Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

HOT NEWS IN EUROPEAN LEGISLATION REGARDING CYBER SECUIRTY

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

About the Lecturer

•Lead Auditor for Management Systems (information security, services, quality, and more).

•Chairman of the **Institute for Artificial Intelligence**.

•Deputy Manager of the **Bulgarian Union of Standardizers**.

•Active participant in numerous European and national cybersecurity projects.

•Assistant Professor at **UniBIT**:

- Cybersecurity Standards
- Cybersecurity Management
- Cryptography
- Zero Trust Architectures

A Winter of Legislative Transformation

Strategic Shift: From Expansion to Consolidation & Precision

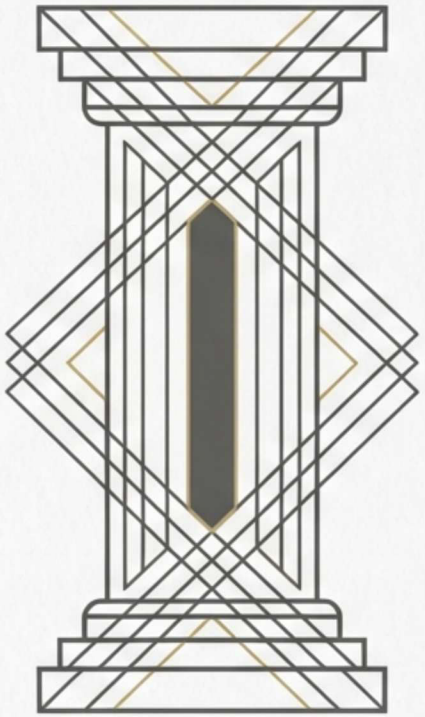
The Digital Omnibus: Clearing the Regulatory Clutter

Proposal 2025/0360 (19.11.2025)

1. **Core Concept:** "A Simpler and Faster Europe" – Reducing administrative burden to support competitiveness.
2. **Key Action:** Repeal of Obsolete Acts.
   - Explicitly repeals P2B Regulation (2019/1150).
   - Superseded by Digital Services Act (DSA) & Digital Markets Act (DMA).
3. **The Big Win:** Consolidated Incident Reporting.
   - Avoids duplication and administrative fatigue for EU businesses.

Cybersecurity Act 2: Strengthening the Enforcers

Proposal 2026/0011 (20.01.2026) – Replacing Regulation 2019/881



ENISA's Enhanced Mandate:

Role expanded to support NIS2 implementation and operational cooperation.

Scope Expansion: Managed Security Services (MSS):

Now explicitly included in the European cybersecurity certification framework.

Objective:

Standardizing the quality of outsourced security services to combat ransomware and state-sponsored threats.

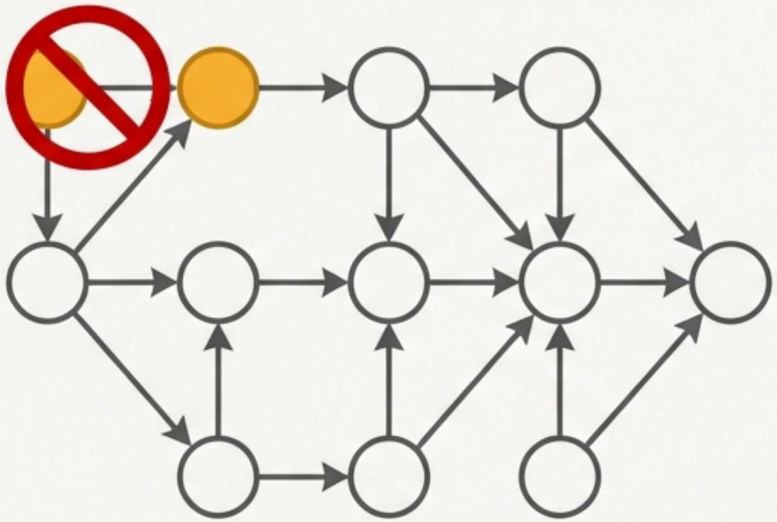
Strategic Focus: Strengthening EU Institutions & Supply Chain Security

CSA 2: Hardening the ICT Supply Chain

Addressing Non-Technical Risks & High-Risk Suppliers

The Focus: 'Non-Technical Risks'

- Foreign state influence.
- Espionage potential.
- Leverage by third.
- Leverage by third countries.



The Consequence: 'High-Risk Supplier' Designation

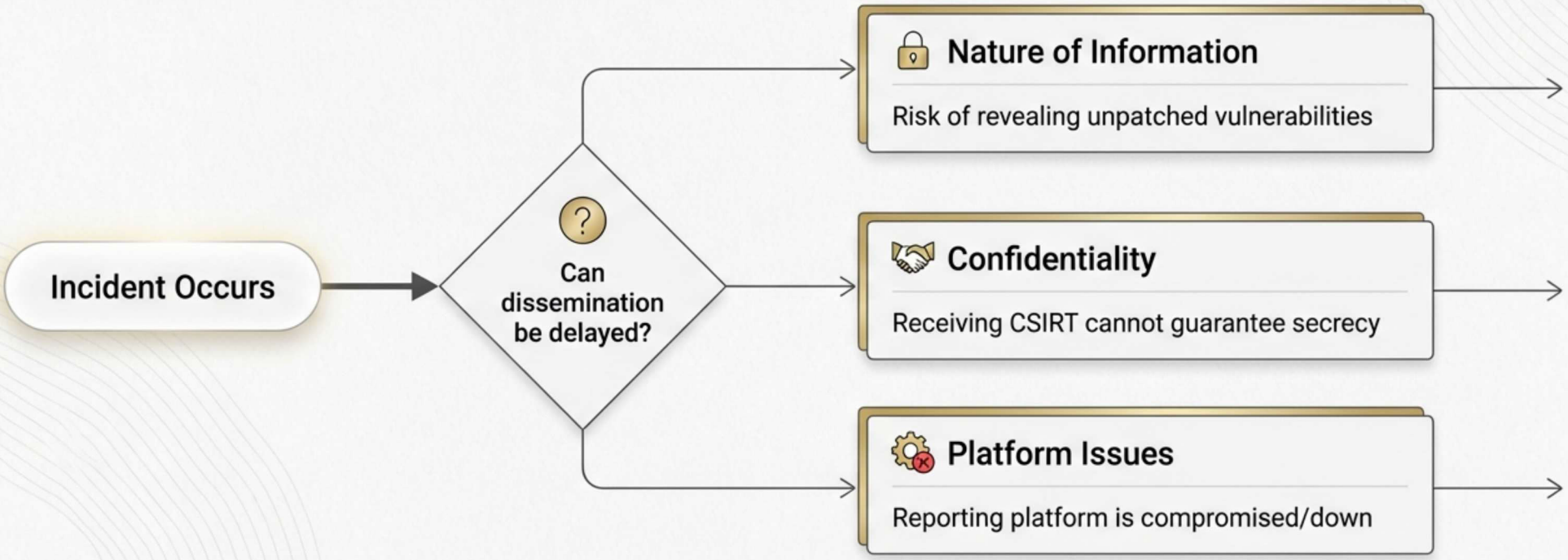
- Barred from EU funding programs.
- Prohibited from use in Key ICT Assets.

Critical Infrastructure Impact:

- Mobile, Fixed, and Satellite networks must phase out high-risk components.

CRA Delegated Regulation: Managing Incident Transparency

Commission Delegated Regulation of 11.12.2025

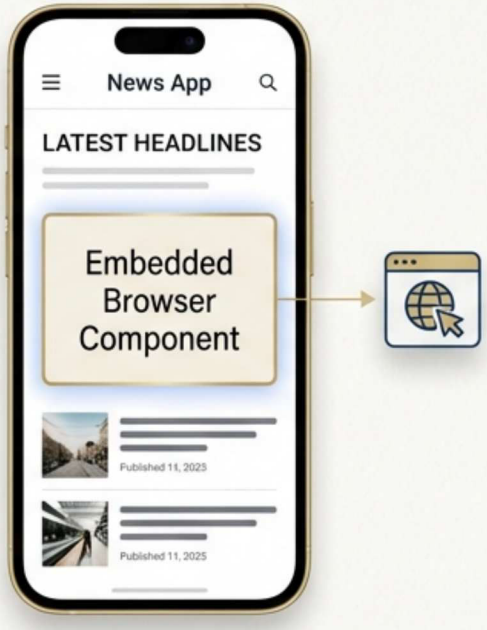


Effective Date: Reporting obligations apply from 11 September 2026.

CRA Implementing Regulation: Defining the Product Landscape

Regulation 2025/2392 (28.11.2025) – The 'Core Functionality' Principle

Part A (Left): The Container & Component



News App with Integrated Browser

Part B (Right): The Core Functionality Principle

The Principle: Categorization is based on Primary Purpose.

The Scenario: A News App integrates a browser component.

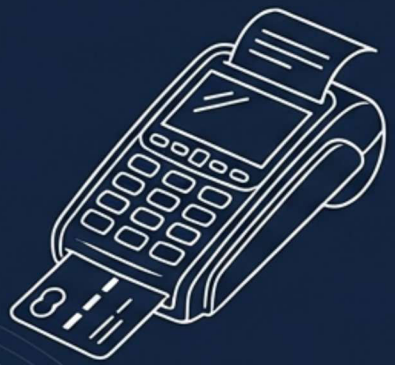
The Ruling: The News App does NOT become a "Class I Browser" because its core function is delivering news.

The Obligation: The manufacturer must ensure the security of the integrated component, but the conformity assessment follows the App's category, not the Browser's.

Effective Date: Reporting obligations apply from 11 September 2026.

The ‘Critical’ List (Annex IV)

Products requiring the strictest conformity assessment (AVA_VAN.4+)

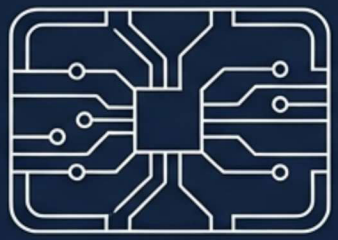


Hardware Devices with Security Boxes

Physical payment terminals, Tachographs, Hardware Security Modules (HSMs).

Smart Meter Gateways

Specifically controlling communication in electricity/gas metering systems.



Smartcards & Secure Elements

TPMs, Identity documents (ePassports), Qualified signature cards.

Effective Date: Reporting obligations apply from 11 September 2026.

The ‘Important’ List (Class I & II)

Regulation 2025/2392 Annex I & II

Class I: Widespread Infrastructure

- Identity Management Systems & PAM

- Standalone & Embedded Browsers

- Password Managers & Antivirus

- VPNs, Network Management, SIEMs

Class II: Deep Infrastructure

- Hypervisors & Container Runtime Systems

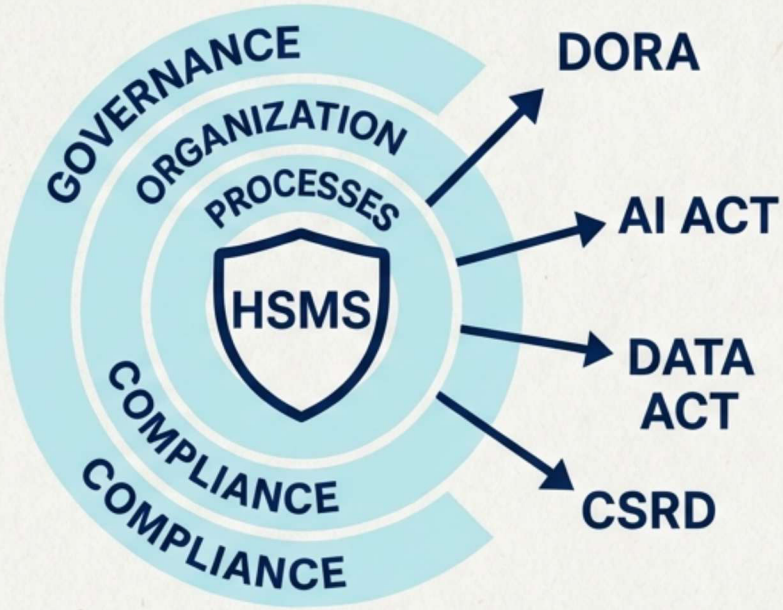
- Firewalls & IDPS

- Tamper-Resistant Microprocessors (AVA_VAN level 2/3)

Effective Date: Reporting obligations apply from 11 September 2026.

The Integrated Approach: HSMS

Harmonizing NIS2, DORA, CRA, and the AI Act



2025 (NIS2) → **2026** (DORA/CRA) → **2027** (CSA)

NIS2 / DATA ACT	DORA / CRA / AI ACT	CSA CSRD

Strategic Action Checklist

- [ ] **Prepare for Consolidated Reporting (Omnibus)**
  Align incident response workflows to the new Single Reporting Mechanism.
- [ ] **Audit the Supply Chain (CSA2)**
  Screen vendors for ‘High-Risk’ non-technical and foreign state influence risks.
- [ ] **Classify Products (CRA)**
  Map portfolio against Reg 2025/2392. Determine Class I, Class II, or Critical status based on Core Functionality.
- [ ] **Define Notification Protocols**
  Update playbooks to include valid grounds for delaying incident dissemination.

Thank You

Navigating the future of European Cybersecurity.

Miroslav Mitev, PhD
phdmitev@gmail.com