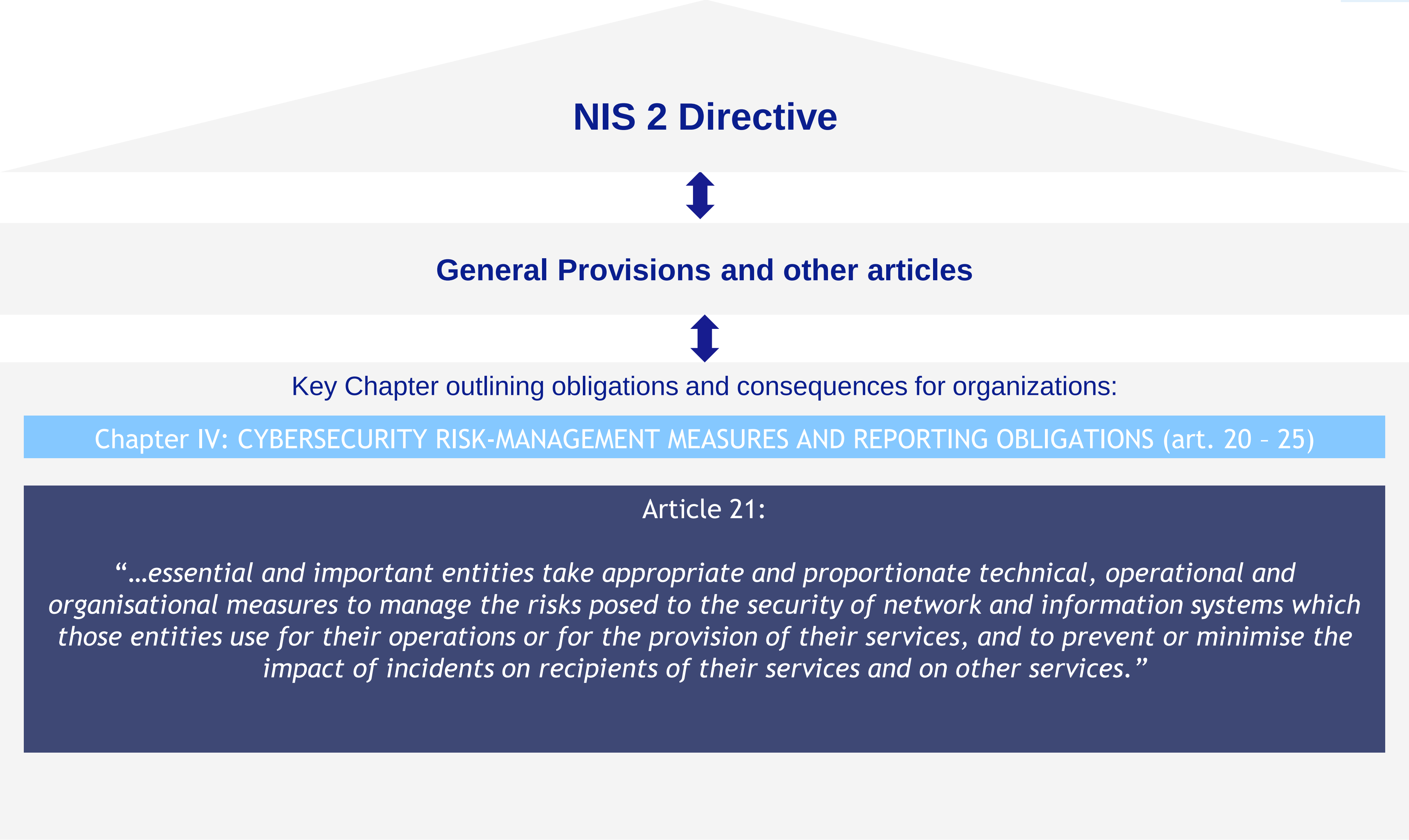
DIGITAL PROVIDERS

RESEARCH

MANUFACTURE, PRODUCTION AND DISTRIBUTION OF CHEMICALS

PRODUCTION, PROCESSING AND DISTRIBUTION OF FOOD

NIS 2 – Outline of requirements



NIS 2 Directive

General Provisions and other articles

Key Chapter outlining obligations and consequences for organizations:

Chapter IV: CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS (art. 20 – 25)

Article 21:

"…essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services."

NIS 2 – General provisions

Registration of entities

Article 3

Highlights

➔ Registration of essential, important entities and DNS services by Member States before April 17, 2025

➔ Should at least include following information:

- Name of entity
- Contact details, e-mail, IP ranges and phone number(s)
- Sector and subsector as per Annex I or II
- List of Member States where service is provided

➔ Might be submitted by entities themselves

- updates within two weeks after change

High lights

NIS 2 – General provisions

Definitions

Article 6

Some definitions

- ‘**Near miss’:** means an event that **could have** compromised the **availability, authenticity, integrity or confidentiality** of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was **successfully prevented** from materialising or that did not materialise
- **‘incident’:** means an event **compromising the availability, authenticity, integrity or confidentiality** of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

- Near misses can be reported on voluntary basis (article 30), Incidents need to be reported (article 23)

NIS 2 – General provisions

National Cybersecurity Strategy

Article 7

Obligations for member states

- National cybersecurity strategy per member state containing among others:
  - Objectives and priorities, covering sectors falling under NIS 2
  - Governance framework on national level
  - Plan to enhance general level of cybersecurity awareness among citizens
  - Addressing cybersecurity in supply chains

NL Cyber security strategy 2022-2028

Goals

Goal 1:
Better insight on threats

Goal 2:
More cybersecurity specialists

Goal 3:
Government and sectors take responsibility

Goal 4:
Better enforcement and necessary rules and regulations

Goal 5:
Clear guidance from national cybersecurity autority

Pillars

**I:
Digital resilience**

**II:
Secure & Innovative**

**III:
Counter digital threats**

**IV:
Cyber skills and jobs**

NIS 2 – General provisions

Essential and Important entities

Essential entities:

- Stricter regime, **ex ante supervisory**
- Documentation obligation of security measures taken
- Periodic targeted security audits by independent body or competent authority
  - Paid by the entity itself
- Submission of audit reports in the field of cybersecurity

Important entities:

- **Ex post supervisory regime**
  - Supervision in the event of indications or evidence that NIS 2 has not been met
- Still provide evidence / undergo audits.
  - Also paid by the entity itself

NIS 2 – Outline of requirements

Cybersecurity risk-management measures

Article 20 - Governance

Highlights

- Management needs to:
  - approve the cybersecurity measures (article 21)
  - Oversee its implementation
- Can be held liable of measures are not implemented
- Management are required to receive training for cybersecurity risk management

A closer look on the risk management measures and reporting obligations

NIS 2 – Outline of requirements

Cybersecurity risk-management measures

Article 21 Cybersecurity Measures

Highlights

- Appropriate and proportionate **technical**, **operational** and **organizational** measures
  - For all risks (e.g. system failures, physical, human)
- Total of 10 categories of measures to be included
  - With everything that goes with it, from business continuity policies and plans to encryption of communications and cybersecurity trainings
- **Further technical and methodological requirements shall be adopted by 17th of October 2024**

forvis mazars

NIS 2 – Outline of requirements

Cybersecurity risk-management measures

Article 21.2

Highlights (10 categories)

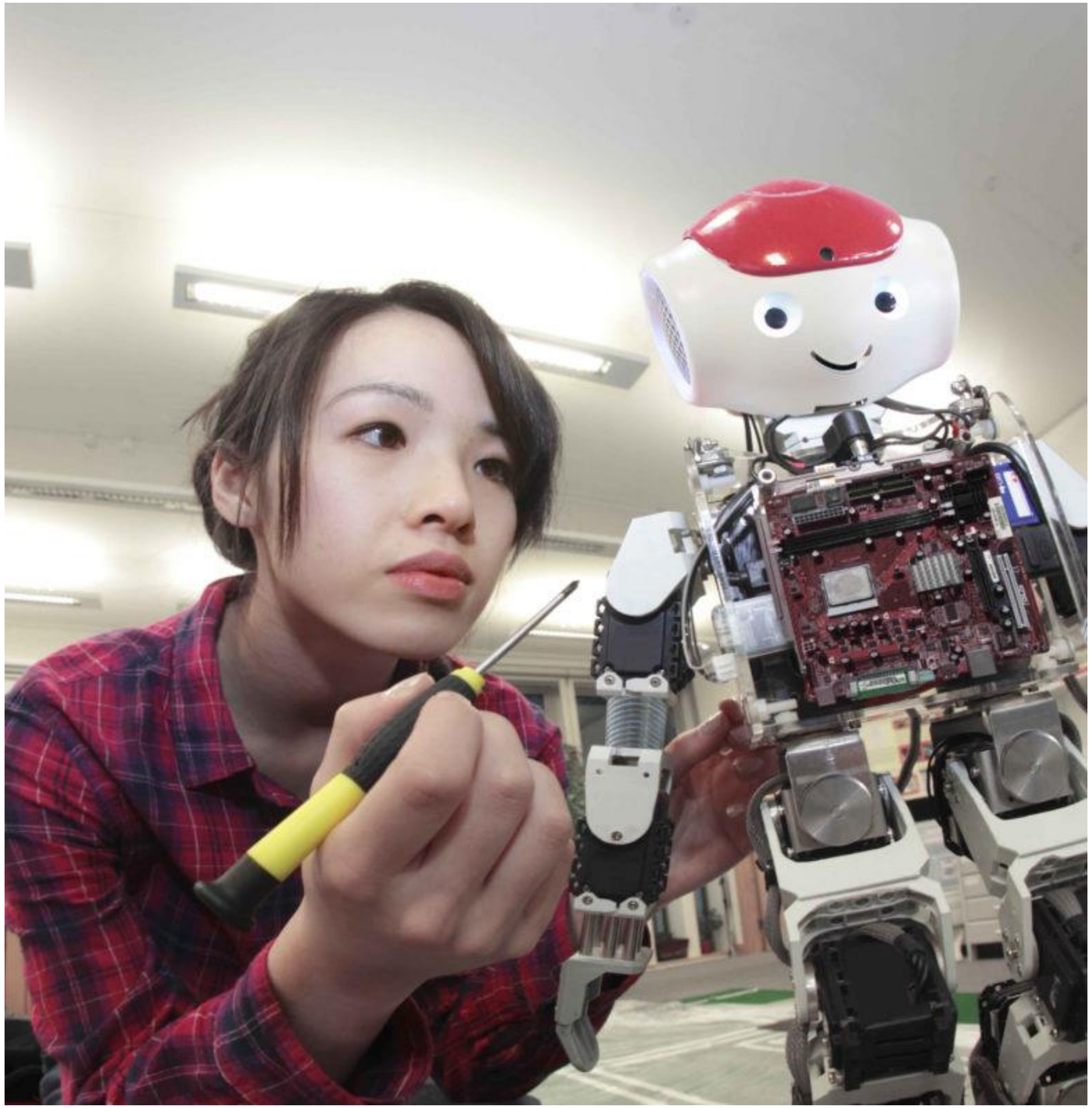
A. Policies on risk analysis and information system security;

B. Incident handling;

C. Business continuity, such as backup management and disaster recovery, and crisis management;

D. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

E. Security in network and information systems acquisition, development and maintenance, **including vulnerability handling** and disclosure;



NIS 2 – Outline of requirements

Cybersecurity risk-management measures

Article 21.2

Highlights

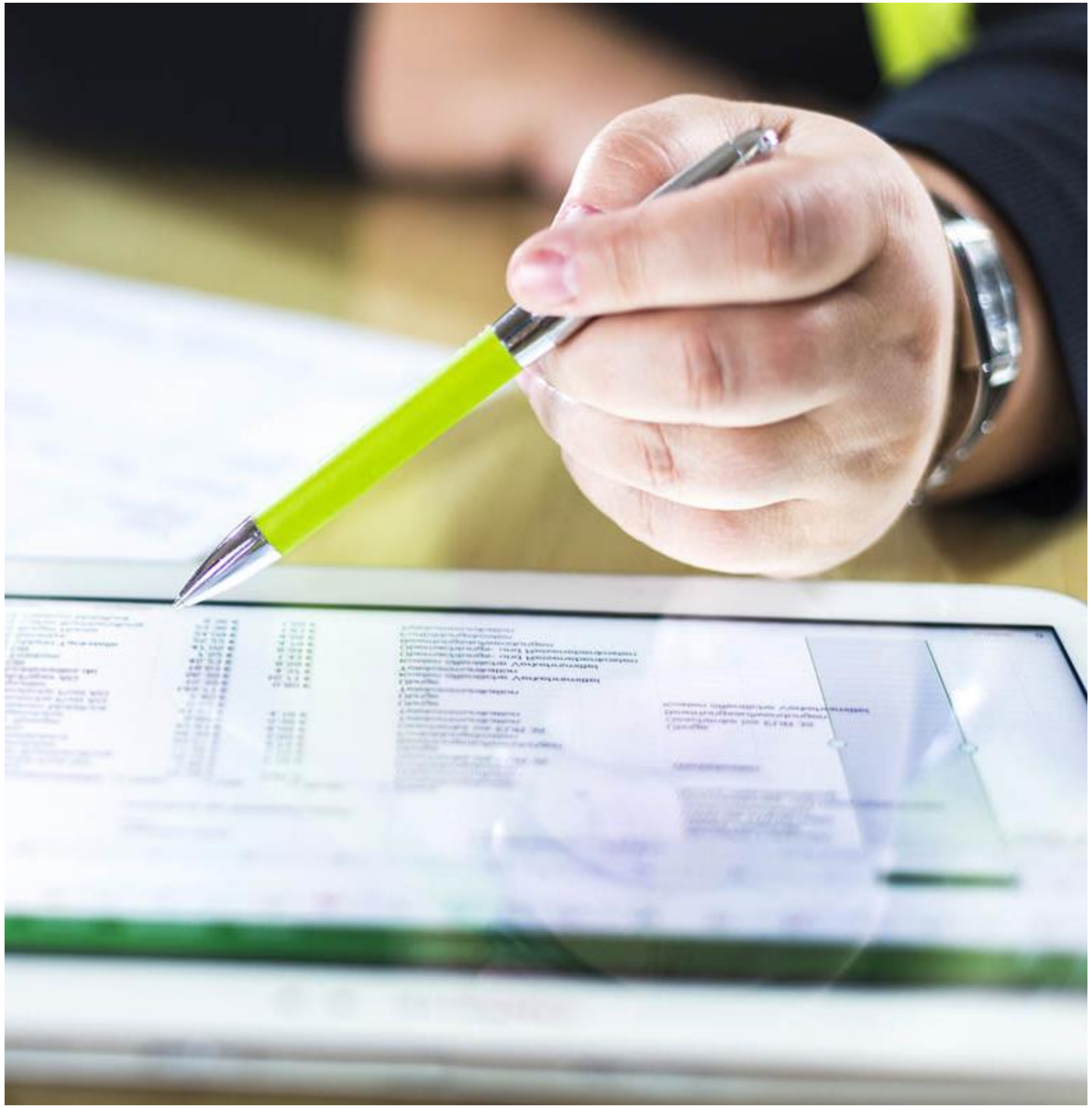
F. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

G. Basic cyber hygiene practices and cybersecurity training;

H. Policies and procedures regarding the use of cryptography and, where appropriate, encryption;

I. Human resources security, access control policies and asset management;

J. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.



NIS 2 – Several obligations explained

Cybersecurity risk-management measures

Article 22 – Union level coordinated security risk assessment of critical supply chains

Highlights

- The Cooperation Group, Commission and ENISA:
  - Coordinated security risk assessments, critical ICT supply chains
- It should help to:
  - Counter critical dependencies
  - Identify single points of failure
  - Identify threats, vulnerabilities and other risks
- Criteria for selection of supply chain:

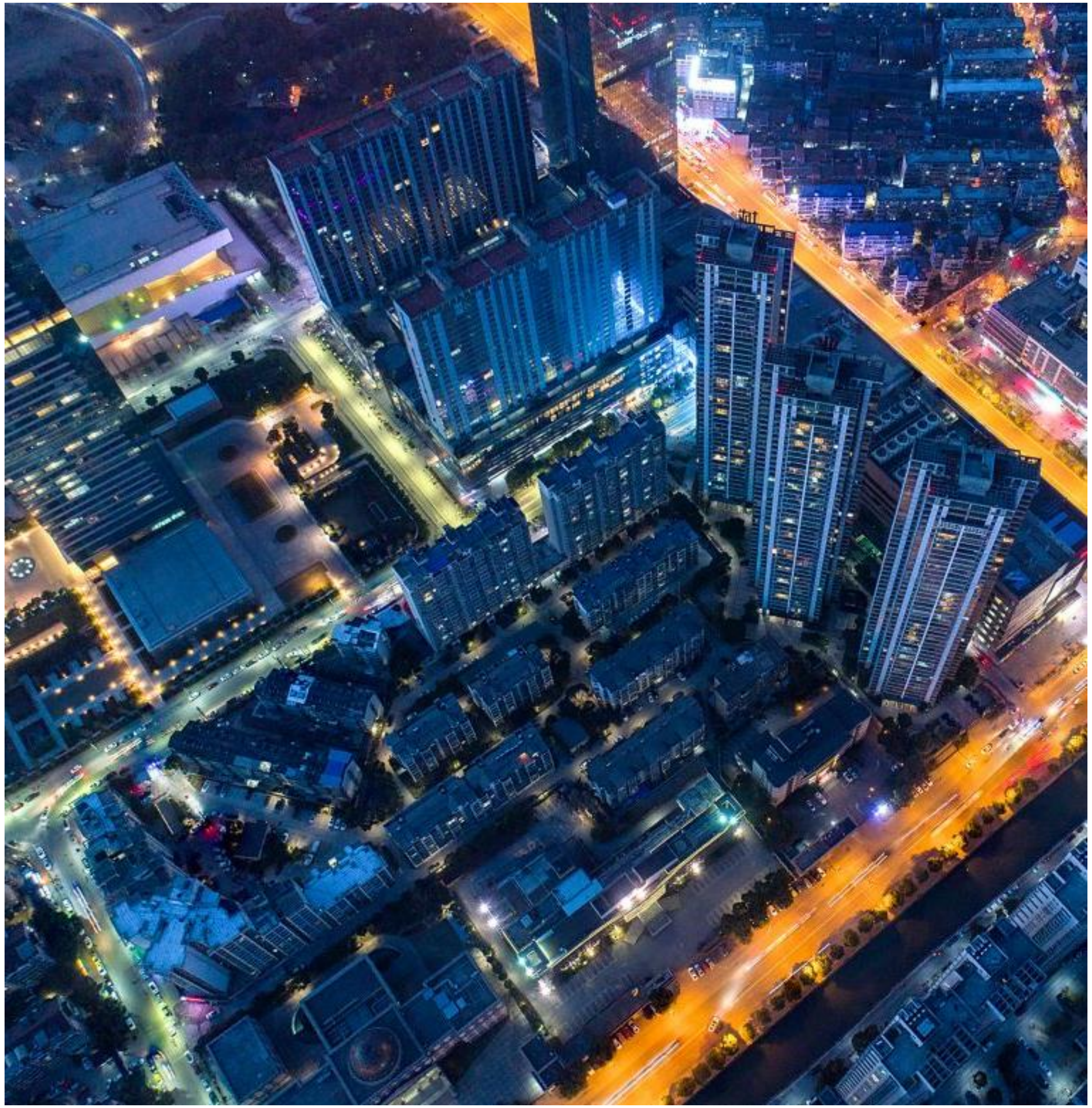
  I. Reliance

  II. Needed for performing critical or sensitive functions

  III. Availability of alternatives

  IV. Resilience of overall supply chain

  V. Potential future significance for the activities



NIS 2 – Monitoring and enforcement

Incident reporting

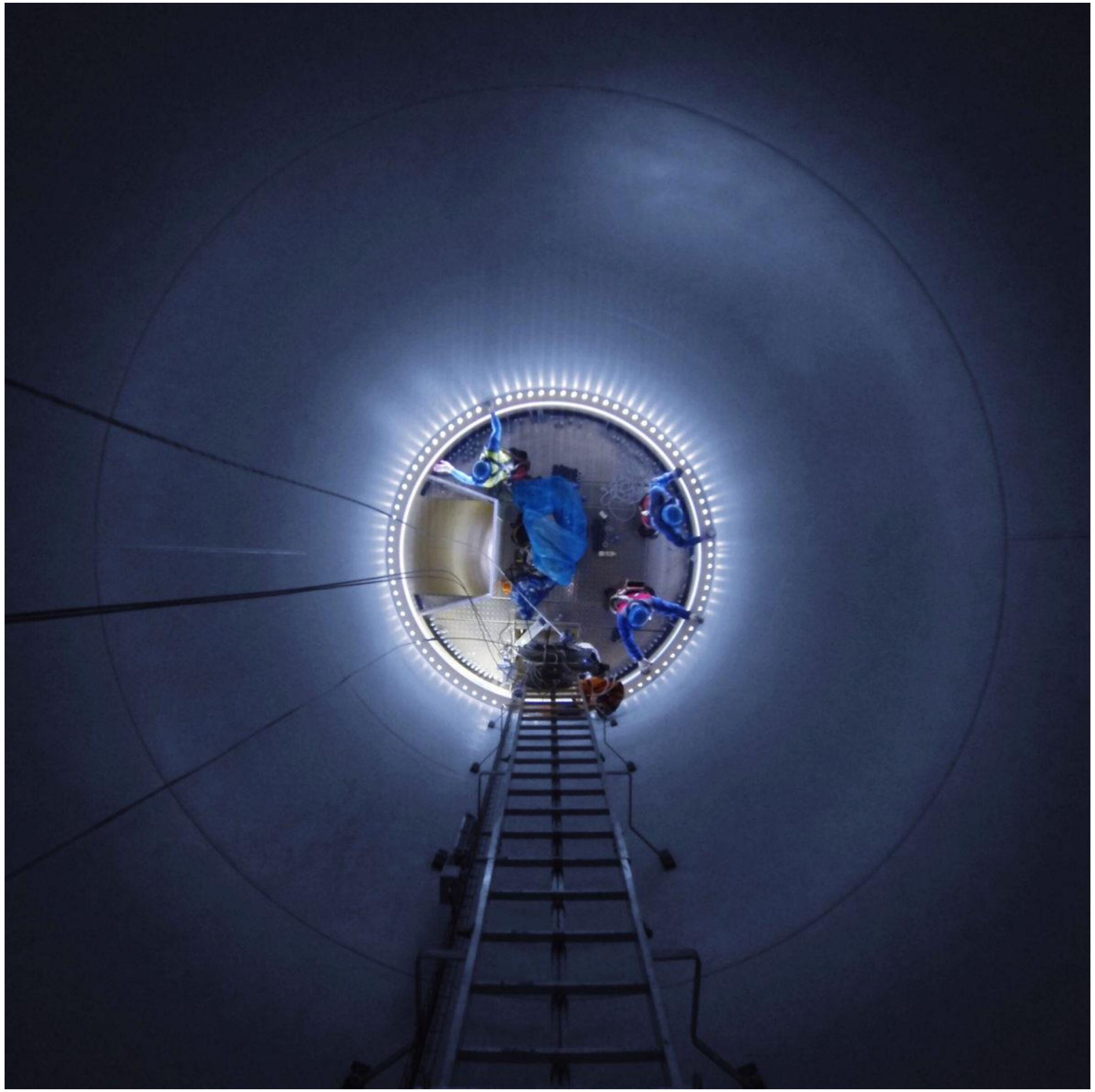
Article 23 - Reporting obligations

Highlights

- Significant incidents must be reported to the CSIRT(s) appointed by the member states of the EU.
  - The recipients of the organisation’s services must also be notified.

- An incident will be considered signifcant when:
  - It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
  - And it has affected or **is capable of affecting** other natural or legal persons by causing considerable material or non-material damage.

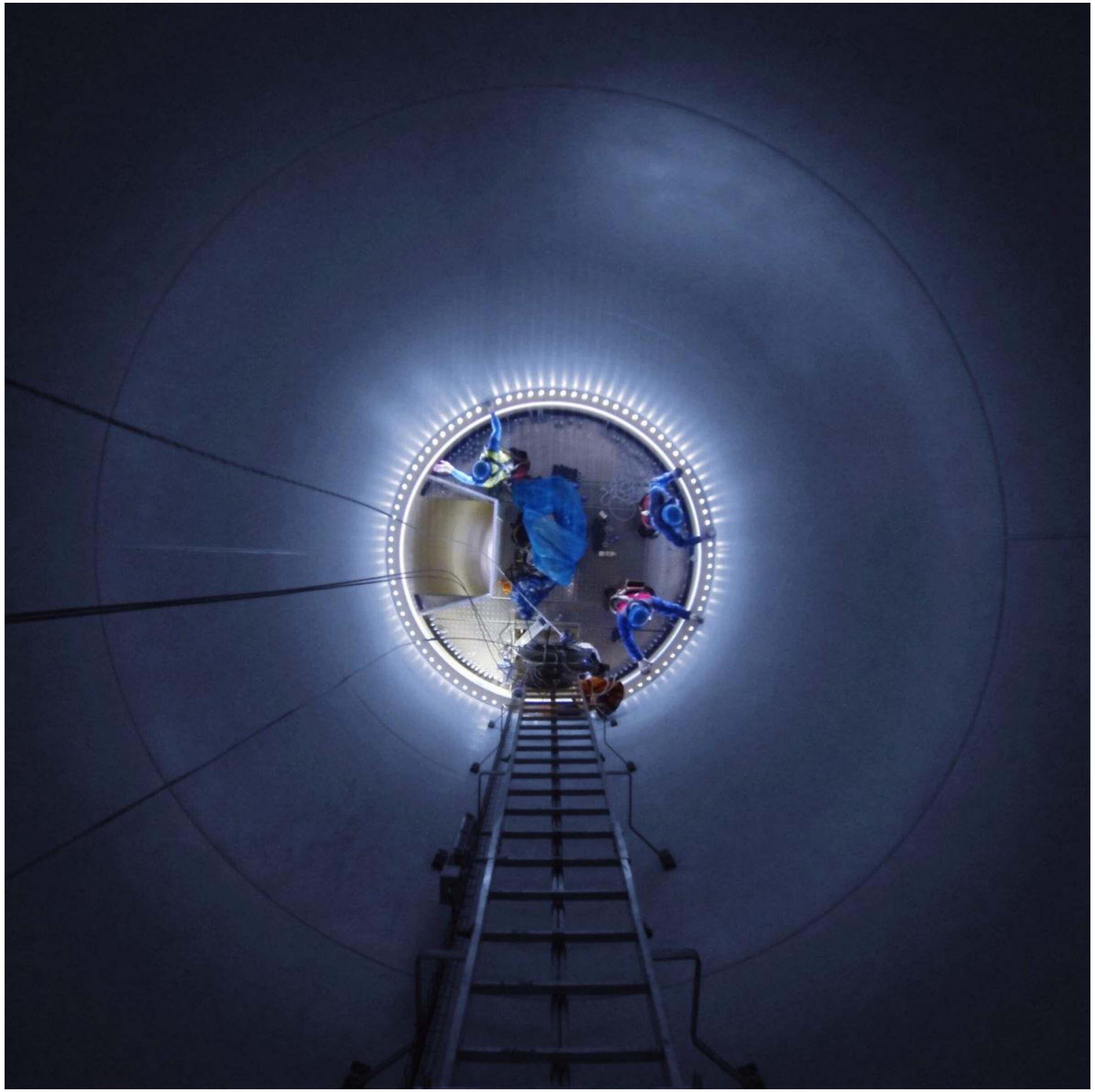
- In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided.



NIS 2 – Monitoring and enforcement

Incident reporting

Article 23 - Reporting obligations



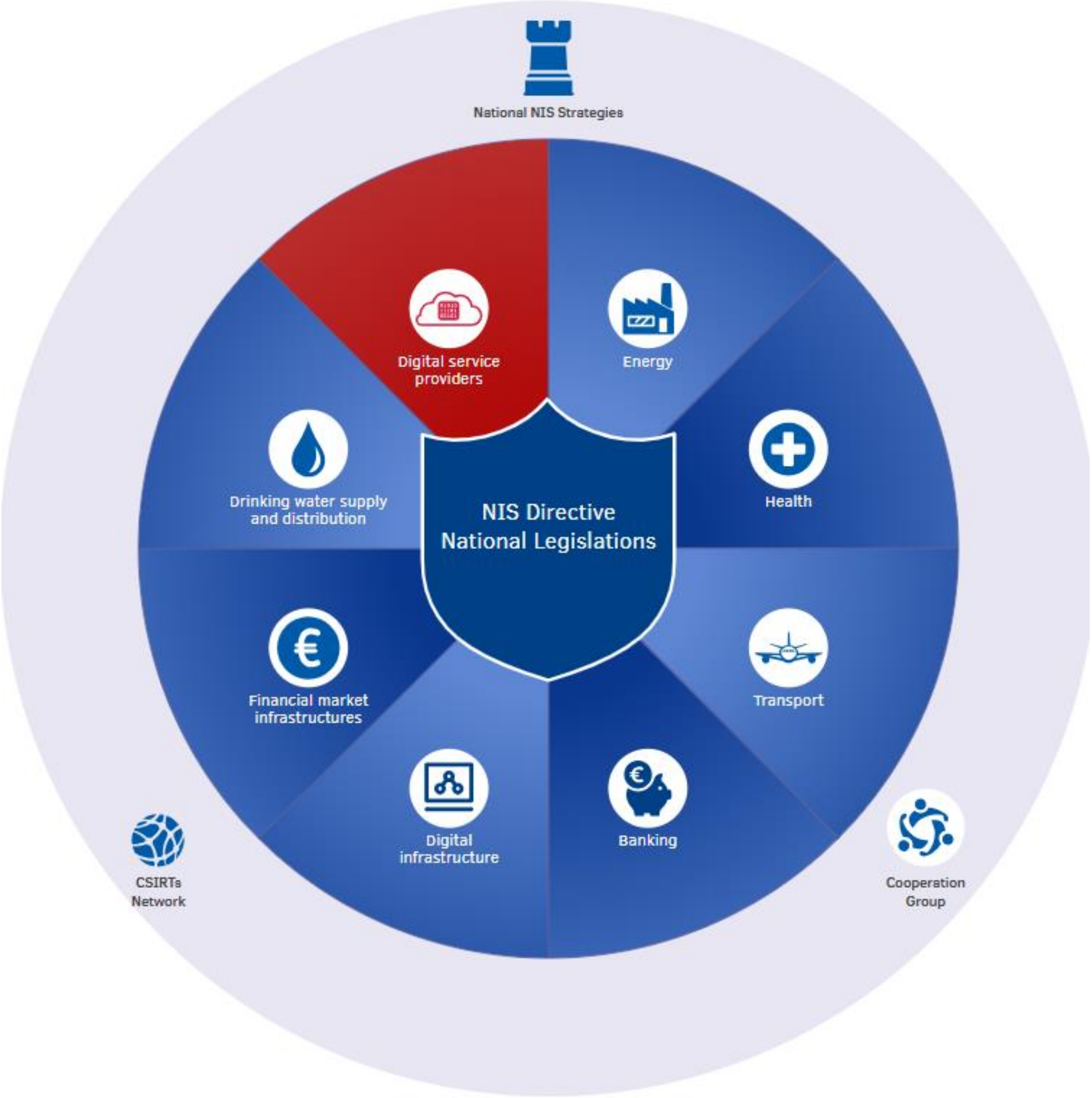
Highlights

- When reporting a significant incident to a CSIRT the following conditions must be met:
  - **In any event within 24 hours of becoming aware of the significant incident.**
    - An early warning, which may indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
  - **After 72 hours:**
    - Update of information and indication of initial assessment of the significant incident
    - Upon the request of a CSIRT or another competent authority, an intermediate report on relevant status updates must be provided;
  - **Not later than one month after the submission of the incident:**
    - A detailed description of the incident, including its severity and impact;
    - The type of threat or root cause that is likely to have triggered the incident;
    - Applied and ongoing mitigation measures;
    - Where applicable, the cross-border impact of the incident;

NIS 2- Reporting
Competent authorities

Where to report?

- ENISA provides an easy to use tool for NIS 1
  - Hopefully it will be updated
- Authorities for NIS 2 yet to be decided by each member state
- Computer Security Incident Response Teams (CSIRTs) to be informed of any incidents, similar to NIS 1



forvis mazars

NIS 2 – Monitoring and enforcement

Certification schemes

Article 24 – Cybersecurity certification schemes

Highlights

- Entities might be required to use particular ICT products, services and processes that are certified
- As defined in the Cyber Security Act
- Work in progress:
  - EUCC (Cybersecurity certification)
  - EUCS (Cybersecurity Cloud services certification)
  - EU5G (5G network certification)

01010
11101
00101
CYBERSECURITY
CERTIFICATION
EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS

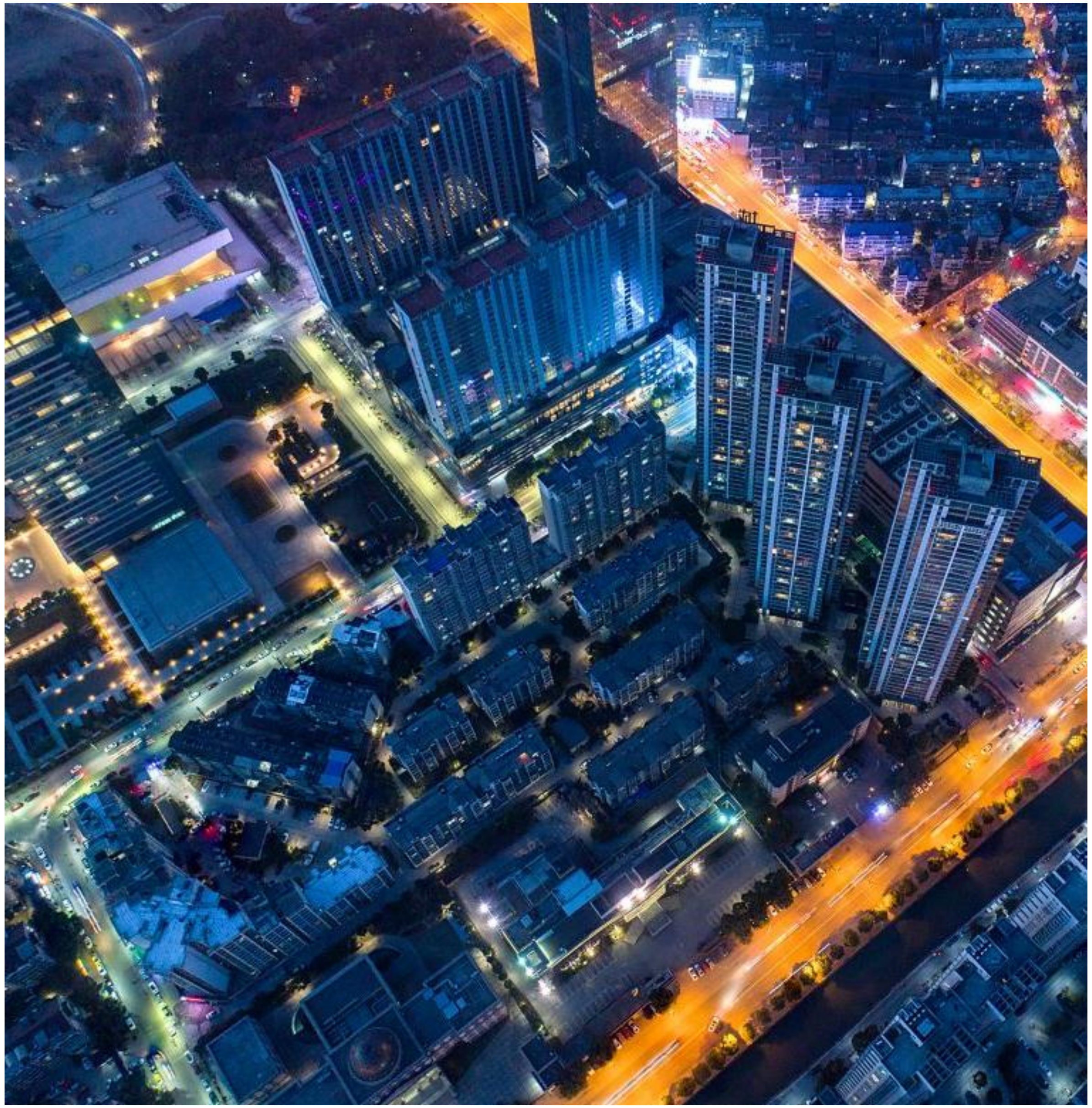
NIS 2 – Several obligations explained

Cybersecurity risk-management measures

Article 32 -33 Supervisory measures

Highlights / limited overview

- Inspections by regulators
- Independent audits and follow up of findings
- Disclosure to the authorized bodies of audits and security assessments
- Security assessments based on transparent and objective criteria
- Documentation and proof of the execution of the security policies
- Appointment of a internal control functionary
- …..



NIS 2: ENISA

Tasks assigned to ENISA for NIS 2:

- The development and maintenance of a European vulnerability registry.
- The secretariat of the European Cyber Crises Liaison Organisation Network (EU-CyCLONe).
- The publication of an annual report on the state of cybersecurity in the EU.
- To support the organisation of peer reviews between member states.
- The creation and maintenance of a registry for entities providing cross-border services e.g DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers and data centre service provider.
- ENISA, in cooperation with Member States and relevant stakeholders, shall draw up advice and guidelines regarding already existing standards, including national standards, which would allow for the new areas of interest to be covered.

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

NIS 2 - Possible consequences

Fines and monitoring

Essential entities

Administration fine for failure to comply with the duty of care or reporting:

- A maximum fine of at least 7,000,000 euros
- Or at least 1.4% of global annual revenue in the prior financial year; depending on which amount is higher

Important entities

Administration fine for failure to comply with the duty of care or reporting:

- A maximum fine of at least 10,000,000 euros
- Or at least 2% of global annual revenue in the prior financial year; depending on which amount is higher

In addition, permits can be temporarily suspended or a natural person, such as the CEO, can be temporarily suspended.

Network and Information Security Directive 2 (NIS 2:

Content

A) Setting the scene:

Why NIS 2

Systemic risks in relation to digitalization

➔ “cybersecurity & data protection” 🡐

B) Reaction government, regulators, organizations

C) Key high lights NIS 2

D) Impact on the IT Audit profession

forvis mazars

Impact on the IT Audit profession

What can you do now?

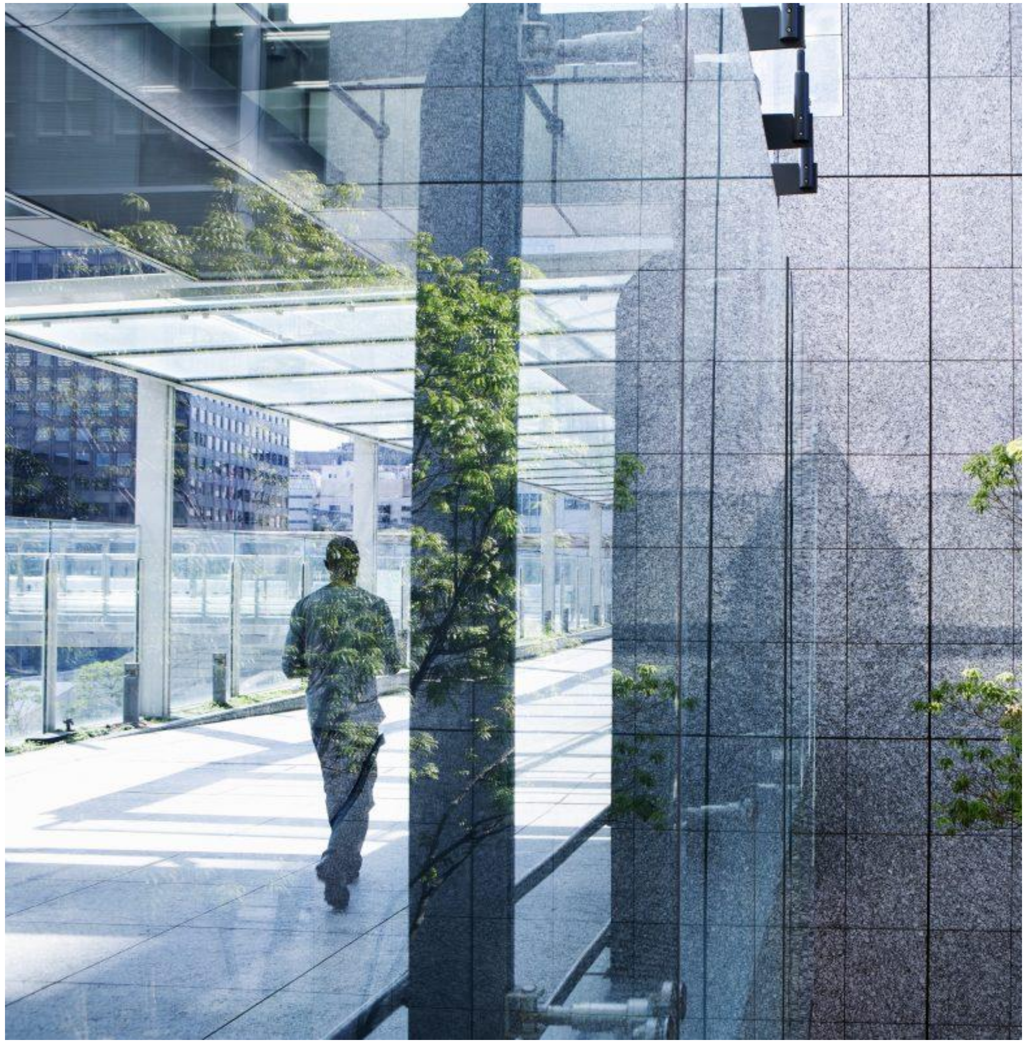
PREPARING FOR NIS 2

What to do now?

- Perform a NIS2 gap analysis.

- Use a standard like NIST CSF (2.0) / ISO27001, BIO 2, …
  - NIST CSF (2.0) chosen because of its flexibility, overlap with NIS 2 measures and general effectiveness
    - Updates based on stakeholder feedback-
    - Review of existing policies and procedures
    - Version 2.0 released in early 2024

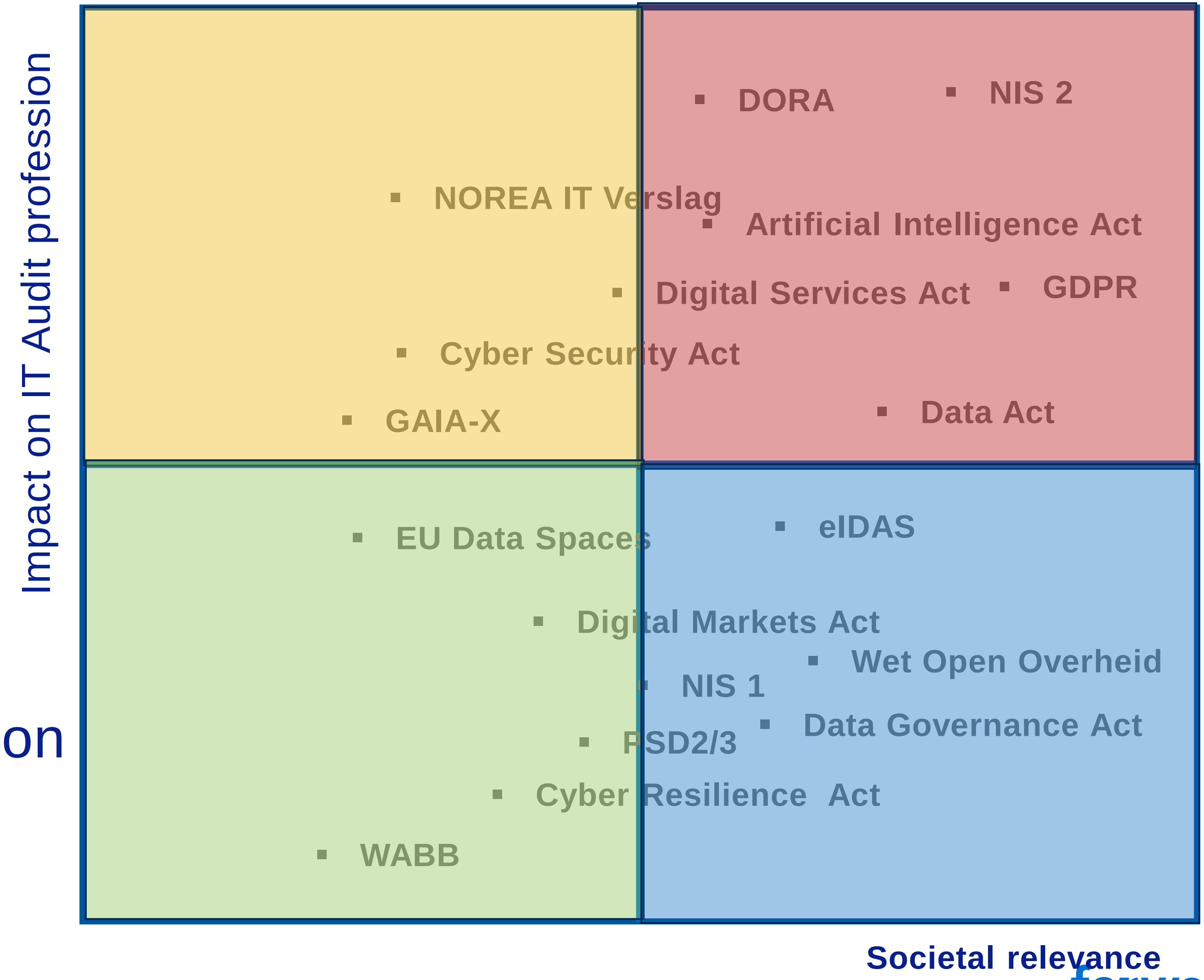
- Based on the results of the NIS2 gap analysis, draw up a roadmap with topics such as
  - ICT risk management
  - ICT incident management
  - Resilience testing
  - Cybersecurity reporting internal / external (non assurance)
  - Third party risk (assurance)



Impact on IT Audit Profession

Heathmap: Artist Impression

EU Digital Regulations



Impact on IT Audit profession

- DORA
- NIS 2
- NOREA IT Verslag
- Artificial Intelligence Act
- Digital Services Act
- GDPR
- Cyber Security Act
- Data Act
- GAIA-X
- EU Data Spaces
- eIDAS
- Digital Markets Act
- Wet Open Overheid
- NIS 1
- Data Governance Act
- PSD2/3
- Cyber Resilience Act
- WABB

Societal relevance

NIS 2 – Impact on the IT Audit profession

a) Responsibility board: increasing need for internal control, monitoring and (non financial) reporting

1) On NIS2 compliance level
2) On operational cyber security and resilience level

b) Revision of risk management to another level (incl. systemic risks and ecosystems, ➔ public interest)

c) Architecture and digital supply chain part of risk management

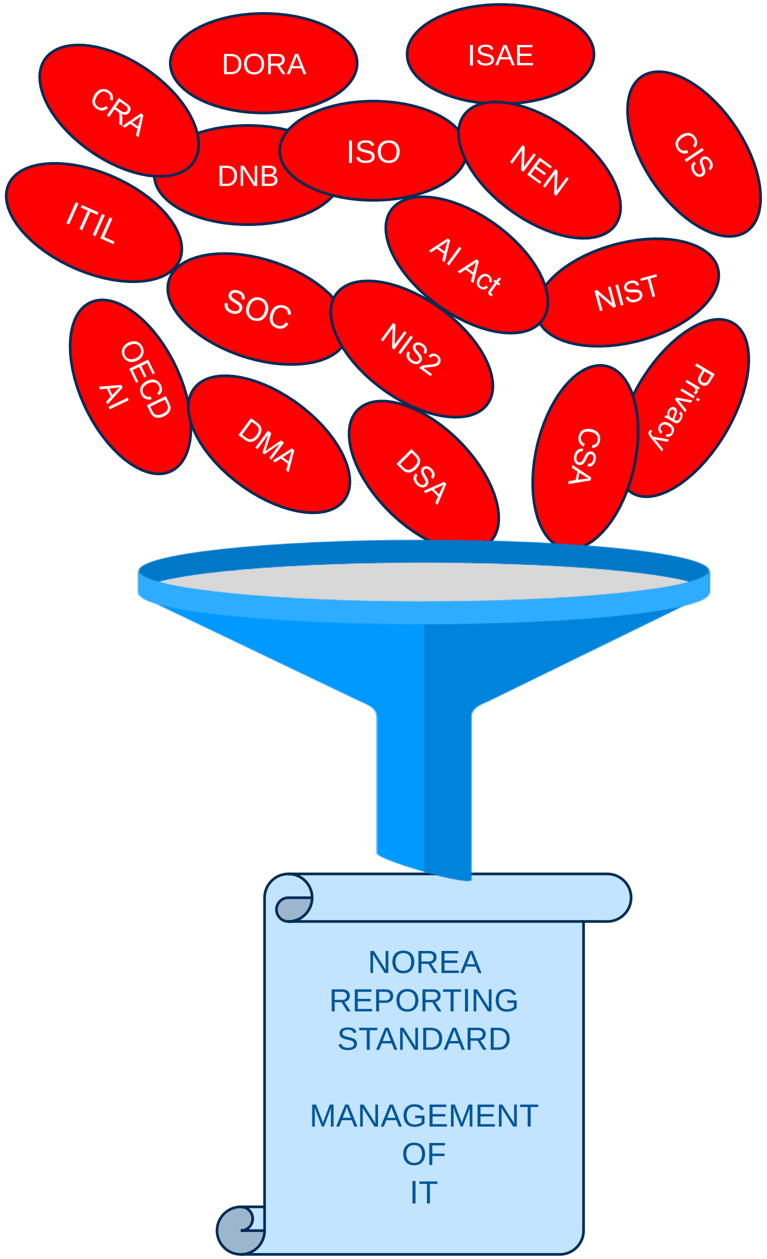
d) Digital supply chain: increasing demand for third party reporting on a “non financial” reporting level”

➔ **More cybersecurity / IT management reporting in the public domain**

e) More frequent change in cyber security resilience guidance and controls as a result of knowledge sharing by ENISA and other information sharing institutes

f) Increasing demand for certification, like ISO27001, BIO 2, TISAX, SeknumCloud, etc. and expect Increasing demand for “product certifications”

NOREA Reporting Initiative on IT management

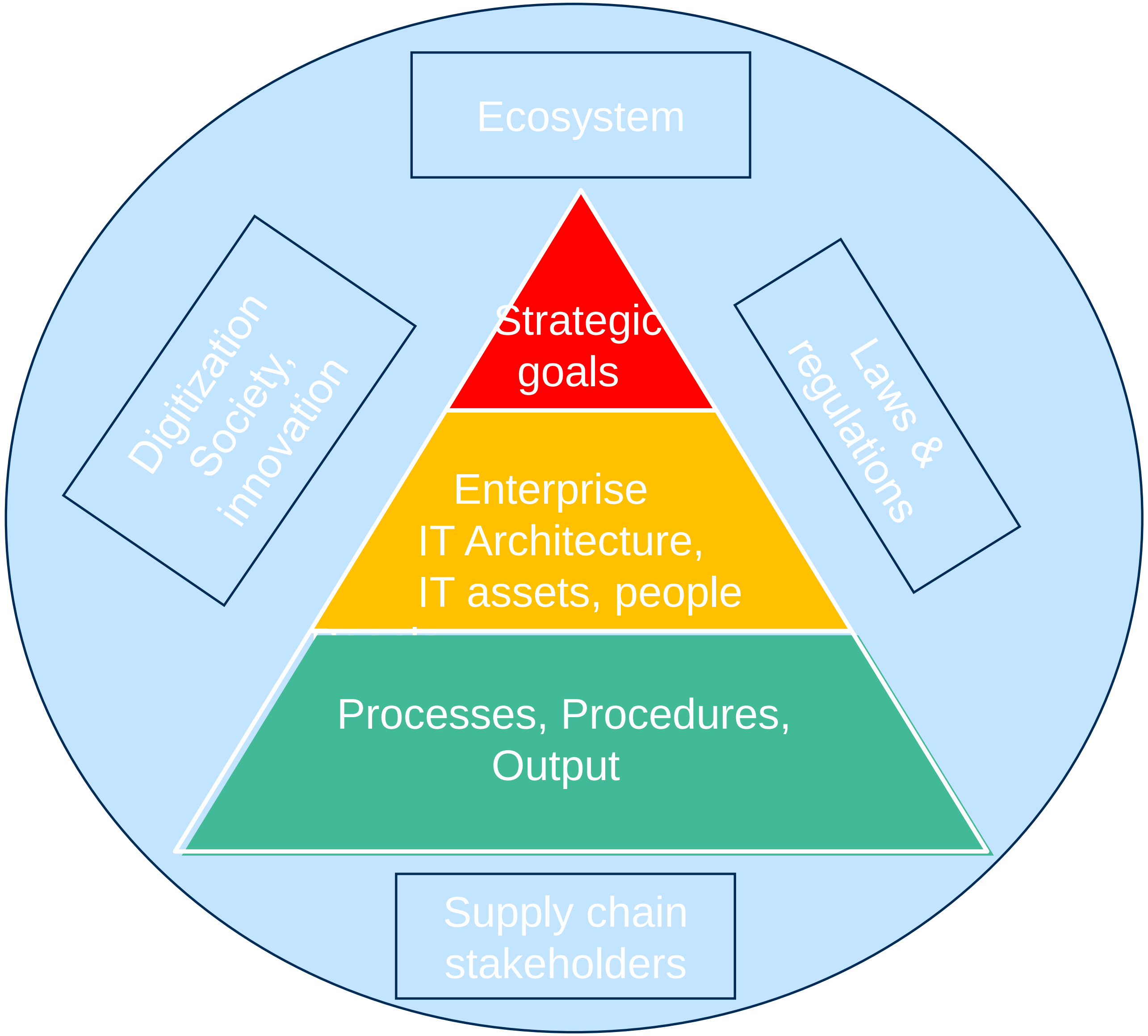


NOREA REPORTING STANDARD

MANAGEMENT OF IT

Managing internal & external reporting on digital risks

Background and conception of the NOREA Reporting Initiative



➔ The content of such report on the management of IT focuses on the measures taken to ensure that an organization has organized its IT in such a controlled manner that it contributes to its strategic goals;

➔ Identifying and managing the related risks (material topics)

➔ taking into account: constraints, opportunities, internal and external IT innovations, compliance and public interests

Background and conception of the NOREA Reporting Initiative

. This reporting initiative covers the following **likely material topics**:

- **Digital Innovation and Transformation;**
- **Data Governance & Ethics;**
- **Outsourcing;**
- **Cybersecurity;**
- **IT Continuity Management;**
- **Privacy.**

This reporting standard pays specific attention to elements that are crucial for an organization and its stakeholders including customers, suppliers, employees and other workers, regulators, investors and society.

Enkele bronnen:

- NCSC, Info sheet NIS2 verplichtingen: Zorgplicht
- Digital Trust Center (DTC), Hoe maak je een risicoanalyse?
- Rijksdienst Digitale Infrastructuur (RDI), NIS Zelfevaluatie NL, regelhulp.
- Stand van zaken invoering NIS 2, Kamerbrief 31 Januari 2024: 17 Oktober 2024 wordt niet gehaald
- NIS 2 – richtlijn informatiebrochure, Rijksoverheid, Juli 2024

Questions?