Cybersecurity Act 2 Simulation: Commission Proposal

The Pirate Academy was made possible by the Greens/EFA group in the European Parliament.

Teaching text. This is a strongly simplified version of the real proposal COM(2026) 11, which has 122 articles and two annexes. The wording, the figures and the structure are fictionalised for the simulation. The Commission's choices below are its opening position: every article can be amended, deleted or rewritten, and new articles can be added.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the security of critical technology supply chains in the Union (Cybersecurity Act 2)

Procedure 2026/0011(COD), teaching version

Recitals

Whereas:

(1) Digital infrastructure now underpins the Union's economy, its essential public services and the functioning of its democratic institutions. Dependence on technology supplied by undertakings subject to the jurisdiction or effective control of third countries whose strategic interests may diverge from those of the Union creates a structural vulnerability that hostile actors could exploit.

(2) Divergent national responses fragment the internal market and weaken collective resilience. A coordinated Union approach offers a higher and more consistent level of protection.

(3) Measures taken under this Regulation should remain necessary, proportionate and consistent with the Charter of Fundamental Rights of the European Union, including the rights to data protection, to property and to good administration.

(4) Restrictions on specific vendors interfere with commercial freedoms and may affect the continuity of essential services. They should therefore rest on a transparent, evidence-based procedure with adequate guarantees for the undertakings concerned.

(5) The European Union Agency for Cybersecurity (ENISA) should be entrusted with coordinating technical assessment and certification, with resources commensurate with those tasks.

Chapter I: General provisions

Article 1: Subject matter

This Regulation establishes a Union framework to:

(a) identify critical technologies and their supply chains;

(b) designate high-risk vendors and phase out their technology;

(c) provide for Union-level security certification;

(d) define the tasks of ENISA under this Regulation;

(e) set out penalties.

Article 2: Definitions

For the purposes of this Regulation:

(1) “critical technology” means hardware, software or a service whose compromise would cause significant disruption to essential services;

(2) “high-risk vendor” means an undertaking designated under Article 6;

(3) “operator” means an entity providing an essential service listed in Annex I that relies on critical technology;

(4) “non-technical risk factor” means a risk arising from the ownership, governance or country of jurisdiction of a vendor, as distinct from the technical quality of its products.

Article 3: Scope

1. This Regulation applies to operators in the sectors listed in Annex I.

2. The Commission is empowered to amend Annex I by implementing act in order to add or remove sectors in the light of technological developments and of the risk assessments under Article 5.

Chapter II: Critical technologies and high-risk vendors

Article 4: List of critical technologies

The Commission, assisted by ENISA, shall adopt, publish and keep up to date a list of critical technology categories. It shall review the list at least every 24 months.

Article 5: Coordinated risk assessment

ENISA and the Member States shall jointly assess the supply chains of the critical technologies listed under Article 4, drawing on technical evidence and on intelligence and threat information supplied by the Member States.

Article 6: Designation of high-risk vendors

1. A vendor may be designated as a high-risk vendor where the coordinated risk assessment establishes one or more of the following:

(a) the vendor is subject to a legal or factual obligation in its country of jurisdiction that could compel it to act against the security interests of the Union or of its Member States;

(b) there is substantiated evidence that the vendor has facilitated a cyber intrusion or compromise;

(c) the vendor has a record of serious or repeated breaches of security obligations.

2. The Commission shall designate high-risk vendors by decision, after consulting the Member States.

Article 7: Phase-out of designated technology

Following designation, operators shall cease new procurement of critical technology from the vendor and shall remove or replace existing affected technology within 18 months of the designation.

Chapter III: Certification

Article 8: Union security certification

1. ENISA shall prepare European cybersecurity certification schemes for critical technologies, to be adopted by the Commission.

2. A Union certificate shall be valid throughout the Union. Where a Union certification scheme exists for a technology, it shall replace national schemes for the same technology.

Chapter IV: Procedural rights and review

Article 9: Rights of the vendor and review of designations

1. The Commission shall notify the vendor of the designation with a statement of reasons.

2. The vendor may submit observations within 15 working days of the notification.

3. The Commission may review a designation at any time. A designation remains in force until the Commission revokes it.

Chapter V: Penalties, ENISA and final provisions

Article 10: Penalties

Member States shall lay down effective, proportionate and dissuasive penalties for infringements of this Regulation. For infringements of Article 7, the maximum penalty shall be at least 7% of the total worldwide annual turnover of the operator.

Article 11: Tasks and resources of ENISA

ENISA shall carry out the tasks assigned to it under Articles 4, 5 and 8. It shall be provided with the financial and human resources necessary for those tasks.

Article 12: Implementing measures

The detailed measures under Articles 3, 4, 6 and 8 shall be adopted by the Commission.

Article 13: Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. It shall apply from 12 months after its entry into force.

Annex I: Sectors

1. Energy (electricity, gas, oil, hydrogen, district heating)

2. Transport

3. Banking and financial market infrastructure

4. Health
5. Drinking water and waste water
6. Digital infrastructure (electronic communications networks, cloud computing services, data centre services, content delivery networks)
7. Public administration
8. Space
9. Postal and courier services
10. Production, processing and distribution of food
11. Manufacturing of critical products and digital providers (online marketplaces, online search engines, social networking platforms)

Decision map

The five questions that the simulation is built around. Your team's goals are in the general factsheet.

Question	**Articles**	**What is decided**
Q1 Designation	4, 6, 12	who decides on the list of critical technologies and on designations, on what grounds, and what role the Parliament has
Q2 Phase-out	7	how fast designated technology must go, what happens to equipment already installed, and who pays
Q3 Certification and ENISA	8, 11	one Union scheme or national exceptions; what ENISA gets
Q4 Procedural rights	9	how a vendor can defend itself, and whether designations are reviewed or lapse
Q5 Scope and penalties	3, 10, Annex I	which sectors are covered and how high the penalties are