simmons+simmons

EU Cybersecurity Laws

What your organisation needs to know

20 May 2026

Introduction

Presenters

Jaap Tempelman

Partner

Corporate & Commercial

Amsterdam

Christopher Götz

Partner

Digital Business

Munich

Jérémie Doornaert

Partner

Dispute Resolution

Brussels

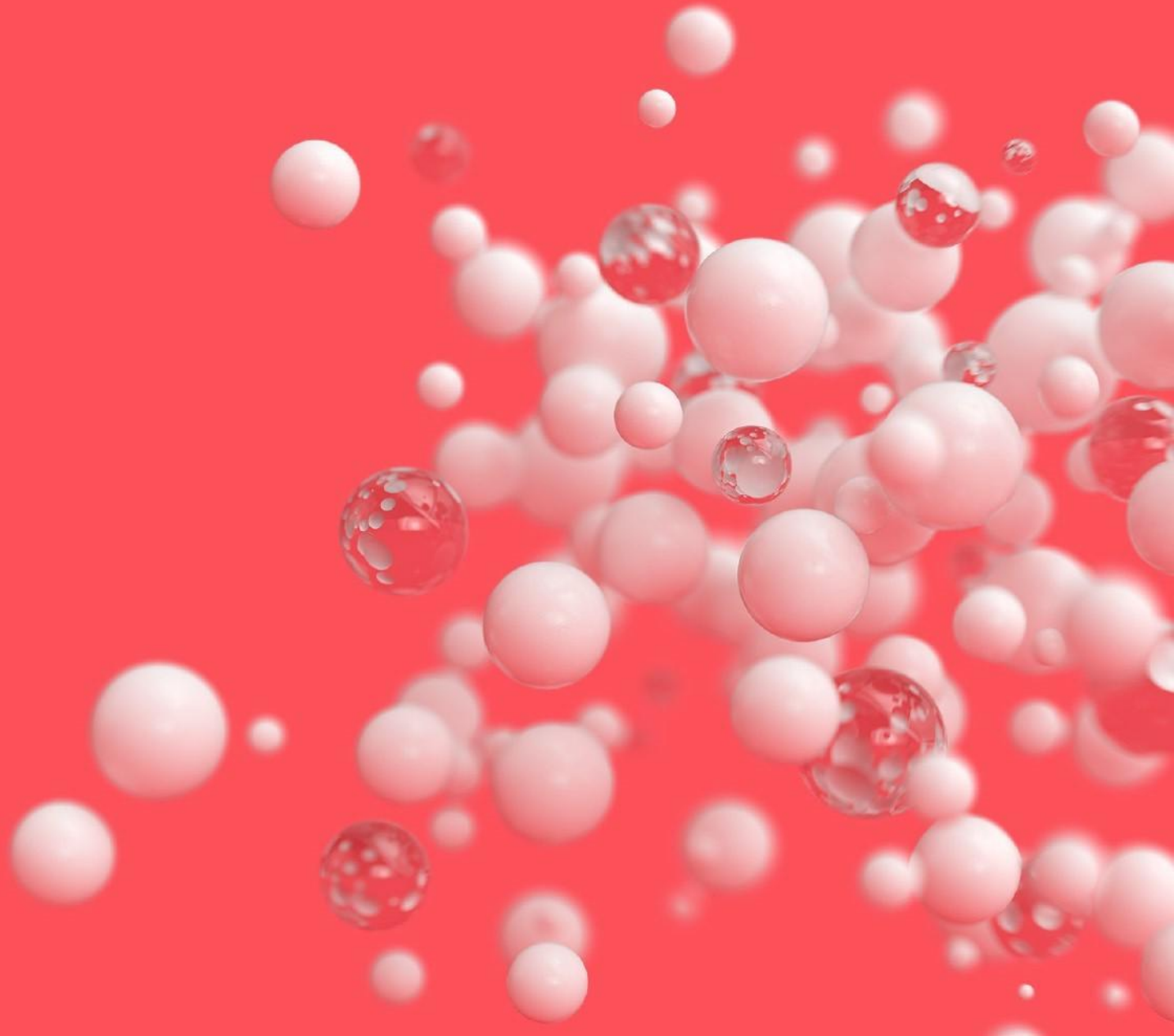
Session overview

What we'll cover

1	NIS2 Directive (Christopher Götz)
2	CER Directive (Jérémie Doornaert)
3	CRA and Cybersecurity Act (Jaap Tempelman)

NIS 2 Directive

Christopher Götz
Partner, Digital Business
Munich



Purpose: What is NIS 2 and why is it relevant?

- EU Directive aiming at a high common level of cybersecurity.
- Minimum harmonisation ⇨ Member States may adopt stricter cybersecurity requirements.
- Harmonises minimum requirements for cyber risk management and incident reporting.
- Applies to public and private entities across 18 critical sectors.
- Governance: cybersecurity becomes an explicit responsibility of the management bodies
  - Must approve cybersecurity risk-management measures and oversee its implementation
  - Can be held liable for the entity's non-compliance with cybersecurity risk management measures

Timeline

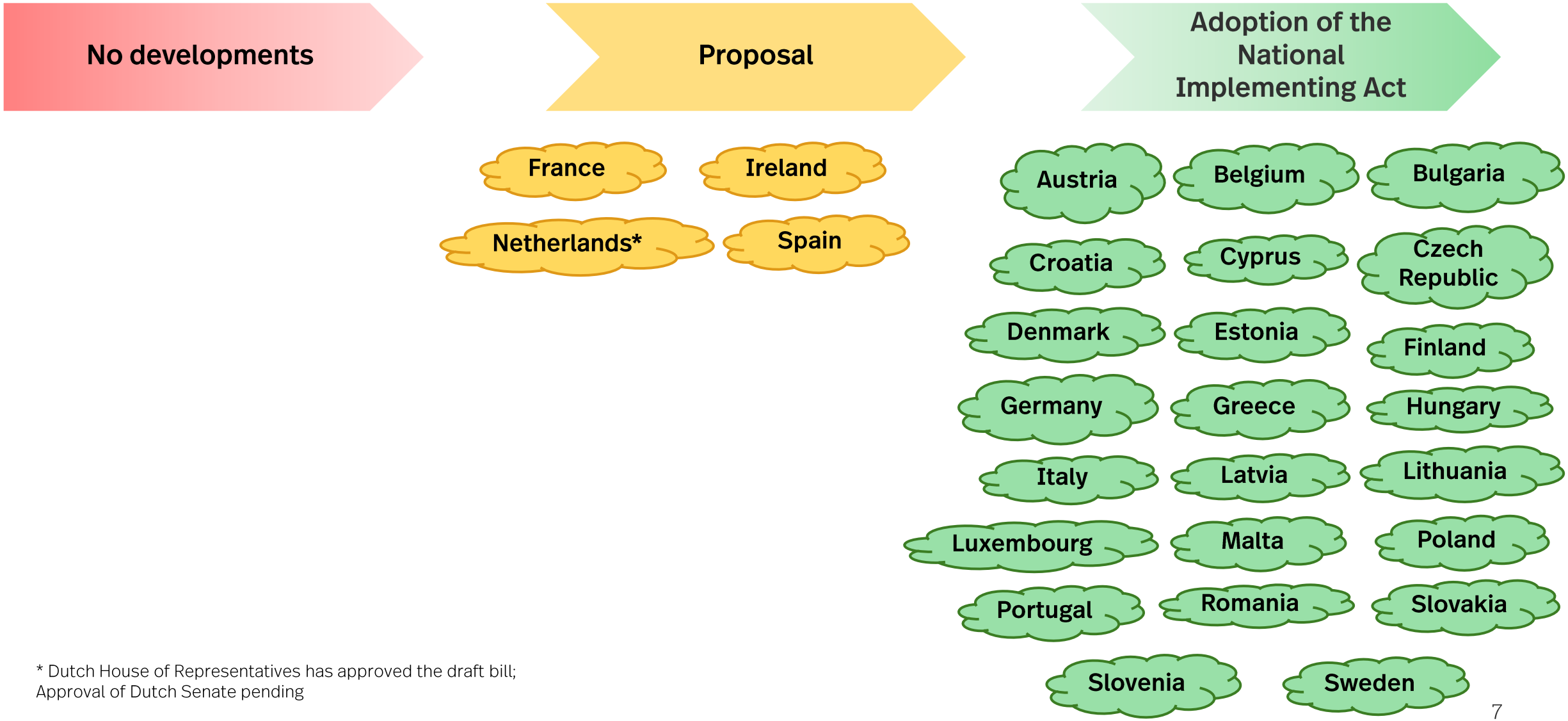
Dec 2022
NIS 2 Adoption

Oct 2024
- Transposition deadline for Member States
- Only a minority of EU Member States met the deadline

Dec 2025
German Implementation Law entered into force

Implementation Status as of May 2026
- 23 of 27 EU Member States: Adoption of a national implementing act
- 4 Member States: Publication of a proposal/in consultation phase

Implementing status across Member States



* Dutch House of Representatives has approved the draft bill; Approval of Dutch Senate pending

NIS vs. NIS 2 – Sectors covered

NIS (Directive 2016/1148)

In force 2016 – 2024

7 sectors

- Energy · Transport · Banking · Financial market infrastructures · Health · Water Management · Digital infrastructure
- Digital Service Providers (online marketplaces, search engines, cloud) under a separate lighter regime

Scope set by Member States

- Each Member State individually identified the Operators of Essential Services (OES)

Coverage in Germany

- ~ 4,500 entities in scope under BSI-Gesetz (pre-NIS 2)

NIS 2 (Directive 2022/2555)

Applicable from 18 October 2024

18 sectors (Annex I + Annex II)

- Expands sectors

Size-cap rule (self-assessment)

- Direct application to medium-sized+ entities in covered sectors – no Member State designation

Coverage in Germany

- ~ 29,500 entities in scope – roughly 6.5× the prior coverage

Scope: Who is affected? (Art. 2)

Art. 2(1) NIS 2:

> "This Directive applies to public or private entities of a **type referred to in Annex I or II** which qualify as **medium-sized enterprises** under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which **provide their services or carry out their activities within the Union**."

- **Sectors:** 18 critical sectors listed in Annex I and Annex II, e.g.: Digital Infrastructure, ICT Service Management, Banking and Financial Market Infrastructures.

- **Threshold:** 50 or more employees, or an annual turnover of more than EUR 10 million and an annual balance sheet total of more than EUR 10 million.

  These thresholds do not apply to certain critical entities listed in Art. 2(2)-(4), e.g. trust service providers.

- **Extraterritorial Effect**

Example: Germany

~29,500 entities in-scope (compared to ~4,500 entities covered by the respective cybersecurity law before)

The 18 critical sectors (Annex I & II)

Annex I – Sectors of high criticality (11)

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (B2B)
- Public administration
- Space

Annex II – Other critical sectors (7)

- Postal & courier services
- Waste management
- Chemicals
- Food
- Manufacturing
- Digital providers
- Research

Same substantive obligations apply across all 18 sectors — Annex I/II classification feeds into Essential vs. Important categorisation (next slides).

Zooming in: the three digital sectors

ANNEX I – point 8
Digital infrastructure

- Internet exchange point (IXP) providers
- DNS service providers (excl. root name server operators)
- TLD name registries
- **Cloud computing service providers → SaaS, IaaS, PaaS**
- Data centre service providers
- Content delivery network (CDN) providers
- Trust service providers (eIDAS)
- Providers of public electronic communications networks
- Providers of publicly available electronic communications services

ANNEX I – point 9
ICT service management (B2B)

- **Managed service providers** (MSPs)
- Managed security service providers (MSSPs)

*Captures B2B outsourcing of IT and security functions: **remote monitoring & management, helpdesk, patch management**, identity & access management, SOC services, network operations, vulnerability management, incident response – irrespective of whether the underlying infrastructure is owned by the provider or the customer.*

ANNEX II — point 6
Digital providers

- Providers of **online marketplaces**
- Providers of **online search engines**
- Providers of **social networking** services platforms

These are the three categories the NIS 1 regime treated as 'Digital Service Providers' under a separate, lighter regime. Under NIS 2 they are integrated into the main framework – but classified as Important (not Essential) entities.

Note: financial-sector cloud, data centre and ICT third-party providers may fall under DORA as lex specialis (Art. 4 NIS 2) – see overview slide.

Scope: Essential vs. important entities (Art. 3)

Essential Entities

- Entities referred to in "**highly critical sectors**" (→ Annex I) plus
- **Exceeding ceiling for medium sized enterprises.**
- Certain key entities irrespective of size (e.g. DNS, trust services, public communications)

Important Entities

- Entities in sectors listed in **Annex I or II** which **do not qualify** as "**essential entity**"
- Broader range of sectors (e.g. manufacturing, digital providers)

- Subject to **stricter supervision** and enforcement (Art. 32 NIS 2)
- **maximum fines** up to **EUR 10 million or 2% of annual turnover** for certain infringements

- **Lighter supervisory regime**
- **maximum fines** up to **EUR 7 million** or **1.4% of total annual turnover** for certain infringements

All in-scope entities must submit and keep up-to-date certain company information to competent authorities (Art. 3(4))

Stricter vs. lighter supervision

	Essential entities – stricter regime (Art. 32 NIS 2)	Important entities – lighter regime (Art. 33 NIS 2)
Substantive cyber obligations	Identical – Art. 21 risk-management measures + Art. 23 incident reporting	Identical – Art. 21 risk-management measures + Art. 23 incident reporting
Supervisory approach	Ex-ante AND ex-post – proactive oversight from day one	Ex-post only – supervisory action requires evidence/indication of non-compliance
Supervisory measures	Regular and targeted audits · ad-hoc audits · on-site & off-site checks · security scans · requests for information & evidence	Ex-post on-site / off-site checks · targeted audits · requests for information – only with cause
Enforcement powers	Binding instructions · suspension of certification or authorisation · temporary ban of CEO / legal representative from management functions	Binding instructions · orders to remedy · publication of infringement – but no suspension of authorisation, no management ban
Admin. fines (DE)	Up to € 10 million or 2 % of global annual turnover (whichever is higher)	Up to € 7 million or 1.4 % of global annual turnover (whichever is higher)

Key takeaway: the substantive cyber obligations are identical – the tier governs HOW the regulator polices compliance, not WHAT entities must do.

Cybersecurity risk-management measures (Art. 21)

Technical, operational and organisational measures

1. Policies on risk analysis and information system security.
2. Incident handling.
3. Business continuity and crisis management.
4. Supply chain security.
5. Security in network and information systems acquisition, development and maintenance.
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measure.
7. Basic cyber hygiene practices and cybersecurity training.
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
9. Human resources security, access control policies and asset management.
10. Multi-factor authentication or continuous authentication solutions, secured voice, video and text communications, secured emergency communication systems.

Reporting of a Significant Incident (Art. 23)

Art. 23(3) NIS 2:

"An incident shall be **considered to be significant** if:

a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage."

Reporting Deadlines (Art. 23(4) NIS 2)

≤ 24h **Early warning**

- Trigger point: "becoming aware of significant incident"

→ Malicious/unlawful?

→ Possible cross-border impact

≤ 72h **Incident notification**

- Initial assessment of the incident

➢ Severity & impact

- Indicators of compromise (if available)

≤ 1 month **Final report**

- 1 month after Incident Notification

→ Detailed description:

- Root cause/threat
- Applied and ongoing mitigation measures
- cross-border impact (if applicable)

NIS 2 in the EU cyber regulatory landscape

NIS 2 does not operate in isolation – overlapping and sector-specific regimes shape concrete obligations:

DORA (Reg. 2022/2554)

Financial sector – lex specialis

- Art. 4 NIS 2: where DORA imposes equivalent or stricter requirements, NIS 2 does NOT apply to financial entities
- Applies from 17 January 2025 – banks, insurers, investment firms, crypto-asset providers, ICT third-party providers
- ICT incident reporting under DORA Art. 19 replaces NIS 2 Art. 23 for financial entities

GDPR (Reg. 2016/679)

Parallel – personal data breaches

- Cyber incident often = personal data breach: parallel notification to DPA under Art. 33 (72h) and to subjects under Art. 34
- Different addressee, different threshold, different deadlines – but the same factual event
- Document both regimes' assessments and timelines

CER Directive (2022/2557)

Physical resilience – sister instrument

- Targets the same 11 highly critical sectors as NIS 2 Annex I
- Covers physical and organisational resilience (continuity, supply chain) – NIS 2 covers cyber/digital
- Entities often qualify under BOTH regimes simultaneously

Cyber Resilience Act (Reg. 2024/2847)

Products with digital elements

- Product-level cybersecurity for hardware and software placed on the EU market
- Manufacturer obligations: secure-by-design, vulnerability handling, CE marking
- Most obligations apply from 11 December 2027 – complements entity-level NIS 2 duties

Cloud providers under NIS 2 and the Data Act

Cloud computing service
Art. 6(30) NIS 2

- **On-demand administration** and broad remote access
- **Scalable and elastic pool** of shareable computing resources
- **Resources may be distributed** across several locations

Data processing service
Art. 2(8) Data Act

- **Ubiquitous, on-demand network access** – NIST-style characteristics
- **Shared pool of configurable, scalable, elastic** resources
- **Centralised, distributed or highly distributed** – captures edge
- **Rapid provisioning**, minimal management effort

Same universe of services: IaaS · PaaS · SaaS *Recital 81 Data Act confirms alignment with cloud computing*

Cybersecurity stream
obligations under NIS 2

- **Art. 21 NIS 2** – technical, operational and organisational risk-management measures
- **Art. 23 NIS 2** – significant incident reporting (24 h / 72 h / 1 month)
- **Supply-chain security** (Art. 21(2)(d))
- **Tier: Annex I** + large = Essential; Annex I + medium-sized = Important

Switching & portability stream
obligations under the Data Act

- Arts. 23–25 – remove contractual, technical and economic obstacles to switching
- Art. 29 – switching charges withdrawn; full removal of egress fees by 12 Jan 2027
- Art. 30 – functional equivalence for IaaS
- Chapter 8 (Arts. 33–36) – interoperability standards
- No size threshold – applies once you qualify as a DPS

Parallel application – NOT a lex specialis relationship (cf. DORA under Art. 4 NIS 2). Two compliance streams on the same product.

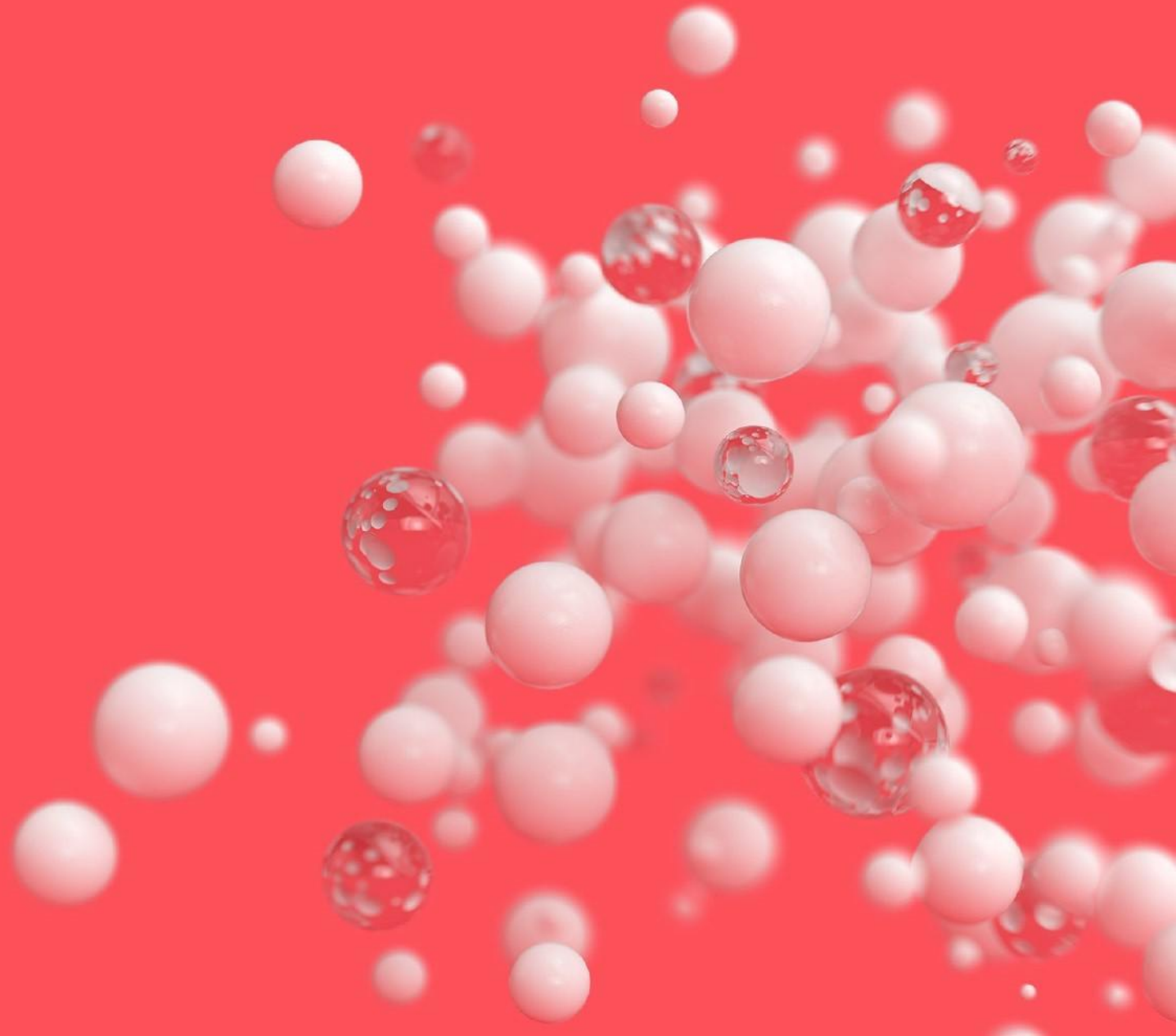
Edge cases: single-tenant private clouds and pure SaaS – both regimes read broadly; financial-sector cloud subject to DORA as lex specialis (Art. 4 NIS 2).

Next steps

1	Assess whether your organisation is in scope and, if positive, submit necessary company information to competent authorities.
2	Establish governance and accountability.
3	Implement risk management measures.
4	Set up incident reporting processes.
5	Prepare for regulatory interaction.

Critical Entities Resilience (CER) Directive

Jérémie Doornaert
Partner, Dispute Resolution
Brussels



Scope of application

Directive (EU) 2022/2557 – CER Directive

- New EU framework on resilience of critical entities
- Replaces Directive 2008/114/EC from 18 October 2024
- Aim : Ensure essential services in the internal market remain uninterrupted

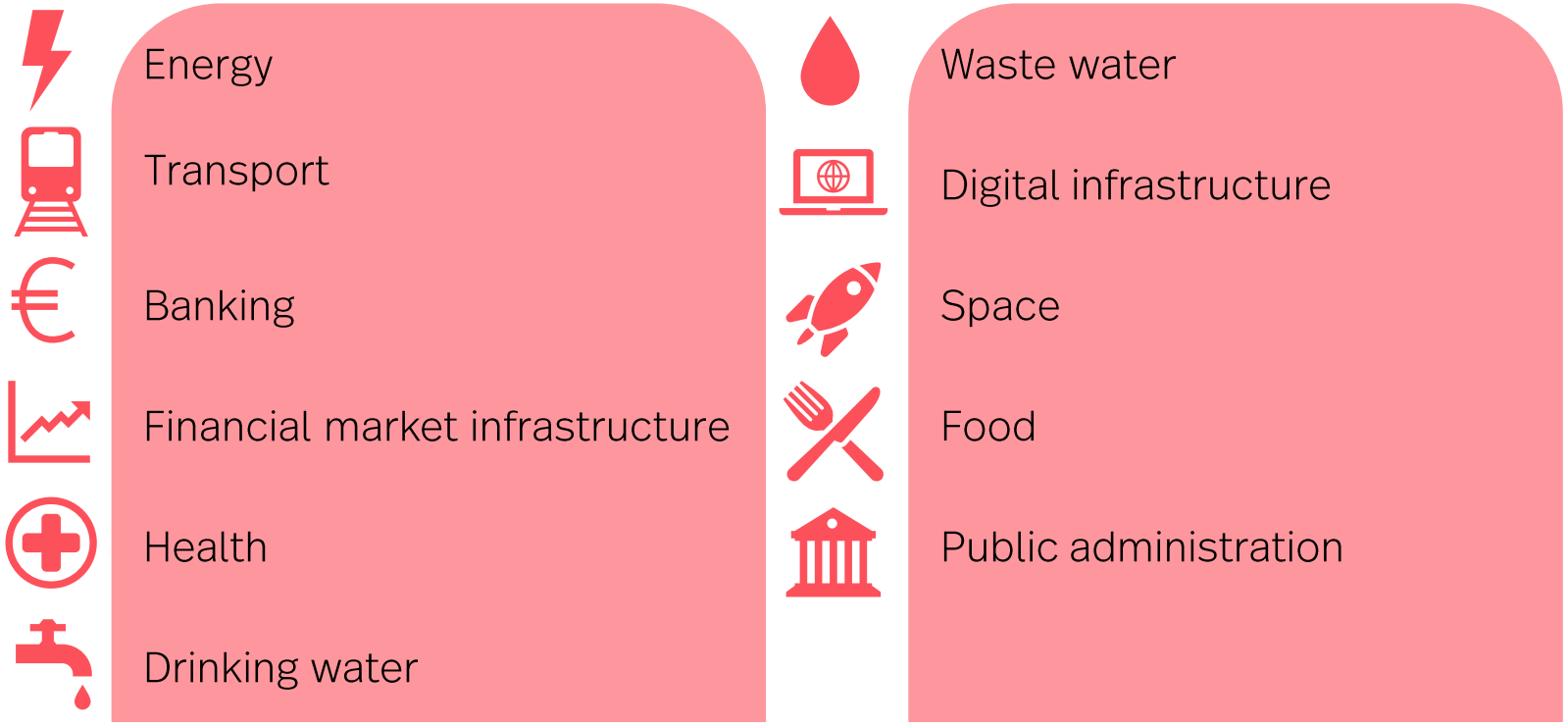
Scope of application

Why a CER Directive?

- A dynamic threat landscape: hybrid threats, terrorism, natural disasters, climate change (Recital 3)
- Cascading effects: a disruption in one sector can impact many others across borders (Recital 5)
- Fragmented national approaches: inconsistent identification of critical entities across Member States (Recital 3)
- Lessons from the COVID-19 pandemic exposing the vulnerability of interdependent societies (Recital 5)
- Replacement of the 2008/114/EC Directive (European Critical Infrastructure) with a broader, all-hazards framework (Recital 4)

Scope of application

What does it cover?



Resilience of entities providing “essential services” : Services crucial for vital societal functions, economy, public health & safety, environment

Scope of application

Where?

- Applies to Member States and critical entities operating within the EU
- Entity deemed to operate in a Member State if:
  - It carries out activities necessary for the essential service there, and
  - Its critical infrastructure used for that service is located on that territory
- Third countries: only indirectly (via cross-border dependencies considered in risk assessments and cooperation)

Who?

- Critical entity = public or private entity in an Annex category, identified by a Member State as critical
- Includes certain public administration entities of central government, except those whose activities are predominantly in national security, public security, defence or law enforcement
- Special treatment: Digital infrastructure and financial sector entities are identified as “critical”, but core resilience/supervision chapters of CER do not apply; NIS2 / financial law cover them instead

Scope of application

What does it exclude?

- Cybersecurity matters → governed by the NIS 2 Directive (2022/2555) - though both must be implemented in a coordinated manner (Art. 1(2))
- National security, defence, public security, law enforcement (Art. 1(5) & Recital 11)
- EU diplomatic and consular missions in third countries (Recital 11)
- EU space programme infrastructure owned/operated by the Union (Recital 5)
- Banking, financial markets & digital infrastructure → exempt from certain obligations (Art. 13 resilience measures) under Article 8 – sector-specific rules apply instead
- Equivalent sector-specific EU law: where national measures are at least equivalent to CER obligations, CER provisions (including supervision/enforcement) do not apply (Art. 1(3))

Main obligations

Obligations of Critical Entities

Risk assessment & planning

- Within 9 months of being notified as critical, then at least every 4 years
- Carry out a critical entity risk assessment (all relevant risks, dependencies)
- Prepare and apply a resilience plan (or equivalent document) describing measures taken

Art. 12-13

Resilience measures (examples)

- Prevent incidents
- Physical protection of premises & critical infrastructure
- Incident response & crisis management procedures and alert routines
- Business continuity & recovery, including alternative supply chains

Art. 13

Governance

- Designate a liaison officer as point of contact with competent authorities

Art. 13

Enforcement & sanctions

Supervision & enforcement

Supervisory tools (art. 21) : Member States must ensure competent authorities can :

- Conduct on-site inspections of critical infrastructure and premises
- Carry out or order audits
- For entities that are also under NIS2: require
  - Information needed to assess whether resilience measures meet CER requirements
  - Evidence of effective implementation

Remedial measures & safeguards (art. 21)

- After supervision, authorities may order critical entities to take necessary and proportionate measures to remedy infringements, within a reasonable deadline, taking seriousness into account
- Exercise of powers must include safeguards:
  - Objectivity, transparency, proportionality
  - Protection of trade/business secrets
  - Rights of defence and effective judicial remedy

Enforcement & sanctions

Penalties

National penalties

- Member States must set rules on penalties for infringements of national measures implementing CER

- Penalties must be:
  - Effective
  - Proportionate
  - Dissuasive

- CER does not harmonise exact amounts or types of fines. It leaves this to national law, but under the “effective, proportionate, dissuasive” standard

Implementation

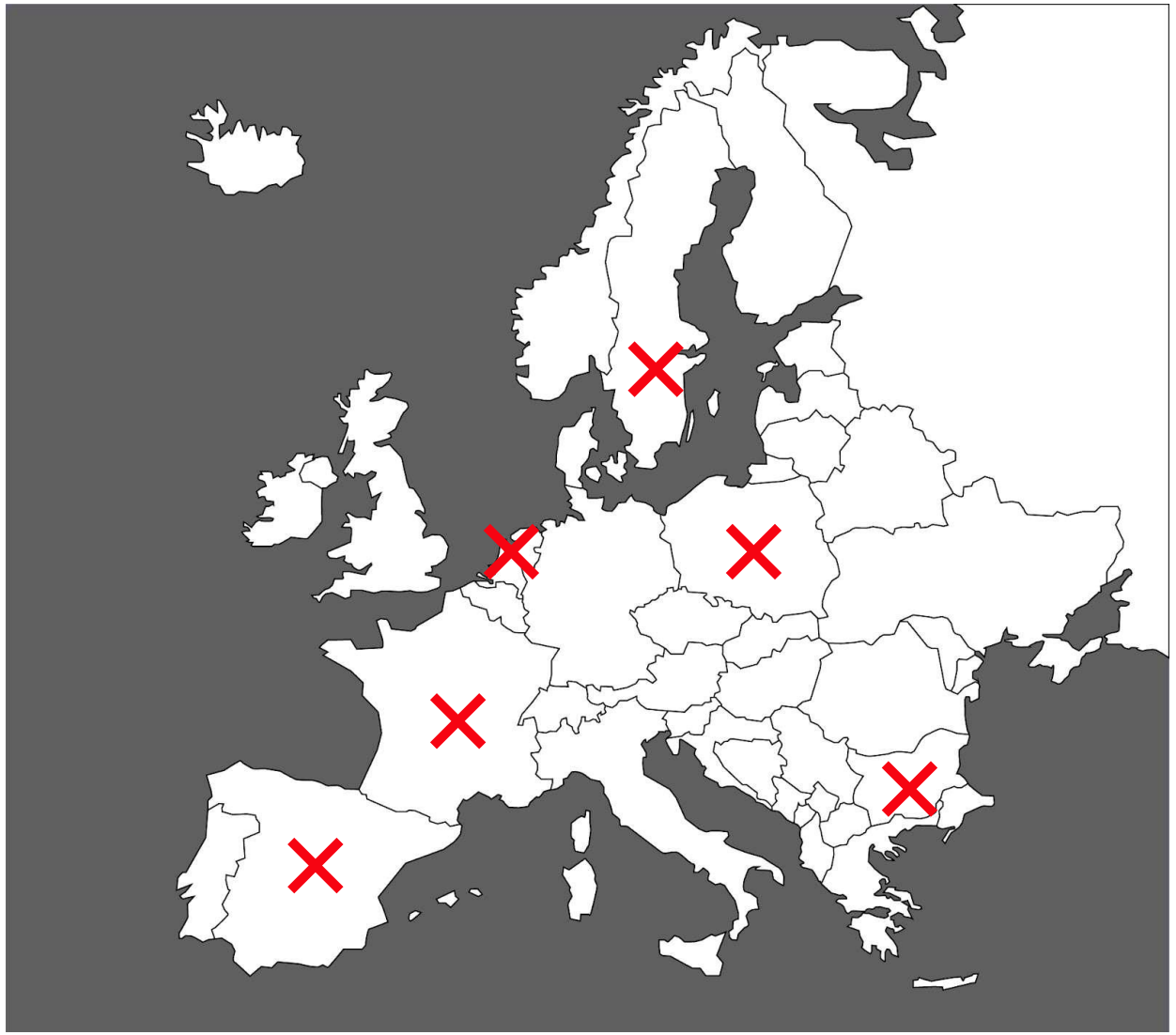
Key deadlines

17 October 2024	Member States must adopt and publish national implementing measures
18 October 2024	• Directive 2008/114/EC is repealed • Member States must apply those measures
17 January 2026	Member States adopt national strategy + complete risk assessment
17 July 2026	Member States identify critical entities
17 July 2027	Commission report on whether Member States have taken necessary measures
17 July 2028	First biennial report by Single Points of Contact
17 June 2029	First overall review of CER

Implementation

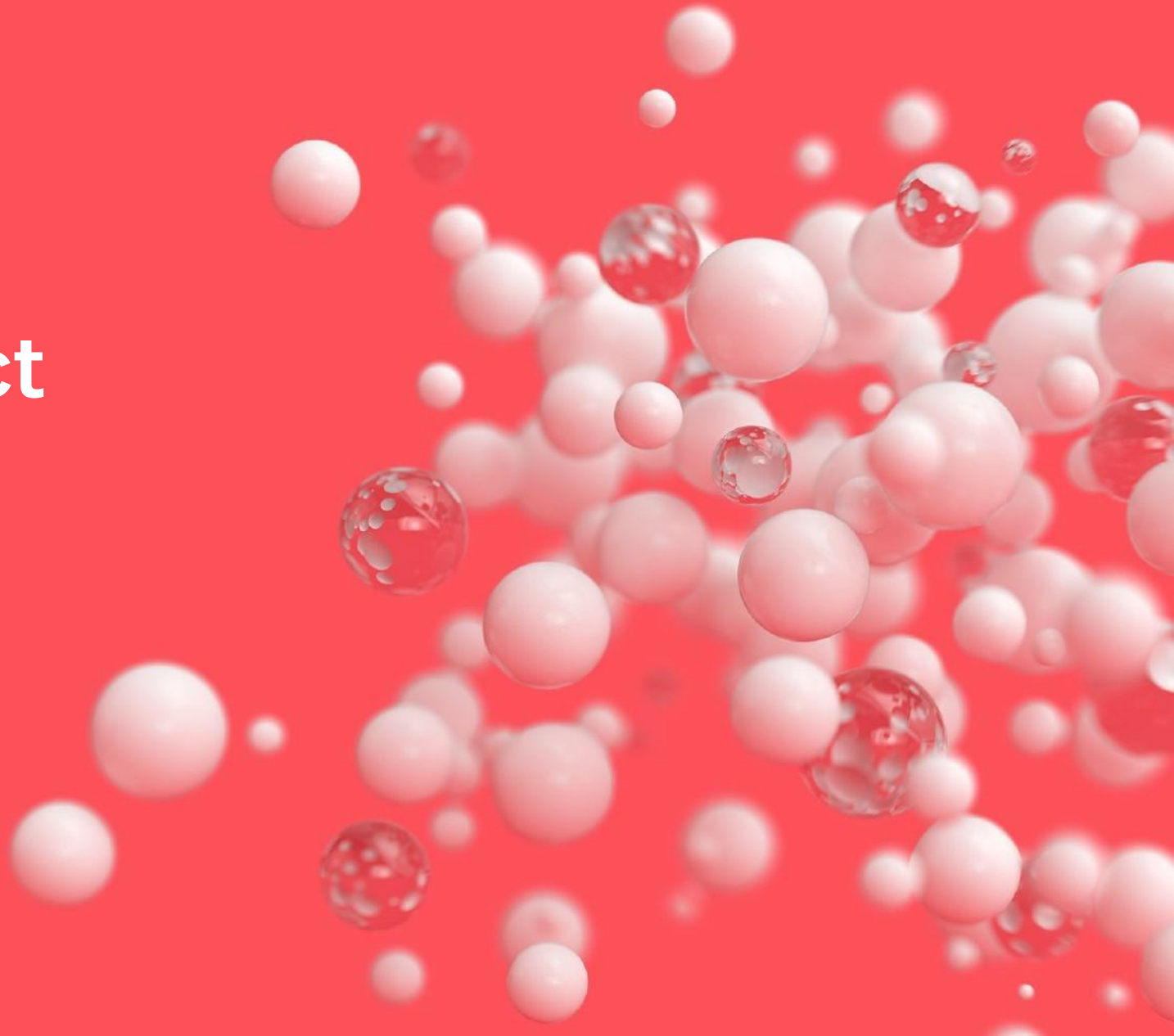
Overview in the EU

AT Austria	Implemented
BE Belgium	Implemented
BG Bulgaria	Pending
HR Croatia	Implemented
CY Cyprus	Implemented
CZ Czechia	Implemented
DK Denmark	Implemented
EE Estonia	Implemented
FI Finland	Implemented
FR France	Pending
DE Germany	Implemented
GR Greece	Implemented
HU Hungary	Implemented
IE Ireland	Implemented
IT Italy	Implemented
LV Latvia	Implemented
LT Lithuania	Implemented
LU Luxembourg	Implemented
MT Malta	Implemented
NL Netherlands	Pending
PL Poland	Pending
PT Portugal	Implemented
RO Romania	Implemented
SK Slovakia	Implemented
SI Slovenia	Implemented
ES Spain	Pending
SE Sweden	Pending



Cyber Resilience Act and Cybersecurity Act

Jaap Tempelman
Partner, Corporate & Commercial
Amsterdam



Scope of application

Regulation (EU) 2024/2847 – Cyber Resilience Act

What does it regulate:

- Harmonised cybersecurity obligations imposed on manufacturers/importers/distributors of products with digital elements that are made available on the EU Market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

- Obligations for open source stewards.

Product with digital elements:
A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.

Remote data processing obligations:
Data processing at a distance for which the software is designed and developed by or under the responsibility of the manufacturer of a PDE, and the absence of which would prevent the PDE from performing one or more of its functions.

Products with digital elements

All PDEs must meet the **Essential Cybersecurity Requirements** (Annex 1)

Presumption of conformity where PDEs meet harmonised EU standards,
otherwise Annex 8 conformity assessment procedures apply

Product Category	Examples	Assessment requirement
Regular PDEs	For example: mobile apps, mobile devices, network (terminal) equipment, etc.	Self-assessment by internal control procedures (module A of Decision (EU) 2008/768)
Important Products Class 1 (Annex III)	Identity management, password managers, smart home, general purpose virtual assistants	• EU-type examination procedure (modules B and C); or • Full quality assurance (module H)
Important Products Class 2 (Annex III)	Hypervisors, firewalls, tamper-resistant microprocessors	European cybersecurity certification scheme (assurance level "substantial")
Critical Products (Annex IV)	Hardware security boxes, smart meter gateways, smartcards	Mandatory certification under an EU cybersecurity certification scheme

Essential cybersecurity requirements

Cybersecurity requirements
(Annex 1, Part 1)

1. No known exploitable vulnerabilities
2. Secure by default configuration
3. (Automatic) security updates (with opt-out/postponement)
4. Protection from unauthorised access, and report on possible unauthorised access
5. Protection of confidentiality of data
6. Protect of integrity of data, and report on corruptions
7. Data minimisation
8. Protect availability of essential and basic functions
9. Minimise negative impact on other devices/networks
10. Designed to limit attack surfaces
11. Designed to reduce the impact of an incident
12. Recording and monitoring internal activity (with opt-out)
13. Enable secure and permanent deletion of all data and settings.

Vulnerability handling requirements
(Annex 1 – Part 2)

1. In relation to risks posed to PDEs, address and remediate vulnerabilities without delay, including by providing security updates (separate from functionality updates)
2. Apply effective and regular tests and reviews of the security of the PDE
3. Upon release of security update, publicly issue information about fixed vulnerabilities
4. Implement policy on coordinated vulnerability disclosure
5. Implement measures to facilitate the sharing of information about potential vulnerabilities in PDEs, including contact address for reporting of vulnerabilities
6. Implement mechanisms to securely distribute updates for PDEs to timely address vulnerabilities (automatically)
7. Ensure timely dissemination of security updates to address identified security issues

Exclusions and exemptions

- PDEs explicitly excluded from the CRA's scope, include those that:
  - are governed as a medical device under EU Regulation 2017/745 or 2017/746;
  - are governed as part of a motor vehicle under Regulation (EU) 2019/2144;
  - have been certified as aeronautical products in line with Regulation (EU) 2018/1139;
  - fall under the scope of marine equipment regulated by Directive 2014/90/EU; and
  - have been developed solely for national security or defence purposes or specifically designed to handle classified information.

- The CRA does not apply to spare parts that are marketed to replace identical components in PDEs and are manufactured according to the same specifications.

- CRA will also not apply to the extent that the relevant essential cybersecurity requirements are addressed by other Union legislation (e.g., NIS2 or DORA).

- PDEs that qualify as high-risk AI systems and comply with the essential cybersecurity requirements are deemed compliant with relevant cybersecurity requirements under Article 15 of the EU AI Act.

EU Cyber Resilience Act

Obligations

Manufacturers	Importers	Distributors
Perform cybersecurity risk assessment and ensure compliance with essential cybersecurity requirements (support 5 years)	Validate that PDEs meet cybersecurity requirements	
Perform conformity assessment, place required markings, and draw up technical documentation and user information (Annex 2)	Verify that conformity assessment has been performed and required technical documentation, information and markings are present	Verify that PDEs bear the required CE marking and that the manufacturer and importer have met their respective obligations as regards technical documentation and information and markings
Report actively exploited vulnerabilities and severe incidents	Notify manufacturer and authorities of vulnerabilities and risks	
Take corrective measures to remedy any non-compliance including withdrawal or recall	Take remedial measures to remedy non-compliance	

Incident reporting

- Manufacturers required to report:
  - Incident having a severe impact on the security of a PDE, i.e. an incident (as per NIS2) that:
    - negatively affects or is capable of negatively affecting the ability of a PDE to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or
    - has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

  - Actively exploited vulnerability: a vulnerability (weakness, susceptibility or flaw of a PDE) for which there is reliable evidence that a malicious actor has successfully exploited them.

Incident reporting

- Reports must be submitted to ENISA (via Single Reporting Platform) and the CSIRT of the Member State where the manufacturer has its main establishment:
  - Within 24 hours: Early warning notification. Must indicate if the incident is suspected to be caused by malicious acts and, where known, the impacted Member States.
  - Within 72 hours: Detailed incident notification. Requires general information, an initial assessment of the nature/severity, and corrective/mitigating measures taken and which users can take.
  - Within 1 month: Comprehensive final report. Must include a deep dive into the incident's severity and impact, root cause/threat type, and applied mitigation measures.

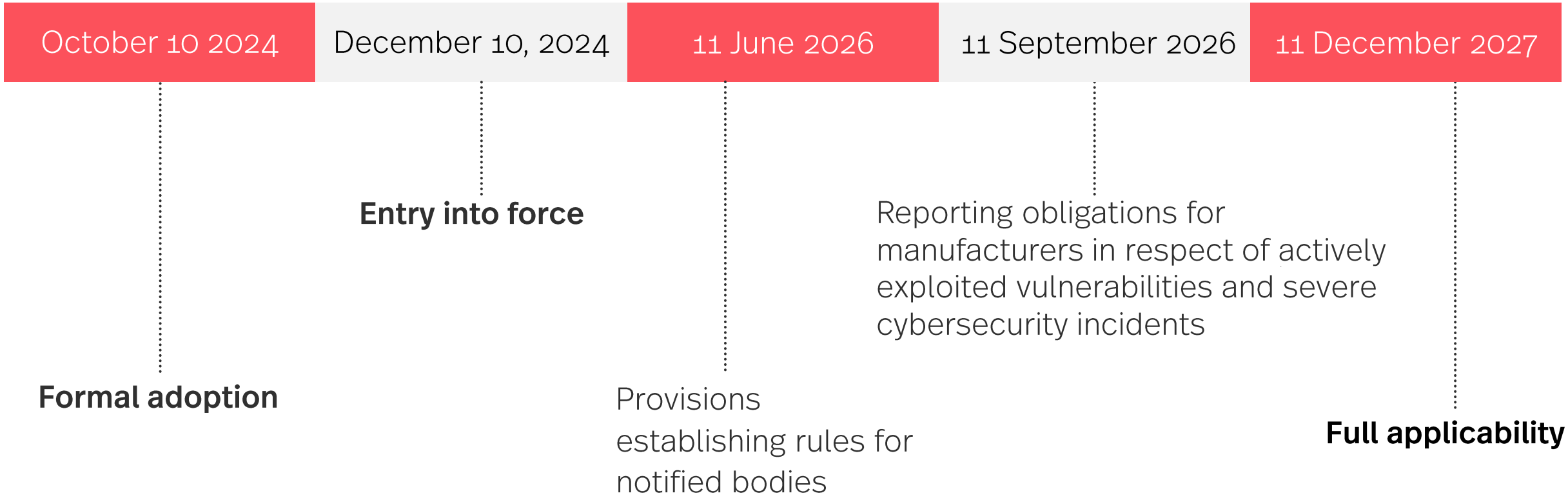
Open-source software stewards

- The CRA does not regulate open-source software that is distributed *outside* the course of a commercial activity.
- Light-touch obligations on 'open-source software stewards' in respect of PDEs that qualify as free and open-source software and are ultimately intended for commercial activities.
- These open-source software stewards are defined as legal persons (including, for example, foundations and not-for-profit entities) who provide support on a sustained basis for the development of the aforementioned PDEs and who play a main role in ensuring the viability of those PDEs.
- The obligations for these stewards include:
  - Development of a cybersecurity policy: a policy that promotes the creation of secure software and demonstrates how developers manage software vulnerabilities;
  - Cooperation with market surveillance authorities: collaborate with authorities that monitor the market and report any cybersecurity vulnerabilities that may arise.

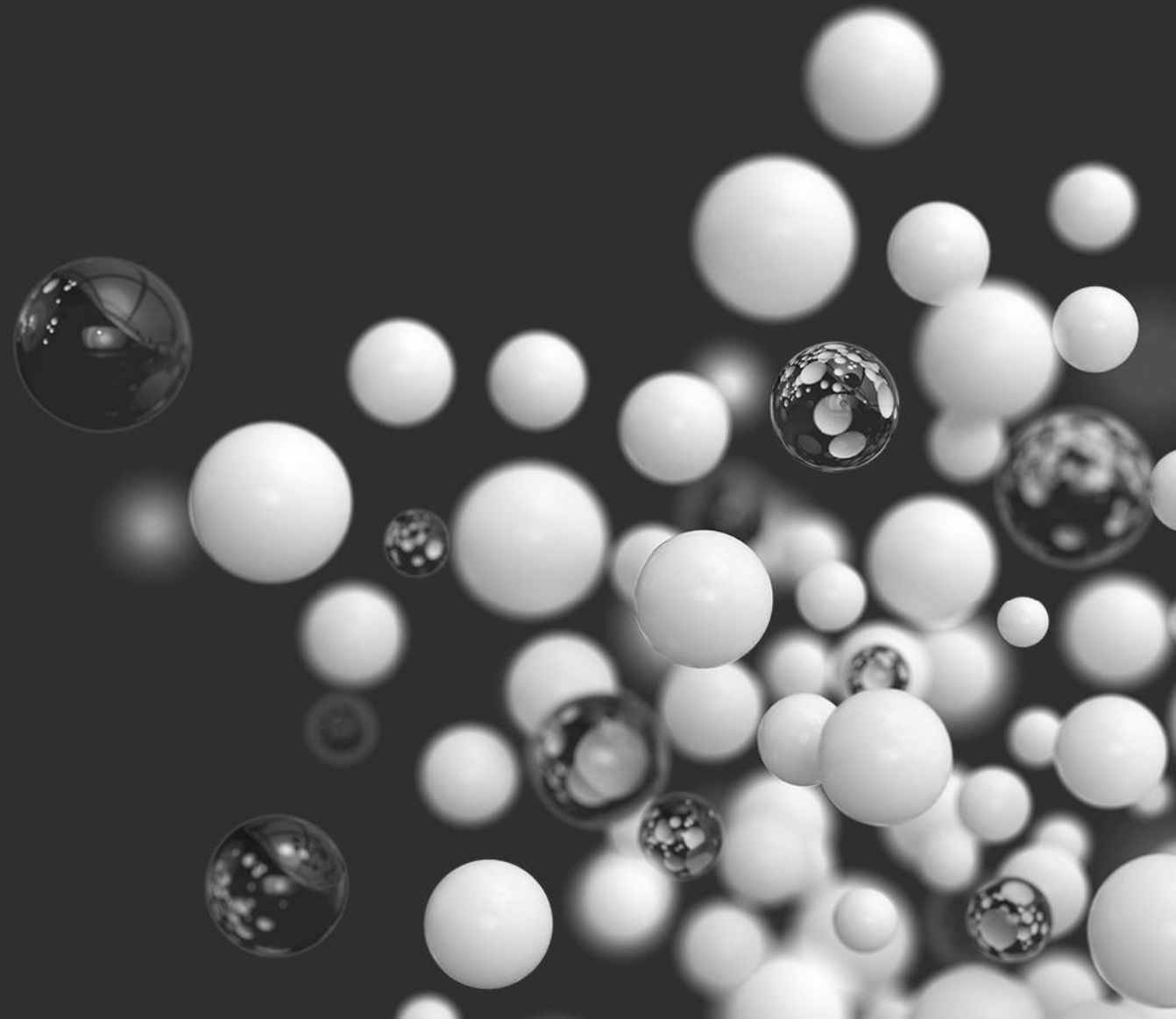
Enforcement and penalties

- Each EU Member State to appoint one or more market surveillance authorities to oversee and enforce the CRA.
- To ensure a uniform application of the CRA, an Administrative Cooperation Group (ADCO) will be established, consisting of representatives of all designated market surveillance authorities.
- Depending on the nature of the violation, breaches may result in administrative fines up to EUR 15 million or 2.5% of the total worldwide annual turnover, whichever is higher.

Timeline


October 10 2024
December 10, 2024
11 June 2026
11 September 2026
11 December 2027
Formal adoption
Entry into force
Provisions establishing rules for notified bodies
Reporting obligations for manufacturers in respect of actively exploited vulnerabilities and severe cybersecurity incidents
Full applicability

Cyber Security Act



EU Cyber Security Act

Overview

- Adopted in 2019.
- Establishes ENISA, the European Union Agency for Cybersecurity.
- Sets up a voluntary European cybersecurity certification framework for ICT products, ICT services and ICT processes.

Cybersecurity Package - Proposal of 20 Jan. 2026

- Broadening role of ENISA, notably to include managing unified incident reporting platform and repository of incidents and threats.
- Strengthening and streamlining certification framework – still voluntary but potentially *de facto* mandatory through procurement rules, market expectations, or national requirements.
- Introduction of supply chain security mechanisms to identify, restrict, or exclude suppliers considered “high-risk” across 18 critical sectors.

EU Cyber Security Act

Supply chain security

- Security risk assessment by NIS Coordination Group of serious and structural non-technical risks to ICT supply chains posed by third countries, taking into account:
  - the existence of laws or practices requiring entities to report software or hardware vulnerabilities to authorities prior to those vulnerabilities being known to have been exploited;
  - the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct the identified security concerns;
  - substantiated information about one or more incidents of threat actors controlled from the third country and operating out of the territory of that country carrying out malicious cyber activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the European Commission or EU Member States to address the risk

- Commission can identify high-risk countries and high-risk suppliers and key ICT assets involved, and (inter alia):
  - Prohibit NIS2 entities from using ICT components from high-risk suppliers;
  - Exclude high-risk suppliers from holding EU certifications, taking part in EU public procurement procedures, and funding programmes.

Useful resources

STRIDE

Simmons Technology Regulations Intelligence for the Digital Economy

simmons+simmons

simmons-simmons.com

Strictly private and confidential