



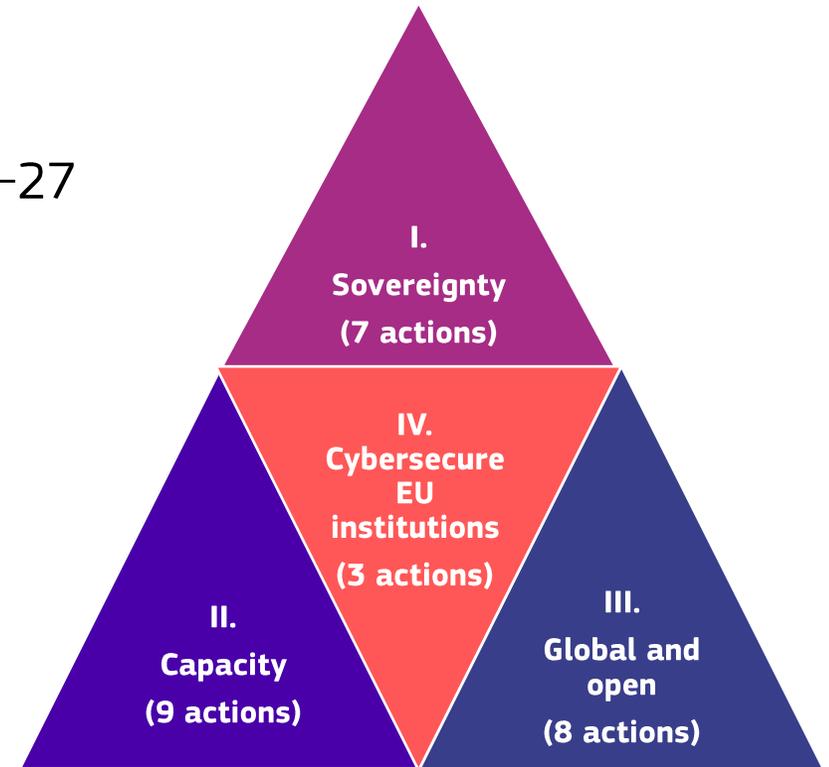
Standards for EU cybersecurity policy

*17 October 2023
presentation for HSBooster*

EU's cybersecurity priorities

The EU's cybersecurity strategy for the Digital Decade

- 27 strategic initiatives/actions
- Smart digital investment: up to €4.5bn for cybersecurity 2021-27 (EU + MS + Industry)
- New regulation (e.g. NIS 2.0, CRA, EU Cyber solidarity act,)
- New policies (Cyber Crisis management, Cybersecurity Skills Academy)
- Comprehensive
 - internal market
 - law enforcement
 - diplomacy
 - defence



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

MEMBER STATE CAPABILITIES

National authorities
National strategies

Coordinated Vulnerability Disclosure (CVD) frameworks

Crisis management frameworks

RISK MANAGEMENT & REPORTING

Large and medium sized entities in 18 critical sectors

Accountability of top management for non-compliance

Streamlined **cybersecurity risk management measures***

Streamlined **incident reporting****

COOPERATION AND INFO EXCHANGE

Cooperation Group
CSIRTs network

CyCLONe

CVD and European vulnerability database

Peer-reviews

Biennial ENISA cybersecurity report

* Cybersecurity risk management measures:

e.g. risk analysis, information security policy, incident handling, business continuity, HR, network and supply chain security, cryptography, MFA, etc.

** Incident reporting:

- *Reporting of significant incidents*
- *multiple-stage approach (24h early warning, 72h notification, 1 month final report)*
- *States to inform each other and ENISA of cross-border incidents*

Next steps: Transposition by Member States until **October 2024** ; adoption of implementing acts by the Commission

Cybersecurity Act – Certification Framework

Objectives:



Increasing the **trustworthiness** in ICT products, services and processes placed in the digital Single Market



Enabling **informed decisions** about how the supply side matches cybersecurity demand



Minimising varying degrees of cyber attack **risks** by coherent security **controls** that **undergo a consistent and objective assessment** with **voluntary certification**

Certification Initiatives:

EUCC

- Common Criteria-based certification of ICT products

EU5G

- Certification of telecommunication ICT processes (NESAS, eUICC, SAS)

Managed Services Providers

- Early stage of discussion with co-legislators

EUCS

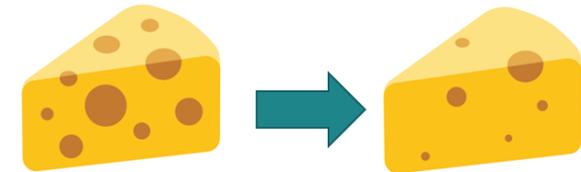
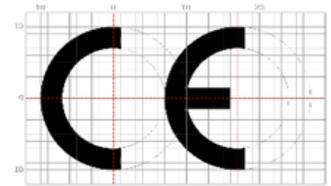
- Certification of ICT Cloud services (SaaS, PaaS, IaaS)

Cyber Resilience Act proposal

Timeline: Proposal on 15 Sept. 2022; Council and European Parliament agreed positions on 19 July 2023.

Main elements :

- **Cybersecurity rules** for the placing on the market of **hardware and software products**
- Based on **New Legislative Framework** (well-established EU product-related legislative setting)
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the **life cycle** (5 years)
- **“Harmonised” standards** to follow (building on existing international, European and national standards)
- **Conformity assessment** – differentiated by level of risk, and **Market surveillance** and enforcement
- **International impact:** role of international standards; possibility for **Mutual Recognition Agreements (MRAs)**



Horizon Europe 2023-2024

- **HORIZON-CL3-2022-CS-01**

Budget EUR 67.30 M – 4 topics:

- 119 evaluated proposals (78 ranked proposals – 14 selected)

- **HORIZON-CL3-2023-CS-01** (*ongoing – deadline 23 Nov 2023*)

Budget EUR 58.70 M – 3 topics:

1. Secure Computing Continuum
2. Privacy-preserving and identity management technologies
3. Security of robust AI systems

- **HORIZON-CL3-2024-CS-01** (*upcoming June 2024*)

Budget EUR 60.40 M – 2 topics:

1. Security in software and hardware development and assessment
2. Post-quantum cryptography transition

Digital Europe Programme 2023-2024

- **DIGITAL-ECCC-2022-CYBER-03**

Budget EUR 176.50 M – 7 topics:

1. Resilience
2. Security Operation Centres (SOCs)
3. 5G
4. Uptake
5. Network of National Coordination Centres (NCC)
6. NIS Directive
7. Testing and Certification Capabilities

- **DIGITAL-ECCC-2022-CYBER-B-03**

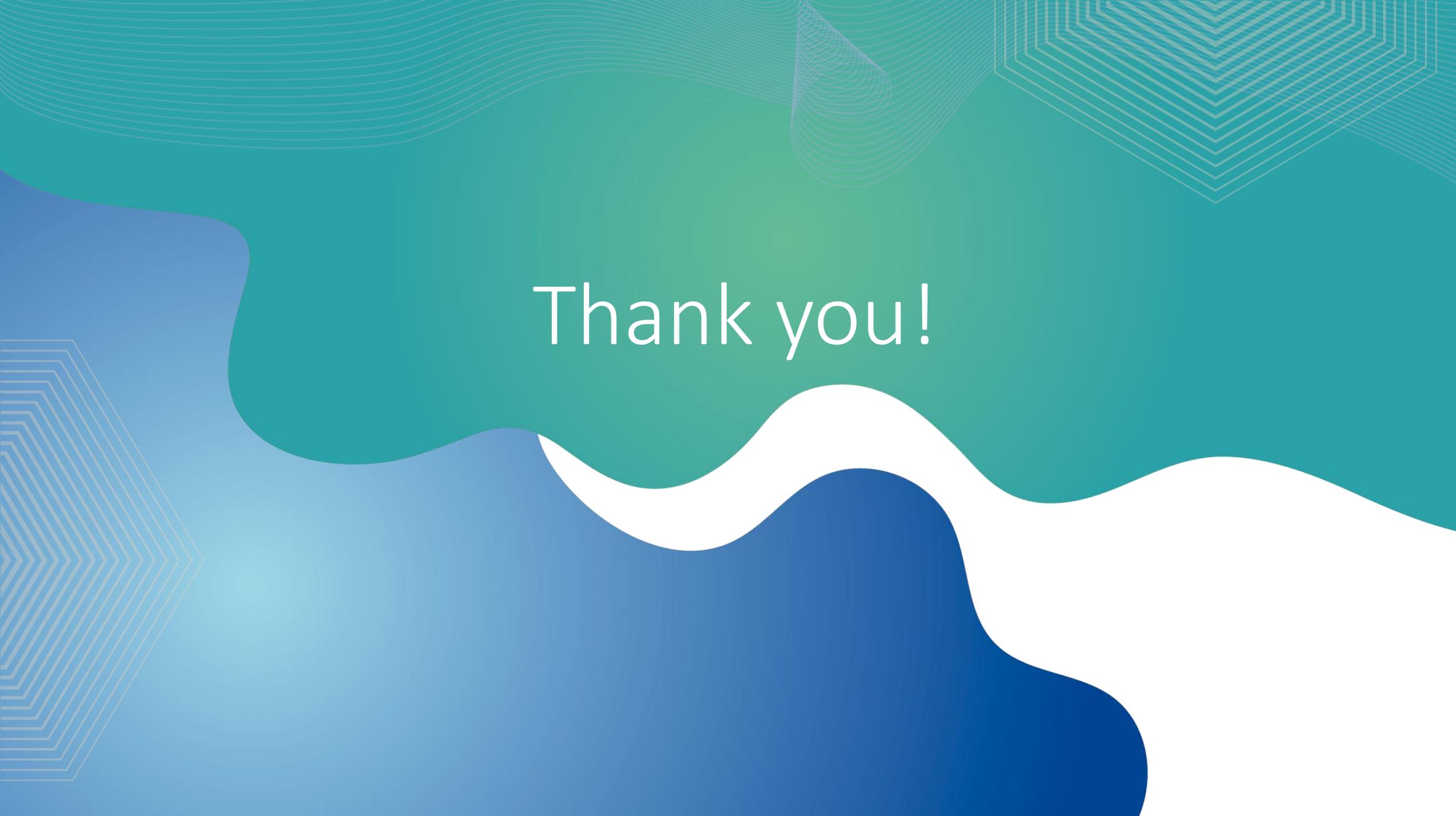
Budget EUR 36.48 M – 3 topics:

1. Resilience
2. Security Operation Centres (SOCs)
3. Uptake

- **DIGITAL-ECCC-2023-DEPLOY-CYBER-04**

Budget EUR 71.00 M – 4 topics:

1. Support and Mutual Assistance
2. Civil Defence
3. Standardisation
4. EU Legislation



Thank you!