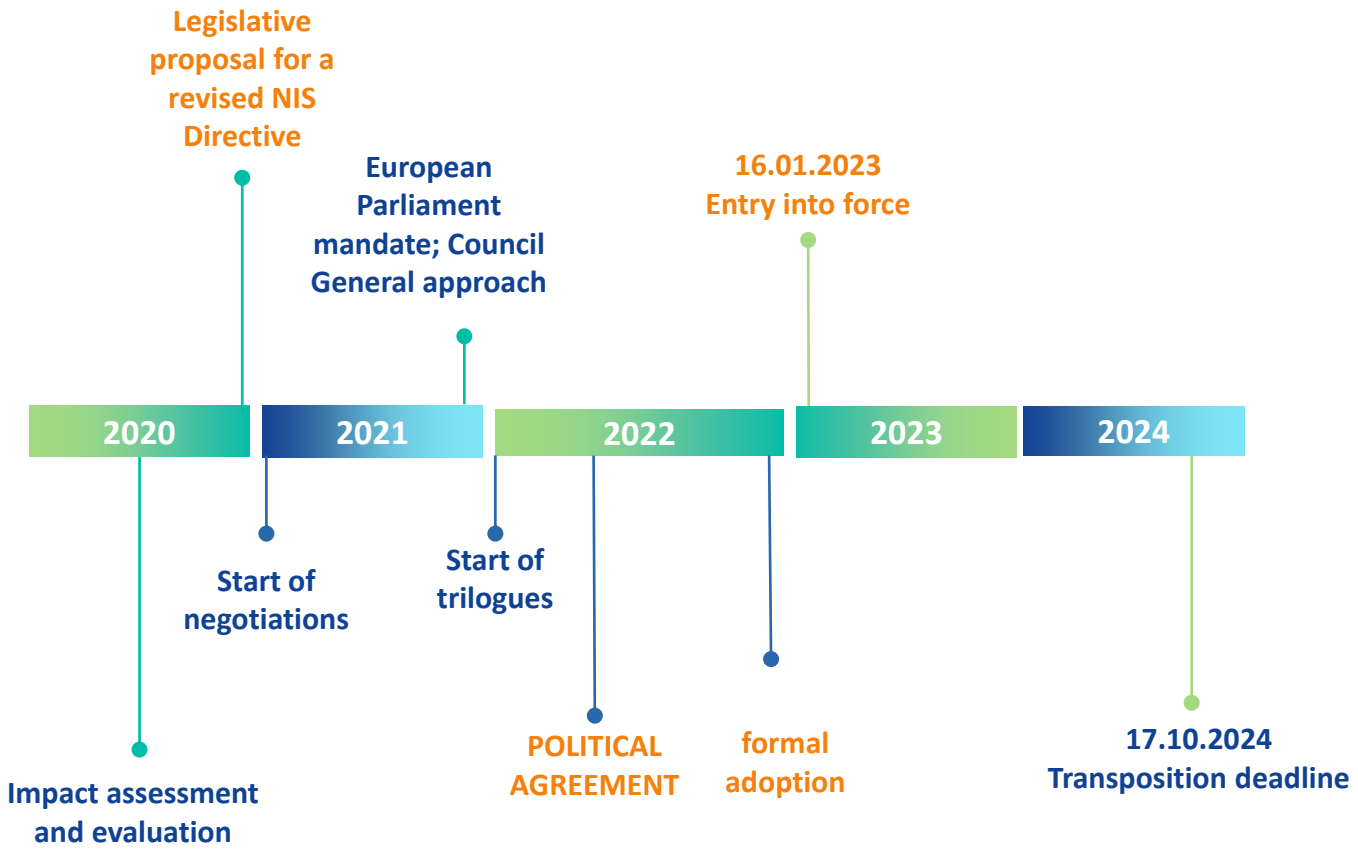
9 TRUST SERVICES AND EID FORUM
Update on NIS2 Security Measures for TSPs, whole NIS2 ecosystem

Vinzenz Heussler

Policy Officer

DG CNECT Unit H2

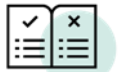
Timeline of the NIS 2 Directive



European Commission

NIS2: Three main pillars

MEMBER STATE CAPABILITIES



National authorities

CSIRTs

National strategies

CVD frameworks

Crisis management frameworks

RISK MANAGEMENT & REPORTING

Accountability for top management

Cybersecurity risk management measures

Reporting obligations

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability database

Peer-reviews

Biennial ENISA cybersecurity report

European Commission

1

SCOPE

European Commission

Entities in scope

- Principle rule: Entities in scope are
  - public or private entities
  - of a type referred to in Annex I or II
  - which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article,
  - and which provide their services or carry out their activities within the Union.

Which sectors are covered?

Annex I	Annex II
Energy (electricity, district heating, oil (incl. central oil stocktaking entities), gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	Research
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, content delivery networks, providers of electronic communications networks & publicly available electronic communications services, trust service providers,)	
ICT Service management	* Red = new in NIS2
Public administration entities	
Space	

Entities in scope regardless of their size

- Some entities are in scope regardless of their size, e.g.
  - Providers of public electronic communications networks or of publicly available electronic communications services
  - **Trust service providers**
  - TLD name registries and DNS service providers
  - Public administration entities
  - Entities identified as critical according to Directive (EU) 2022/2557 (CER Directive)
  - Et alia (Art 2(2)(b)-(e)

Essential entities

- **Essential entities**
  - Entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises
  - **Qualified trust service providers** and TLD name registries as well as DNS service providers, **regardless of their size**
  - Providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises
  - Public administration entities
  - Any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities
  - Entities identified as critical entities under Directive (EU) 2022/2557 (CER Directive)
  - If the Member State so provides, operators of essential services under NIS1
- **Important entities**
  - Entities which do not qualify as essential entities

Two regulatory regimes

	Essential entities	Important entities
Security requirements	Risk-based cybersecurity risk-management obligations, including accountability of top management	
Reporting obligations	Significant incidents	
Supervision	Ex-ante + ex-post	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines. Only for essential entities*: ultima ratio* possibility to suspend authorisation or impose temporary ban on managerial duties	
Jurisdiction	General rule: MS where the entities are established Exception: providers of electronic communications networks & publicly available electronic communications services: MS where they provide services; Certain digital infrastructures and digital providers – main establishment in the EU	

2

RISK MANAGEMENT

European Commission

More harmonised security requirements

- **Accountability for top management**
  - Management bodies shall approve the cybersecurity risk-management measures, oversee its implementation and can be held liable for infringements
  - Management bodies are required to follow training (gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity)

- **Cybersecurity risk-management measures**
  - Risk-based approach
  - All-hazards approach
  - Minimum set of measures

More harmonised security requirements

- Appropriate and proportionate technical, operational and organisational measures to manage the risks
- Prevent or minimise the impact of incidents on recipients of their services and on other services
- Scope: Network and information systems which entities use for their operations or for the provision of their services
- Proportionality: degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact

Minimum set of security requirements

- Policies on **risk analysis** and information system security
- **Incident handling**
- **Business continuity**, such as backup management and disaster recovery, and **crisis management**
- **Supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- Security in network and information systems **acquisition, development and maintenance**, including vulnerability handling and disclosure
- Policies and procedures to assess the **effectiveness** of cybersecurity risk-management measures
- Basic **cyber hygiene** practices and cybersecurity **training**
- Policies and procedures regarding the use of **cryptography** and, where appropriate, **encryption**
- **Human resources** security, **access control** policies and **asset management**
- Use of **MFA** or continuous **authentication solutions**, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

3

INCIDENT REPORTING

European Commission

More harmonised incident reporting obligations

- Entities have to report significant incidents to the CSIRT or competent authority
- Multiple-stage approach:
    1. Early warning, without undue delay and at the latest within 24 hours of becoming aware of the significant incident,
    2. Incident notification, without undue delay and at the latest within 72 hours
    3. Final report, no later than one month.
- TSP shall, with regard to significant incidents that have an impact on the provision of its trust services, notify without undue delay and in any event within 24 hours of becoming aware of the significant incident.

Significant incidents

- An incident shall be considered to be significant if:
  - it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
  - it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage

4

IMPLEMENTING ACTS

European Commission

Implementing Acts

- Certain entities should be subject to a high degree of harmonisation at EU level due to their cross-border nature.
- The implementation of cybersecurity risk-management measures and reporting obligations with regard to those entities should therefore be facilitated by an implementing act.
- NIS Cooperation Group has the task to exchange advice and cooperate with the Commission on draft delegated or implementing acts adopted pursuant to NIS2.

Implementing Acts

Cybersecurity risk-management measures	Reporting obligations
Legal basis	
Article 21 (5) NIS2	Article 23 (11) NIS2
Obligatory for Commission to adopt	
Yes	Yes
Deadline	
17 October 2024	17 October 2024
Subject matter	
Technical and methodological requirements of the cybersecurity risk-management measures referred to in Article 21(2) NIS2	Specifying the cases in which an incident shall be considered to be significant.
Scope and addressees as required by NIS2	
- Certain entities providing cross-border digital services (e.g. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, CDN, MSP, MSSP, etc.)	- Certain entities providing cross-border digital services (e.g. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, CDN, MSP, MSSP, etc.)

Thank you!

European Commission