EDIH TRAKIA

Cyber security act and certification schema

Digital Innovation Hub Trakia

European Digital Innovation Hubs Network

European Commission

CYBER
4 ALL STAR

Cyber security act

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee (1),
Having regard to the opinion of the Committee of the Regions (2),
Acting in accordance with the ordinary legislative procedure (3)

Whereas: 110 reasons

69

Articles
+
1 Annex

Cyber security act

5 logical groups building consistent logic

1. Foundation and Principles

Establishes the fundamental goals, definitions, and guiding principles for the regulation, laying the groundwork for a cohesive and robust cybersecurity strategy.

2. Governance and Structure

Outlines the governance structure, defining the roles and responsibilities of ENISA, its management board, executive director, and the necessary transparency and integrity measures.

Cyber security act

5 logical groups building consistent logic

3. Operational Framework

Details the operational framework including work programmes, legal and administrative provisions necessary for ENISA to function effectively and achieve its objectives.

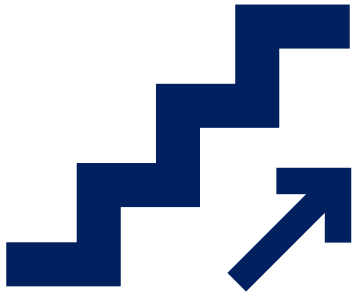
4. Cybersecurity Certification Framework

Sets up the certification framework to enhance cybersecurity across the EU, detailing the procedures, bodies involved, and coordination mechanisms between national and European levels..

Cyber security act

5 logical groups building consistent logic

5. Implementation and Compliance
Ensures the regulation is effectively implemented and complied with through penalties, evaluation, and transitional provisions to ensure a smooth transition and continuous improvement in cybersecurity.



CYBER
4 ALL STAR

Working together is the better way

Cyber security act

Details you need to focus on

1. **Foundation and Principles**

Establishment and Objectives:

- **Article 1:** Subject Matter and Scope
- **Article 2:** Definitions

Core Principles:

- **Article 5:** General Principles

Articles 3,4 and 6 considers ENISA

Cyber security act

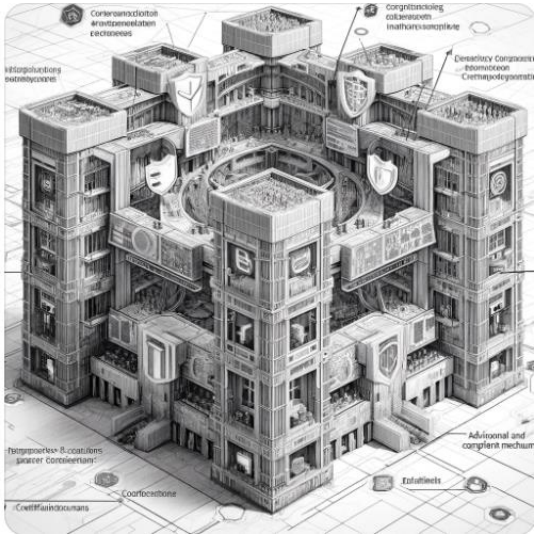
4. **Cybersecurity Certification Framework**

•**Framework Establishment:**

Article 46: European Cybersecurity Certification Framework
Article 47: Union Rolling Work Programme

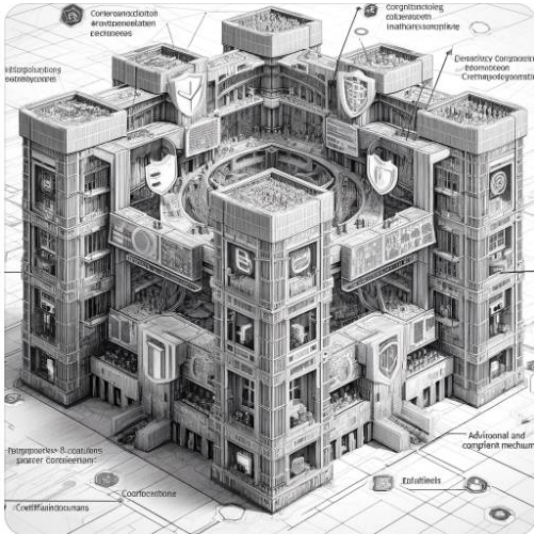
•**Certification Procedures and Bodies:**

Articles 48-56: Certification Procedures and Requirements
Article 60: Conformity Assessment Bodies
Article 61: Notification Procedures



Cyber security act

4. **Cybersecurity Certification Framework**



•**National and European Coordination:**
Article 57: National Certification Schemes
Article 58: National Cybersecurity Certification Authorities
Article 59: Peer Review

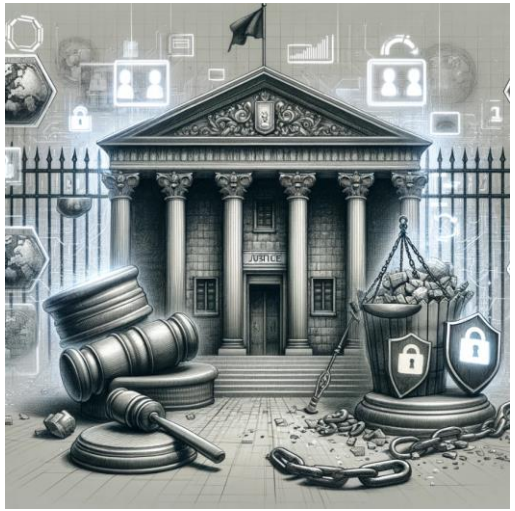
•**Advisory and Complaint Mechanisms:**
Article 62: European Cybersecurity Certification Group
Article 63: Right to Lodge a Complaint
Article 64: Right to an Effective Judicial Remedy

Cyber security act

Details you need to focus on

5. Implementation and Compliance

- **Penalties and Compliance:**
  - **Article 65:** Penalties
- **Evaluation and Review:**
  - **Articles 66-67:** Committee Procedure and Evaluation
- **Transitional Provisions:**
  - **Article 68:** Repeal and Succession
  - **Article 69:** Entry into Force



WARNING

Next two slides are breaking all good practices of presentation styling, but you need this summary!

Aspects under certification

1. ICT Products, Services, and Processes

ICT Products:

- Hardware devices such as routers, firewalls, computers, and IoT devices.
- Software applications including operating systems, databases, and mobile apps.
- Integrated systems that combine hardware and software components.

ICT Services:

- Cloud computing services including IaaS, PaaS, and SaaS.
- Digital service providers such as online marketplaces, search engines, and social media platforms.
- Managed security services like threat detection, incident response, and vulnerability management.

ICT Processes:

- Software development and deployment processes.
- Data processing and storage operations.
- Network and information system management procedures.

Aspects under certification

2. Certification Schemes and Assurance Levels

•European Cybersecurity Certification Schemes:

- Specific certification schemes tailored for different categories of ICT products, services, and processes.
- Schemes may be based on existing national and international standards and frameworks.

•Assurance Levels:

- **Basic Assurance Level:**
  - Suitable for products and services with low complexity and low risk.
  - Self-assessment by manufacturers or providers may be sufficient.
- **Substantial Assurance Level:**
  - Suitable for products and services with moderate risk.
  - Requires verification of compliance with technical documentation and security functionalities.
- **High Assurance Level:**
  - Suitable for high-risk products and services.
  - Involves rigorous evaluation, including efficiency testing against sophisticated cyberattacks.

4 aspects are hidden in the comments. Ask for the PPTX presentation

Recap

Local schemas will be replaced by single EU one – EUCC

Your primary source for schemas is :
https://certification.enisa.europa.eu/index_en

Producers will use one schema for single market og 500 000 000 consumers

Consumers will have the possibility easy to compare products by security

Existing Schemas

1. **European Cybersecurity Certification Scheme on Common Criteria (EUCC)** The EUCC is the first scheme adopted under the EU cybersecurity framework. It certifies ICT products like hardware and software based on the Common Criteria (ISO/IEC 15408 and ISO/IEC 18045). This voluntary scheme helps suppliers prove their products meet high cybersecurity standards, enhancing trust across the EU market
2. **European Certification Scheme for Cloud Services (EUCS)** The EUCS scheme, in development, focuses on cloud services, ensuring security in data protection, privacy, and service reliability. It aims to harmonize cloud service certifications across the EU (since December 22, 2020)
3. **European Certification Scheme for 5G (EU5G)** The EU5G scheme addresses the cybersecurity needs of 5G networks and devices. Developed in phases, it ensures the security of critical next-generation mobile networks (since EUCC Implementing Act) on January 31, 2024)

ENISA is exploring certification schemes for emerging technologies, such as AI, to address potential cybersecurity needs once regulatory frameworks are established (EU Cyber Cert) (ENISA).

CYBER
4 ALL STAR

Contact us on time

edihtrakia.org

yasen.tanev@edihtrakia.org

Пловдив 4000, ул. Белград №6. етаж 1