
NIS 2 Directive

**DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022**

on measures for a high common level of cybersecurity across the Union



Article 41: Local laws by 17.10.2024,
Applicable 18.10.2024



License

- This Presentation © 2024 by Cyberismo is licensed under Creative Commons Attribution-ShareAlike 4.0 International.
- To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0/>
- The [Cyberismo trademark policy](#) applies to this presentation.
- If you have feedback or other comments, please contact us at info@cyberismo.com

Agenda

- Who is within the NIS2 scope
- Main requirement areas
 - Top Management responsibilities
 - Cybersecurity risk management
 - Cybersecurity risk management measures
 - Incident reporting
 - Registry of entities
- Supervision and enforcement
- Timeline

Note: This presentation is based on original NIS2 directive and law proposal in Finland (kyberturvallisuuslaki). Other EU countries might introduce additional requirements in their local laws.

Scope and essential/important entities

- Article 2: Public and private entities of defined types (Annex I and II) that qualify as medium or exceed ceiling for medium-sized enterprises
 - Medium: 50 employees OR annual turnover & balance over 10 M€
 - Bigger: 250 employees OR annual turnover > 50M€ and balance > 43 M€
 - Certain entities regardless of their size (Article 2.2-2.4)
- Essential entities: Bigger entities from Annex I and separately specified entities (Article 3.1 b-g, mainly already in NIS1 scope)
- Important entities: Entities defined in Annex I & II that are not essential

Annex I: Sectors of High Criticality



Energy



Transport



Banking



Financial market
infrastructures



Health



Drinking water



Waste water



Digital
infrastructure



ICT service
management (B2B)

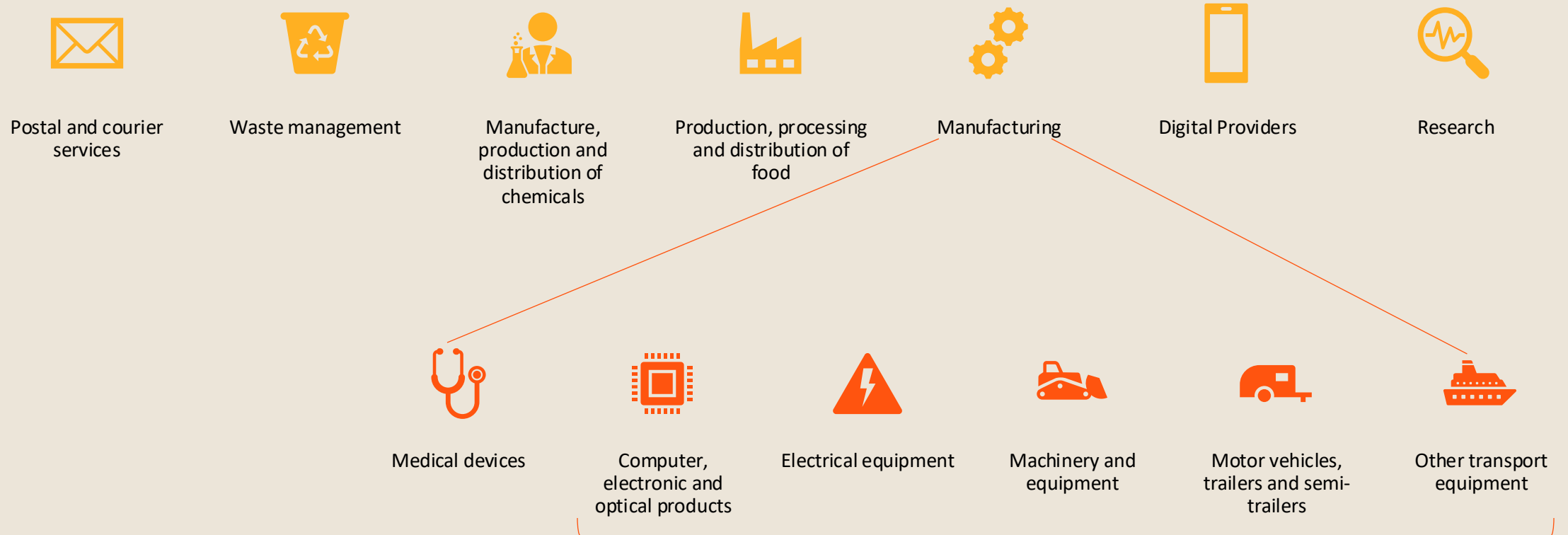


Public
administration



Space

Annex II: Other Critical Sectors



Divisions 26-30 on pages 67-69 of [NACE Rev. 2](#)

Main requirement areas

Top management responsibilities

Cybersecurity risk management

Cybersecurity risk management measures

Incident reporting

Submit information for registry of entities

Article 20: Governance (Management responsibilities)

- Management bodies **approve the cybersecurity risk management measures** taken in order to comply with Article 21
- Management bodies **oversee implementation** of risk management measures
- Management bodies of *essential entities* **can be held responsible** for infringements of Article 21
- Management bodies **are required to gain sufficient knowledge and skills** to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the provided services

Article 21: Cybersecurity risk-management

- Document objectives, procedures, and responsibilities of cybersecurity risk management
- Utilize *all-hazards approach* to **protect network and information systems and the physical environment of those systems** from incidents
- Implement technical, operational and organizational measures to manage the risks posed to the security of network and information systems
 - Prevent or minimize the impact of incidents on recipients of their services and on other services
 - Ensure level of security of network and information systems is appropriate and proportionate to the risks posed
 - Ensure measures are proportionate to degree of exposure to risk, entity's size, likelihood of occurrence of incidents and severity, including societal and economic impact

Article 21.2: Cybersecurity risk-management measures

- Policies on risk analysis and effectiveness evaluation (a, f)
- Policies network and information system security (a)
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure (e)
- Supply chain security (d) (overall quality and resilience, risk management, specific vulnerabilities, cybersecurity practices)
- Asset management (i)
- Human resource security and cybersecurity training (g, i)
- Access controls and authentication (MFA, continuous authentication) policies (i, j)
- Policies for the use of cryptography and use of secured communication systems (h, j)
- Incident handling and business continuity (b, c)
- Basic cyber hygiene practices (g)
- Physical security for networks and information systems, ensuring sufficient resources (FI/HE)

Article 23: Reporting obligations

- Notify authorities of any incident that has a significant impact on the provision of their services (significant incident)
 - 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.
- Early warning within 24 hours of becoming aware
- Incident notification without undue delay (within 72 hours)
- Intermediate reports upon request
- Final report (or progress report) not later than one month after incident notification (handling of the incident)
 - Detailed description incl. severity and impact, type of threat or root cause, applied and ongoing mitigation measures, cross-border impact of the incident

Article 27: Registry of entities

Entities need to supply the following information to competent authorities:

- (a) the name of the entity;
- (b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;
- (c) the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3);
- (d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3);
- (e) the Member States where the entity provides services; and
- (f) the entity's IP ranges.

Summary	Reference	Topics
Cybersecurity Risk Governance	Article 20	Management responsibilities, cybersecurity risk management knowledge and skills, approving and supervising the approach
Cybersecurity Risk Management approach	Article 21	Scope and coverage, Identification using all-hazards approach, Assessment, Treatment (technical, operational and organizational), Monitoring (reporting, effectiveness)
Cybersecurity Risk Management measures (at minimum)	Article 21.2	Network and information system security, system acquisition, development and maintenance, vulnerability handling and disclosure, supply chain security , asset management, human resource security and cybersecurity training, access controls and authentication, use of cryptography, use of secured communication systems, incident handling and business continuity, basic cyber hygiene practices, physical security, effectiveness evaluation
Incident Reporting practises	Article 23	Notification responsibilities, channels, content and strict reporting deadlines

Inspections, audits, warnings, instructions, fines

- Article 32: Supervisory tasks for essential entities – e.g., on-site inspections, random checks, regular security audits, security scans, ...
- Article 33: **Ex post** supervisory tasks for important entities – e.g., on-site inspections and off-site ex post supervision, targeted security audits, ...
- Article 34: Administrative fines for infringing Article 21 or 23
 - Essential entities: 10 000 0000€ or 2 % of the total worldwide annual turnover
 - Important entities: 7 000 000€ or 1.4 % of the total worldwide annual turnover
- Article 37: When multiple member states are involved, the competent authorities of the Member States concerned shall cooperate.
- **Note:** At least in Finland administrative fines can be given also if company information is not submitted to competent authorities

Timeline

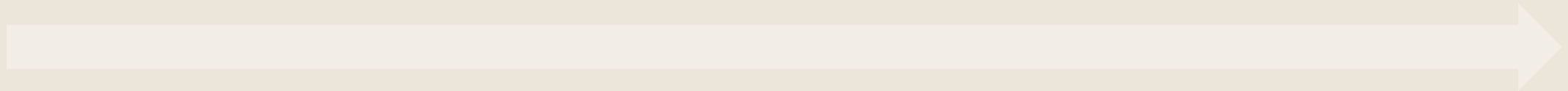
NIS2 law preparations
NIS2 projects in organizations



Oct 18, 2024
Requirements apply



Dec 31, 2024
Entities must submit
their info to authorities (FIN)



Continuous cybersecurity management in organisations

Executive summary

Top management responsibilities:

1. Approve cybersecurity risk management approach
2. Oversee implementation of cybersecurity risk management measures
3. Gain sufficient knowledge and skills to complete the above mentioned tasks

Tips for avoiding administrative fines

Adopt holistic cybersecurity risk management approach

Implement required risk management measures

Report significant incidents in timely manner

Submit company info for registry on entities

CYBERISMO!



> Make a difference in **cybersecurity**.