



THE NIS2 DIRECTIVE: EUROPE'S RESPONSE TO CYBER SHENANIGANS

DEFCAMP, BUCHAREST

NOVEMBER 24TH, 2023

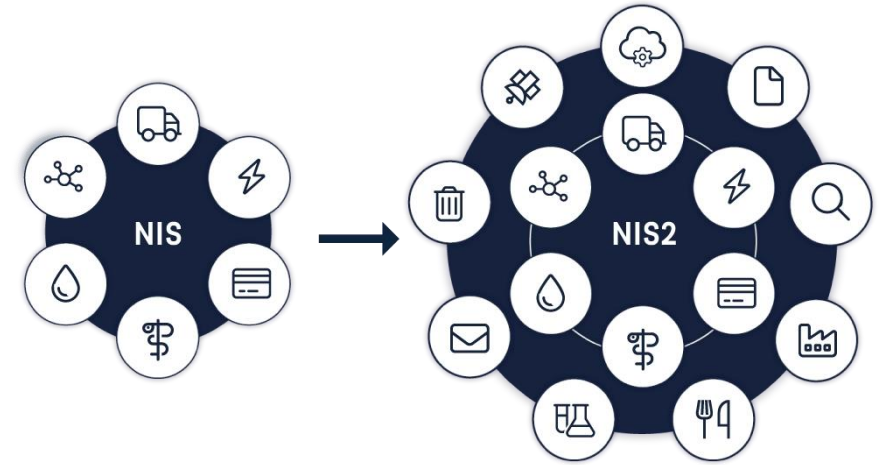
TUDOR DAMIAN

- **Cloud & Cybersecurity Advisor @ D3 Cyber**
 - Cybersecurity & vCISO Services
 - Cloud Strategy & Governance
 - IT Risk Management
 - Business Process Optimization
- **Email:** tudor.damian@d3cyber.eu
- **Contact:** tudy.ro



THE NIS2 DIRECTIVE, DEMYSTIFIED

- A bit of history
- What exactly is NIS2?
- Which sectors does it cover?
- Which organizations are impacted by NIS2?
- What requirements does it impose?
- Minimum measures to implement
- What happens if you don't comply?
- Conclusions & next steps
- Bonus: Cyber Resilience Act



The background is a dark blue field filled with numerous small, bright blue dots. These dots are arranged in various patterns, including straight lines, curves, and clusters, creating a sense of digital data or a network. At the top of the image, there are three horizontal bars of a slightly lighter blue color, each composed of many small dots.

THE NIS2 DIRECTIVE

FROM NIS TO NIS2



WHAT IS NIS2?

■ What Is The NIS2 Directive?

- Directive (EU) 2022/2555, introduced in 2020, came into effect on **Jan 16, 2023**
- Expands the previous EU **Network and Information Security (NIS) Directive**
- Aims to **enhance the security of network and information systems** within the EU
- Requires **operators of critical infrastructure and essential services** to implement appropriate **security measures** and **report any incidents** to the relevant authorities

■ NIS2 Becomes Law in 2024

- Member States have until **October 17, 2024**, to transpose the Directive into national law

■ Essential changes:

- Broader scope (more affected sectors and organizations)
- EU-wide cooperation (establishes the Cyber Crisis Liaison Organization Network - **EU-CyCLONe**)
- Stricter requirements (risk management, business continuity)
- Worse repercussions (corporate accountability, incident reporting, increased fines)

5 NEED-TO-KNOWS

01

Fines of up to **10 mil. EUR** or **2% of total** annual worldwide **turnover**

02

Extended scope compared to NIS1, revising how companies are classified and requiring **more of them** to comply with its directives

03

Senior management is **liable** for infringements, and authorities may **suspend activities or performance of their role**

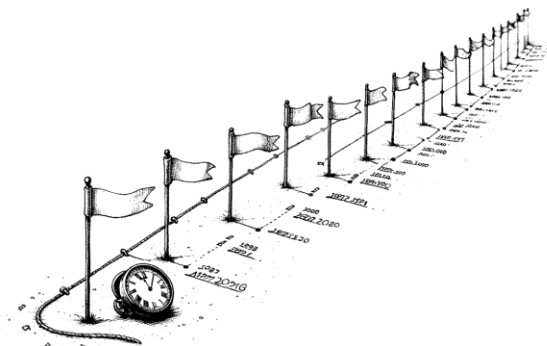
04

Extensive **security risk-management measures**, and a shift to a risk-based approach

05

Initial reporting of **security incidents within 24h**, follow-up **within 72h**, and final/ongoing reporting **within 1 month**

TIMELINE



Dec 2020

- **Proposal** by the European Commission for an update of NIS1, called the **NIS2 directive**

Jan 16th, 2023

- **In force**, 20 days after announcement in the Official Journal

Oct 17th, 2024

- **Deadline for implementation** into national law by Member States

Jan 17th, 2025

- CSIRTs network shall **assess progress** made regarding operational cooperation

Oct 17th, 2027

- **Revision** of the Directive

Dec 2022

- **Adoption** of NIS2 by the EU Parliament and Council

Jul 17th, 2024

- First Cyber Crises Liaison Organization Network (**EU-CyCLONe**) report

Oct 18th, 2024

- **Application** by the Member States

Apr 17th, 2025

- Member States shall establish a **list of essential and important entities**




















Insert Web P















This app allows you to insert se
web pages are not supported f

NIS2 IMPROVEMENTS & NOVELTIES

	Increase of sectoral scope	Hardening expectations for cyber resilience and incident response	Expansion of sanctions	Enhancement of EU cyber crisis cooperation
NIS 1	<p>Several sectors of Operators of Essential Services (OSE) & Digital Service Providers (DSP)</p> <p>30 types of entities</p>	<p>Risk-based approach, with no obligation of prior compliance to the directive</p>	<p>Sanctions TBD by Member States</p>	
NIS 2	<p>Sectors of high criticality and critical sectors</p> <p>67 types of entities</p> <p>Inclusion of SMEs under certain criteria</p> <p>Inclusion of Supply Chain</p>	<p>Ex ante audits by authorities</p> <p>Incident notification in 24h and a more detailed report in 72h</p> <p>Clear responsibility matrix across all entities and supply chain</p> <p>Supply chain compliance</p> <p>Risk management TOMs (technical & organizational measures) covering multiple areas</p>	<p>10 mil. EUR or 2% of turnover for Essential Sectors</p> <p>7 mil. EUR or 1.4% of turnover for Important Sectors</p> <p>Suspension of certifications or pending authorizations</p> <p>Criminal sanctions</p> <p>Temporary ban on management positions</p>	<p>Creation of the Cyber Crisis Liaison Organization Network (EU-CyCLONe)</p>

WHICH SECTORS DOES NIS2 COVER? (ANNEX 1 & 2)

Essential business sectors											
Energy  Electricity  Gas  Oil  Hydrogen  District heating and cooling					Transport  Air  Rail  Water  Road				Health  Healthcare providers  Pharmaceutical industry		Space 
Drinking water 	Waste water 	Public administration 	Digital infrastructure 	Banking 	Financial market infrastructures 	ICT service management (B-to-B) 					

Important business sectors							
Postal and courier services 	Waste management 	Digital providers  Online marketplaces  Online search engines  Social networking services platforms			Chemicals  Manufacture, production and distribution	Food  Production, processing and distribution	Research 
Manufacturing  Manufacture of medical devices and <i>in vitro</i> diagnostic medical devices  Manufacture of computer, electronic and optical products  Manufacture of electrical equipment  Manufacture of machinery and equipment n.e.c.  Manufacture of motor vehicles, trailers and semi-trailers  Manufacture of other transport equipment							

 Sectors added by NIS 2 directive

WHICH ORGANIZATIONS ARE IMPACTED BY NIS2?

Size of the entity	Number of employees	Revenue (mil. EUR)	Balance sheet (mil. EUR)	Sectors of high criticality	Other critical sectors
Intermediate and large	$y \geq 250$	$y \geq 50$	$z \geq 43$	Essential Entities	Important Entities
Medium	$50 \leq x < 250$	$10 \leq x < 50$	$10 \leq z < 43$	Important Entities	Important Entities
Micro and small	$x < 50$	$y < 10$	$z < 10$	Not concerned*	Not concerned*

*There are some **exceptions to the rule**, where entities such as, for example, qualified trust service providers, public administration, “sole providers”, top-level domain name registries as well as DNS service providers, **can be designated as essential regardless of the size of their organization** - see Article 3(1)



NIS2 – REQUIREMENTS FOR ORGANIZATIONS



MANAGEMENT

It is necessary for management to **be aware** of and **understand** the requirements of the directive and the risk management efforts.

They have a **direct responsibility** to identify and address cyber risks to comply with the requirements.

REPORTING

Organizations need to have **established processes** for ensuring proper **reporting to authorities**.

There are **requirements**, for example, that **major incidents** should be reported within 24 hours.

RISK MANAGEMENT

To meet the new requirements, organizations must implement measures to **minimize risks and consequences**.

This includes, for example, incident management, improved supply chain security, network security, access control, and encryption.

BUSINESS CONTINUITY

Organizations must consider how to ensure **business continuity** in the event of major cyber incidents.

This includes, for example, system recovery, emergency procedures, and establishment of a crisis response team.

CYBERSECURITY RISK-MANAGEMENT MEASURES (ART. 21)

1. MFA and Authentication Solutions

2. Strategy and Governance

3. Incident Handling

4. Risk Management

5. Supply Chain Security

6. Training and Awareness

7. Access Control and Asset Management

8. Crisis Management

9. Cryptography and Encryption

10. Business Continuity and Disaster Recovery

EXAMPLE: TECHNICAL AND ORGANIZATIONAL MEASURES



REPORTING INCIDENTS (ART. 6 & 23)

■ Significant security incident

- Serious (possible) **disruption of services** or **financial losses**
- Other natural or legal persons have been or may be adversely affected by **substantial material or immaterial damage**

■ Reporting deadlines

- **24 hours:** Early warning
- **72 hours:** Update of the early warning and initial assessment of the security incident
- **Intermediate:** Upon request and concerning relevant status updates
- **1 month:** Final report (detailed description, root cause analysis, mitigations, cross-border impact)



WHAT HAPPENS IF YOU DON'T COMPLY? (ART 33-34)

- Authorities are given **broad inspection powers**
 - On-site inspections, security audits, instructions or orders
- **Essential entities:**
 - **Fines of EUR 10 mil.** / max of **2%** of total worldwide annual turnover
 - **Management Accountability:** potential discharge of C-Suite managerial functions (temporary exclusion of management from its duties)
 - **Suspension of certifications/authorizations** concerning (part or all of) the services or activities provided by the essential entity
- **Important entities:**
 - **Fines of EUR 7 mil.** / max of **1.4%** of total worldwide annual turnover



WHAT'S NEXT?

- Determine if your **business is impacted** by NIS2
- Raise NIS2 awareness with **senior management**
- **Educate** management about cybersecurity risks
- Estimate **expenses** and plan **budget**
- Review **NIS2 cybersecurity risk management** measures
- Assess your **supply chain**
- Simplify **incident reporting**
- Develop **business continuity** and **crisis management** plan
- **Implement an Information Security Management System** as per NIS2 criteria
 - ISO 27001 covers about 70% of the NIS2 requirements
- Ensure **secure development** practices



WHAT'S NEXT, REALLY?

- *“You don't have to run faster than the bear to get away. You just have to run faster than the guy next to you.” (Jim Butcher)*



A 3D maze structure made of dark blue blocks with glowing cyan edges, set against a dark blue background with glowing yellow and orange circuit lines and dots. The maze is circular with a complex, winding path.

EU CYBER RESILIENCE ACT

BONUS 



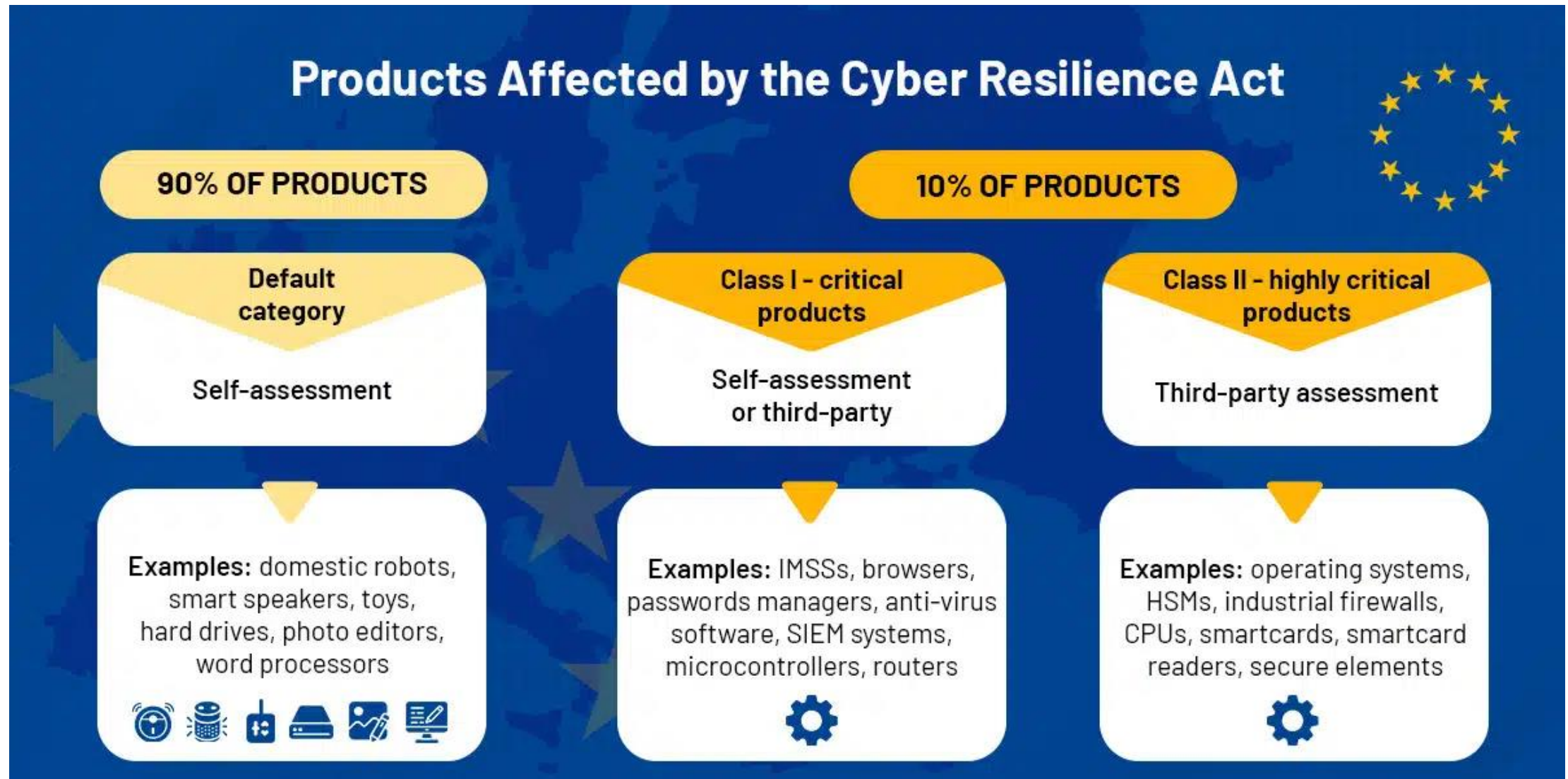
“If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces[...] This is why we need a European cyber defence policy, including legislation setting common standards under a new European Cyber Resilience Act.”

(Ursula von der Leyen, European Commission President)

CYBER RESILIENCE ACT

- **Cybersecurity regulation on a broad scale**, applicable to all products with digital elements
- Intended or reasonably foreseeable use includes a **direct or indirect logical or physical data connection to a device or network**
 - Any **software or hardware product** and **related Cloud solutions**
 - **Software and hardware components** placed on the market separately
- Also so-called “**critical products with digital elements**”
 - Divided into **two risk classes** (class I and class II)
 - Special conformity procedure

HOW THE CRA WILL WORK IN PRACTICE



CYBER RESILIENCE ACT: ADDRESSEES

Manufacturers	Importers	Distributors
<p>Any natural or legal person who develops or manufactures digital products.</p> <p>Also, natural or legal persons who have digital products designed, developed or manufactured and distribute them under their name or trademark.</p>	<p>Any natural or legal person established in the Union who places on the market a product with digital elements that bears the name or trademark of a natural or legal person established outside the Union.</p>	<p>Any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties.</p>

CYBER RESILIENCE ACT: MAIN REQUIREMENTS

Assess cyber risks prior to market launch

Monitor products for their entire life cycle

Provide **free security updates**

Reporting obligations in case of **security incidents**

Extensive **documentation**

Requirements (among others):

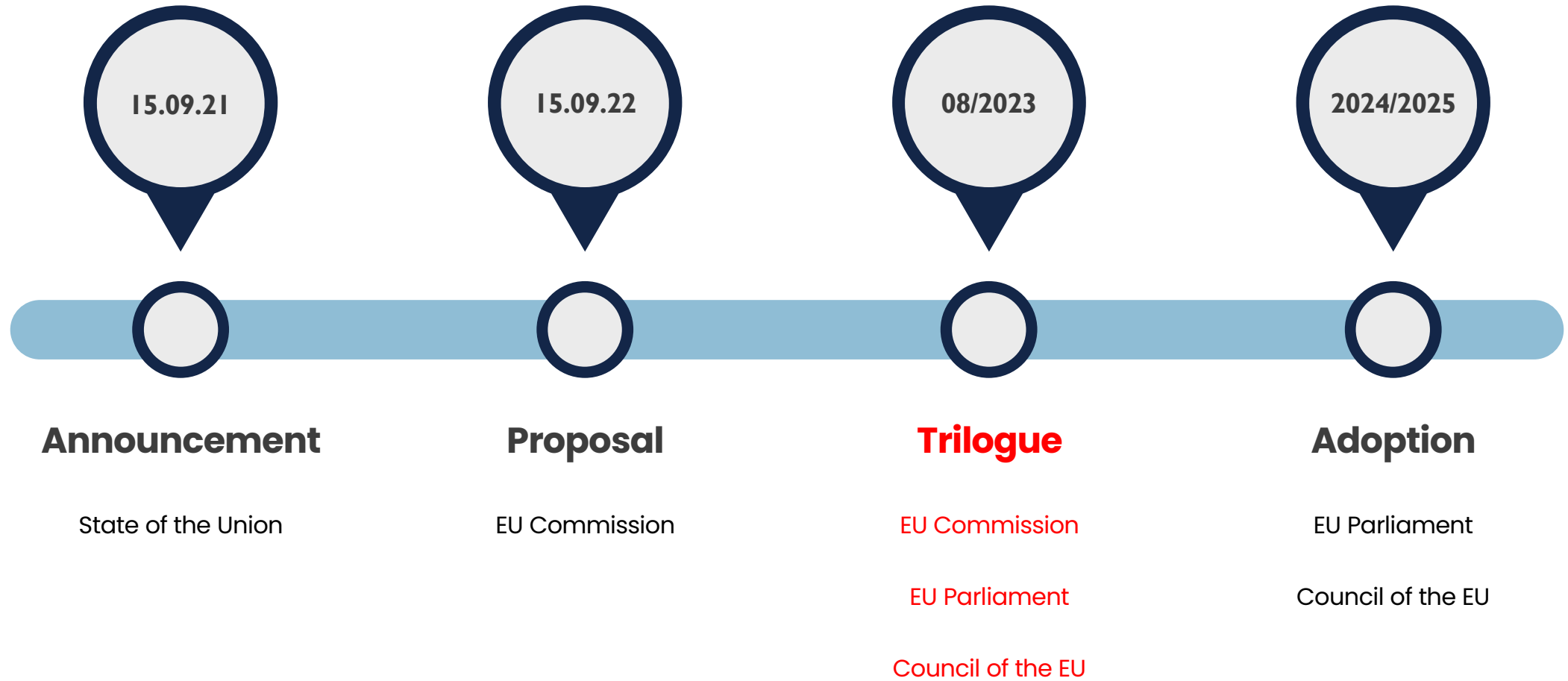
- Only placing of products with **CRA conformity** on the market
- **Additional information** requirements (especially contact information)
- In case of **non-compliance with CRA**: withdrawal/recall
- In the case of vulnerabilities, **notify relevant market surveillance authorities** in the Member States

CYBER RESILIENCE ACT: SANCTIONS AND FINES

- Authorities are given **broad inspection powers**
 - On-site inspections, security audits, and instructions or orders
- **Sanction measures:**
 - In case of inadequate action or non-action by the manufacturer: **prohibition of the product distribution** possible
 - **Fines up to 15 mil. EUR** or up to **2.5% of the total worldwide annual turnover** in the preceding fiscal year
 - Multiple fines for the **same infringement** not excluded



CYBER RESILIENCE ACT: ROADMAP



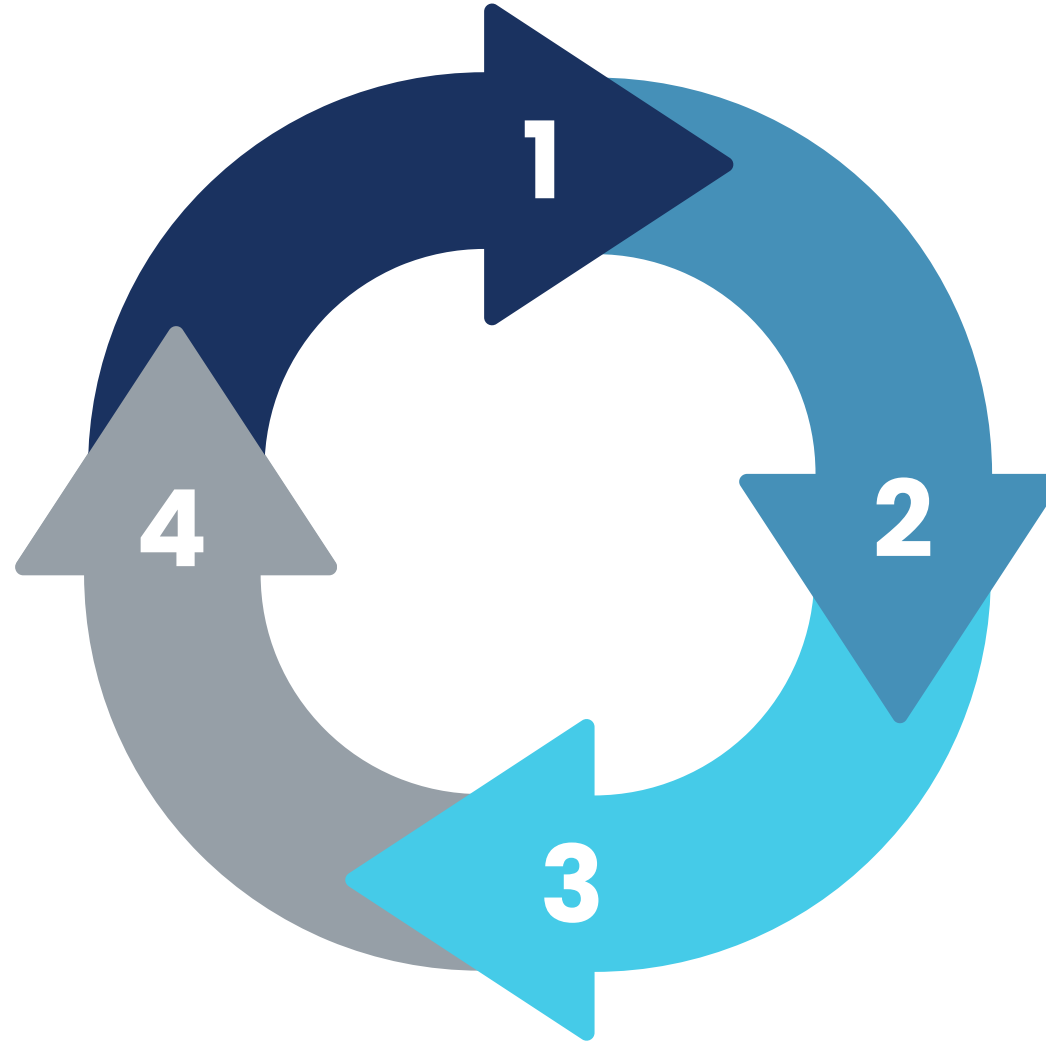
BEST PRACTICES: CYBERSECURITY COMPLIANCE MANAGEMENT

1 – Check Affectedness

Legislation
Norms and standards
Guidelines & recommendations

4 – Monitoring

Internal processes
Business model
Legal situation



2 – Derive Specifications

Technology
Organization
Processes

3 – Implementation

Risk assessment
Corrective measures
Documentation

WHY YOU SHOULD START PREPARING FOR NIS2 / CRA NOW

- You will **save costs**
- Compliance **takes time**
- **A lot of people** are involved
- You will **avoid potential penalties**
- You can **get peace of mind**
- Contribute to **national security**
- You can **avoid operational disruptions**





THANK YOU!

CONTACT ME: TUDOR.DAMIAN@D3CYBER.EU | TUDY.RO