

2



26

NIS2: The 2026 Amendment Package

European Commission Proposal • Jan 20, 2026

5 CRITICAL CHANGES FOR CISOs & COMPLIANCE LEADERS

FROM FRAGMENTATION TO HARMONIZATION

CURRENT STATE



2026 PROPOSAL



🔗 **THE CATALYST:** Alignment with the proposed Cybersecurity Act 2 (CSA2).

🎯 **THE GOAL:** A Single Framework for reporting and supervision.

💡 **KEY INSIGHT:** "Clarify scope... harmonize technical measures."

1. THE END OF 'GOLD-PLATING'



THE PROBLEM:

Member States currently adding extra national rules.

THE FIX:

New ban on additional technical requirements once EU acts are adopted.

THE IMPACT:

One EU standard = One national standard.

2. Stricter Ransomware Reporting



DATA REQUIREMENT CHECKLIST

- ☐ • Attack vector & detection method
- ☒ • **Did you pay the ransom?
(Mandatory Disclosure)**
- ☐ • Payment amount & method
- ☐ • Crypto-wallet / recipient details

3. The 'Cyber-Posture' Certificate



Concept:

Entity-level certification under CSA2.

Benefit:

Replaces repetitive national security audits.

Efficiency:

Valid EU certificate stops duplicate supervisory requests.

4. Supervision & Scope Updates



'SUPERVISION FRAMEWORK'

ENISA Role: Operational supervision for cross-border entities. Facilitates joint actions.

'CROSS-BORDER COORDINATION: ACTIVE'



'SCOPE REFINEMENT'

New Category: 'Small Mid-Caps' (<750 employees, <€150M turnover) added as Important Entities.

Refinement: Chemical distribution removed; DNS providers subject to size thresholds.

'ENTITY THRESHOLD: <750 EMPLOYEES'

'EXCLUSION: CHEMICAL DISTRIBUTION'

The 2026 Snapshot

- **Harmonization:** Ban on national 'gold-plating' of technical rules.
- **Ransomware:** Mandatory reporting of payments & crypto-wallets.
- **Certification:** EU-wide 'Cyber-Posture' certificate limits audits.
- **Supervision:** ENISA gains operational cross-border powers.
- **Scope:** 'Small Mid-Caps' added to Important Entities.