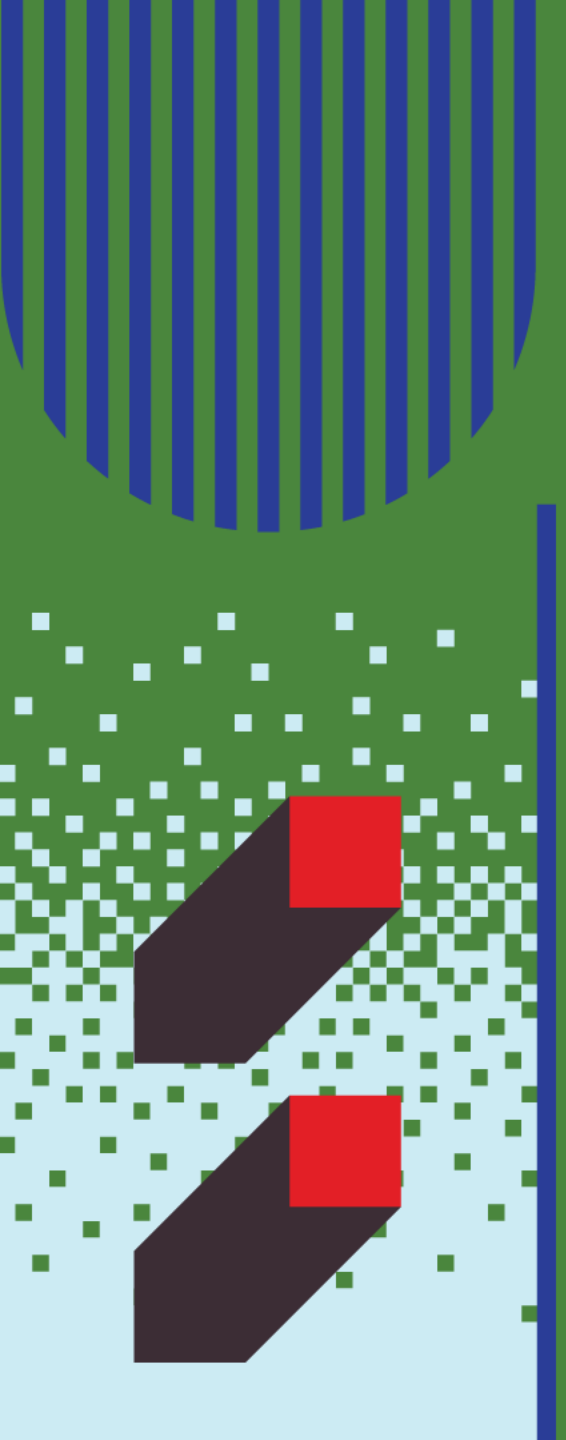


IAPP Global Summit 2026

Privacy | AI governance | Cybersecurity law

Conference 30-31 March

Workshops 1 April

Training 1-2 April

WASHINGTON, DC

#IAPPSummit26

Cybersecurity Compliance in Europe: Lessons Learned from the First Year

Corey Dennis
Assistant General Counsel & Chief Privacy Officer
Legend Biotech

Jim Dempsey
Lecturer, UC Berkeley Law; Managing Director, Cybersecurity Law Center
IAPP

Dr. Natallia Karniyevich
Partner
McDermott Will & Schulte

Devon Ackerman
Global Head, Digital Forensics and Incident Response
LevelBlue

Agenda

1. European cybersecurity legislation - regulatory overview

2. NIS2 Directive

- Latest developments

- Key elements

- Assessment of applicability

3. Critical Entities Resilience (CER) Directive

4. Digital Operational Resilience Act (DORA)

5. Cyber Resilience Act (CRA)

6. Practical steps to prepare for NIS2 (and CRA, CER & DORA)

European cybersecurity legislation (1/2)

Regulatory overview

2016

Network and Information Systems (NIS) Directive – "*Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security … appropriate to the risk posed.*"

2018

General Data Protection Regulation - Art. 32, appropriate technical and organisational security measures to ensure … security appropriate to the risk; Art. 33, breach notice to authorities; Art. 34, breach notice to data subjects

2019

EU Cybersecurity Act – authorizes ENISA and framework for voluntary certification of ICT products, ICT services and ICT processes

2022

Radio Equipment Directive (RED) Delegated Act – security of mobile phones and other devices

European cybersecurity legislation (2/2)

Regulatory overview

2023

- Network and Information Systems Directive 2 (NIS2)
- Directive on the resilience of critical entities (CER)
- Regulation on digital operational resilience for the financial sector (DORA)

2024

- NIS2 national implementations
- CER national implementations
- NIS2 Commission Implementing Regulation
- Cyber Resilience Act (CRA) – EU-wide cybersecurity requirements for products (hardware and software)

2025 / 2026

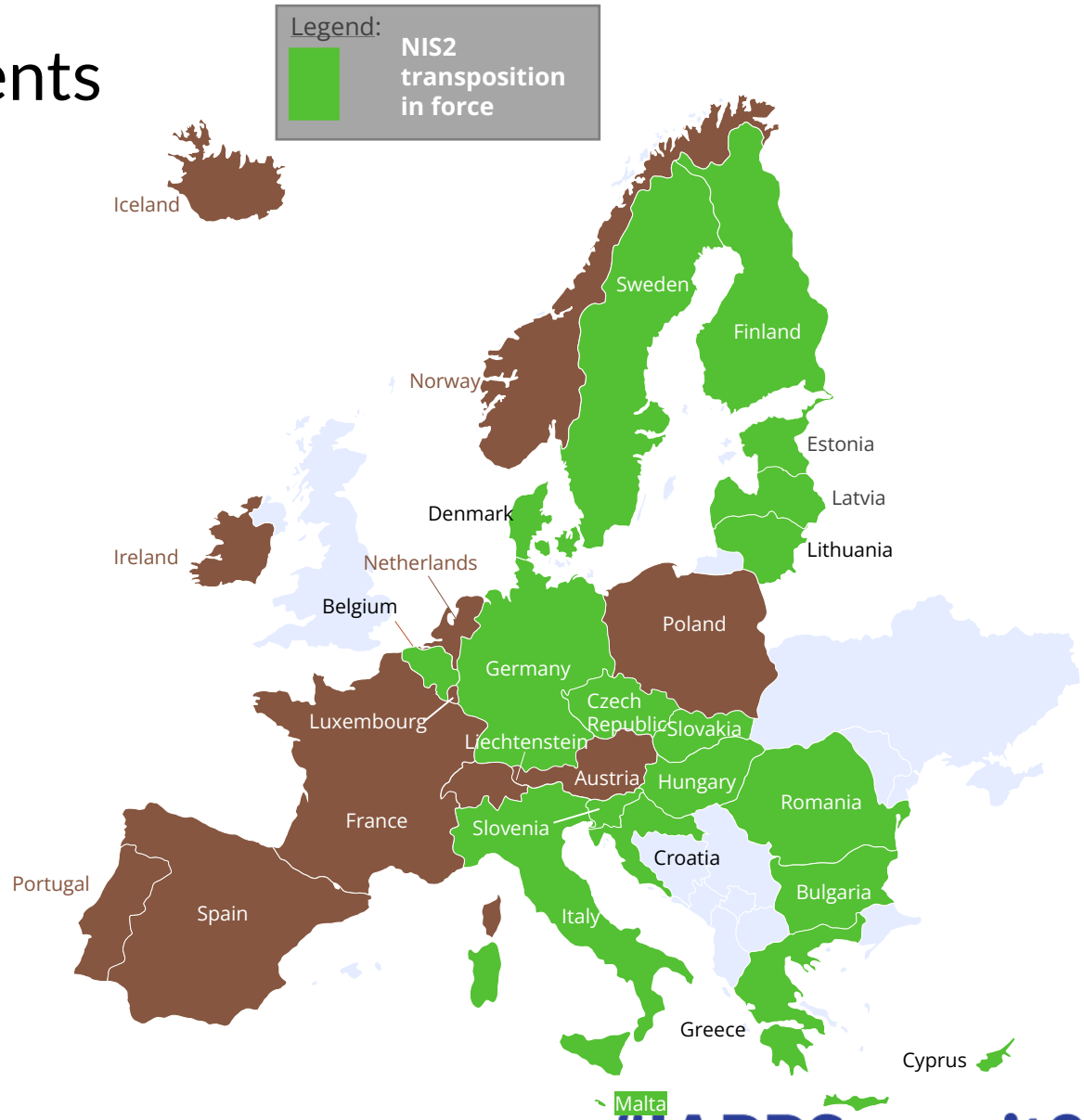
- NIS2 national implementations
- CER national implementations
- Digital Omnibus proposal
- Data Union Strategy
- European Business Wallet proposal

NIS2 Directive – Latest developments

Transposition is underway (deadline was 17 Oct. 2024)

In 20 European countries, NIS2 implementing legislation is already in force

Additional measures to ensure a higher level of cybersecurity may be adopted or maintained, provided they remain consistent with applicable law



NIS2 Directive – Key elements

- Enforcement: Member States must ensure that their regulatory authorities have the power to issue binding orders and conduct onsite inspections and audits
- Obligations: Risk management measures of covered entities must include specific elements (audit, supply chain security, training, etc.)
- Incident reporting requirements
- Companies must align compliance with other regulatory obligations (e.g., CER, GDPR)
- Service providers and vendors need to facilitate compliance of covered entities
- Trend towards mandatory deployment of certified ICT products, ICT services and ICT processes

What sectors are covered by NIS2?

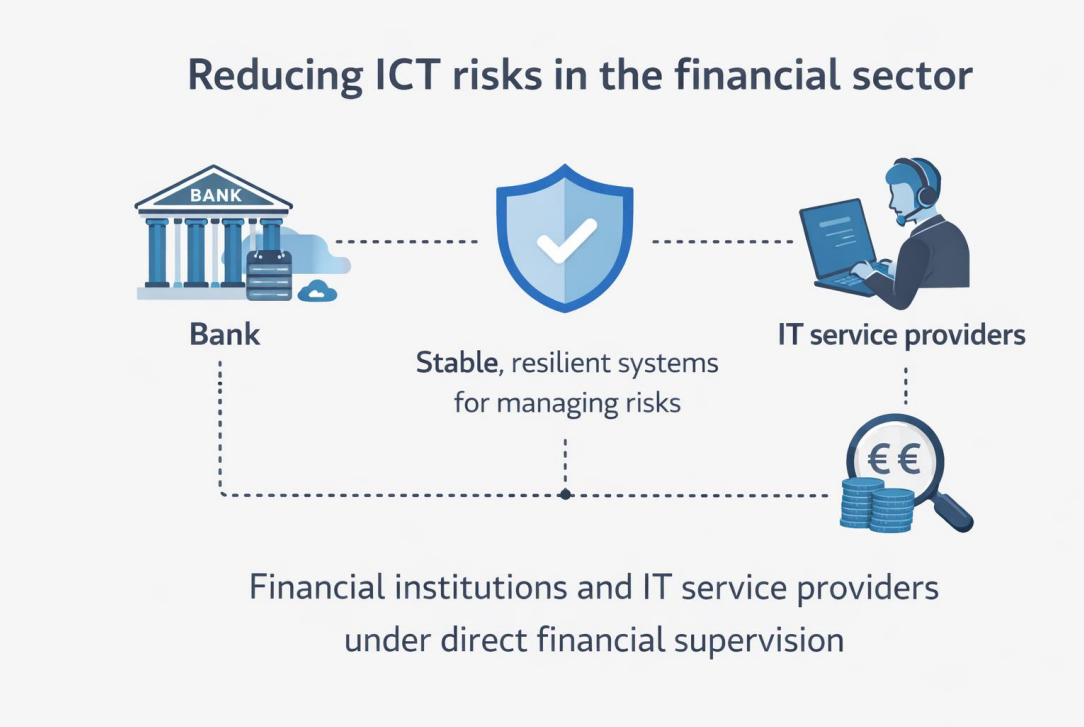
Distinction between essential entities and important entities. Both have same obligations, but essential entities face higher fines and ex ante supervision.

Critical Entities Resilience (CER) Directive – Key elements

- All hazards (natural or man-made, accidental or intentional)
- Applies to "*critical entities*" providing essential services
  - Essential services identified by the Commission
  - Critical entities determined by national authorities
- Critical entities must take appropriate and proportionate technical, security and organizational measures to ensure their resilience
- Entities identified as critical entities under CER Directive should be considered essential entities under NIS2 Directive.
  - NIS2 defines the cyber obligations of those entities.

DORA (Digital Operational Resilience) – Key elements

- Effective Jan 2025. Intended to address operational risks stemming from all types of ICT services within the financial sector.
- Further regulatory guidance in Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS). Some RTSs and ITSs are in force; others are still pending.
- Directly applicable, EU-wide regulation, but each member state designates regulatory authority in national law (Competent Authorities).
- Applies to EU financial institutions and their ICT service providers (see Art. 2):
  - Banks
  - Insurers
  - Payment and e-money institutions
  - Investment firms
  - Crypto-asset service providence.



CRA (Cyber Resilience Act) - Key elements (1/2)

Mandatory cybersecurity requirements for products with digital elements (hardware and software), throughout their whole lifecycle

Enable end users to have sufficient information about the cybersecurity of the products they buy and use

Does not apply to medical devices, aviation or cars for which cybersecurity requirements are already in place

Increase the responsibility of manufacturers by obliging them to provide security support and software updates

Report vulnerabilities and incidents

Applies to all products that are connected either directly or indirectly to another device or network

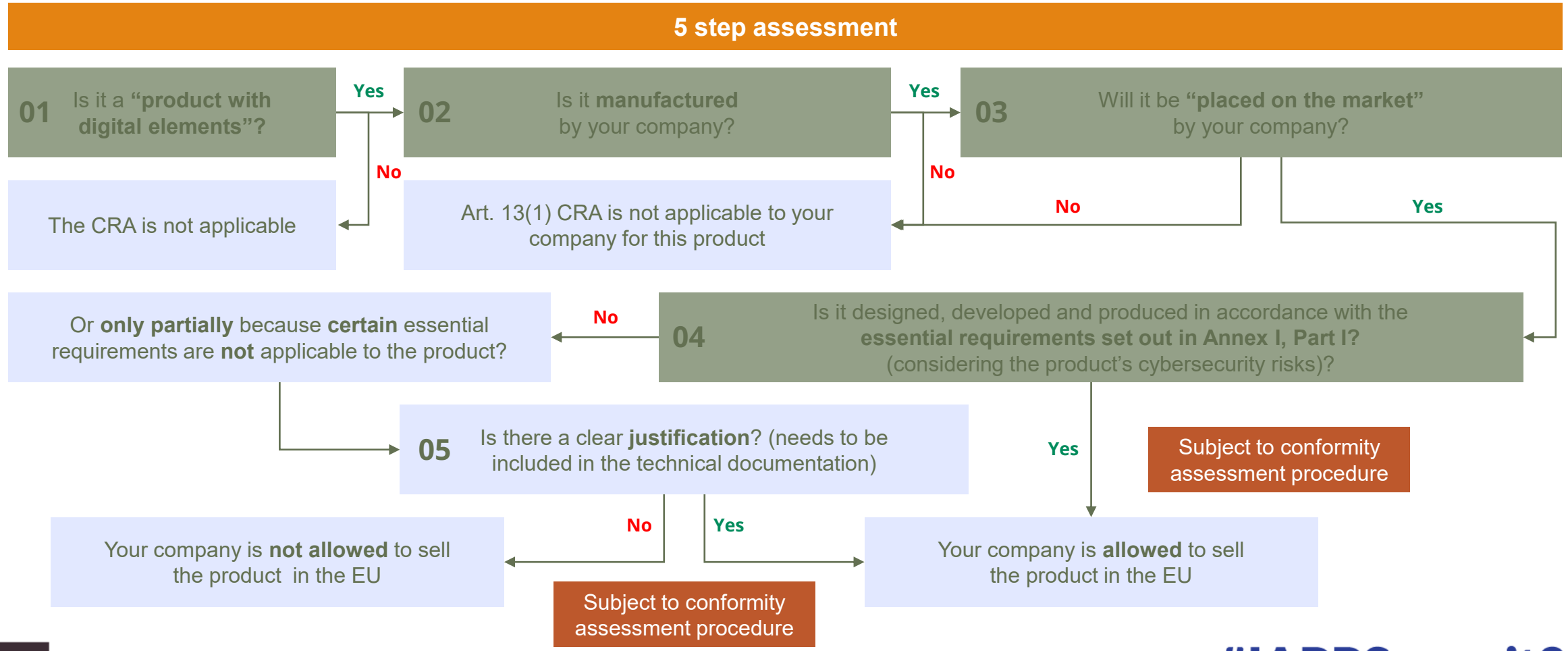
Rules on market surveillance and enforcement on Member State level

Maximum harmonization, however:

- Member States may subject products with digital elements to additional cybersecurity requirements for the procurement or use of those products for specific purposes
- For example, purchasing hardware or software for government agencies for military, defence or national security purposes.

Cyber Resilience Act (2/2)

Are your company's products CRA-ready?



Practical Steps to Prepare for NIS2 (and CRA, CER & DORA)

Don’t wait for the national laws, act now.

Determine

- The services/ products and entities within scope
- Jurisdictions of interest
- Consequent actions

Update

- Policies & procedures
- Incident response plans
- Training
- Vendor due diligence & procurement
- Risk register

Manage obligations

- Contracts with customers and vendors
- Risk at management level
- Regulator relationships
- Insurance

Maintain

- Monitor developments
- Appropriate governance
- Interplay with other laws (e.g., GDPR, CER, CRA)

NIS2 - Security obligations

Technical, operational and organizational measures (Art. 21)

- **Appropriate and proportionate measures** to manage the risks related to the services, and to prevent or minimize the impact of incidents
- **All-hazards** approach
- NIS2 specifies **10 kinds of measures**, including vulnerability disclosure, training, access control, and MFA
- Emphasis on **supply chain security**
- EC has adopted an **implementing regulation** with further details on these obligations for specific providers, including cloud computing service providers, data center service providers, managed service providers and providers of online marketplaces

- **Cybersecurity certifications**: Member States or EC may require use of certified ICT products, services, or processes
- The Cooperation Group can carry out coordinated security risk assessments of specific supply chains of critical ICT services/ systems/ products
- **ENISA technical implementation guidance**

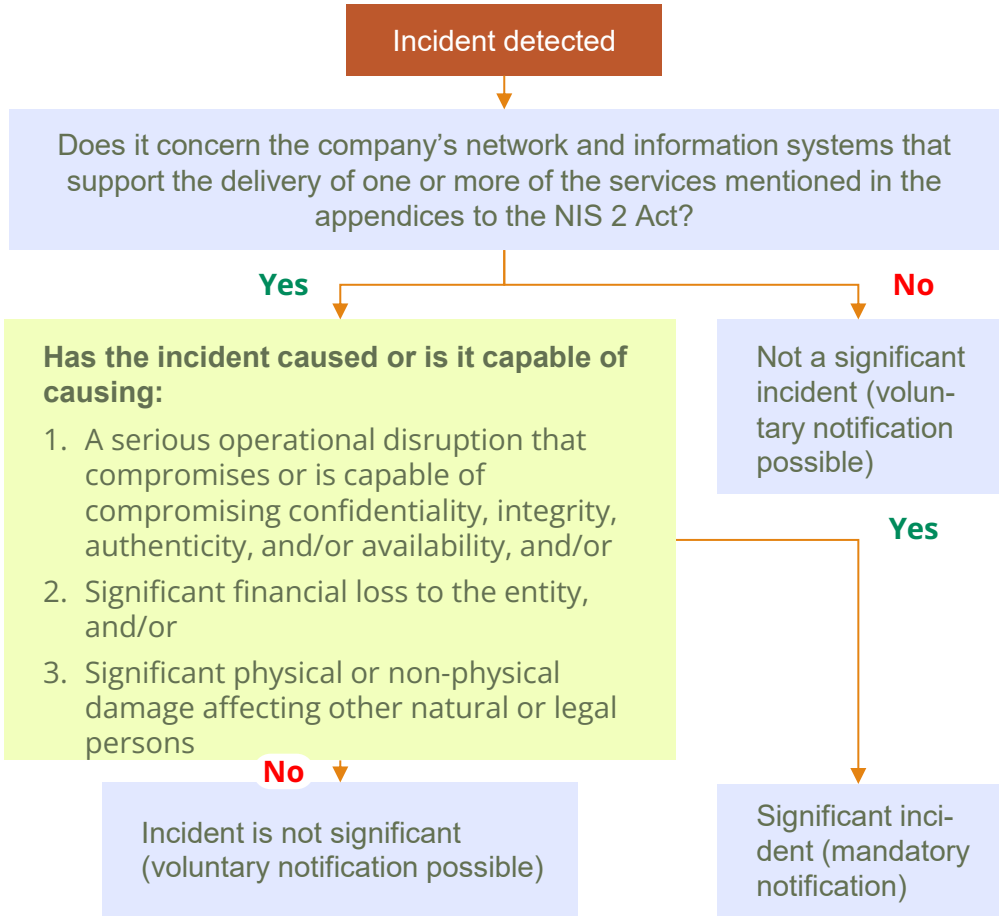
NIS2 - Reporting obligations (1/2)

CSIRT, competent authorities, recipients of the services (Art. 23)

- **Report to who?** CSIRT/ Competent authority
- **What?** Incident that has a significant impact on the provision of their services **(significant incident)**
- **When?**
  - **Early warning**: without undue delay and in any event within **24 hours** of becoming aware
  - **Incident notification**: without undue delay and in any event within **72 hours**
  - **Final report**: not later than **one month** after the notification

Also

- **Report to who?** Recipients of the services
- **What?**
  - **Significant incidents** that are likely to adversely affect the provision of those services
  - **Significant cyber threat** and suggested measures or remedies in response to such threat
- **When?** Without undue delay



NIS2 - Reporting obligations (2/2)

CSIRT, competent authorities, recipients of the services (Art. 23)

24 hours

Early warning

Is it a suspected malicious act with potential cross-border impacts?

72 hours

Official incident notification

Assessment of the incident, severity and impact, plus indicators of compromise

Intermediate status report

At the request of CSIRT or relevant competent authority

1 month

Final report

Or, if incident ongoing at time of final report, a progress report and final report 1 month after end

May need to notify affected recipients.
May need to notify the public

European cybersecurity legislation

EU Digital Agenda

H1 2026

- Cybersecurity Package
- Cloud & AI Development Act (CADA)
- Chips Act 2.0
- Digital Networks Act (DNA)
- European Research Act
- European Innovation Act

H2 2026

- Digital Fairness Act (DFA)
- Audiovisual Services Media review
- Public procurement reform
- Digital Markets Act evaluation
- Encryption Tech Roadmap
- Quantum Act

Resources

- NIS2 text https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02022L2555-20221227&qid=1728321105522
- ENISA, NIS2 Technical Implementation Guidance https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
- NIS2 Commission implementing regulation on critical entities and networks https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks
- Cyber Resilience Act (CRA) text https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
- IAPP, EU NIS2 Directive101 https://iapp.org/media/pdf/resource_center/nis2-directive-101-chart.pdf
- IAPP Incident Notification and Information Sharing Requirements: EU Digital Law https://iapp.org/resources/article/incident-notification-requirements-eu-laws
- IAPP, Digital Services Act: Mapping the Interplays with the GDPR https://iapp.org/resources/article/mapping-interplays-gdpr-dsa
- IAPP, Data Act: Mapping the Interplays with the GDPR https://iapp.org/resources/article/mapping-interplays-gdpr-data-act

HAVE A QUESTION?

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Summit 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all questions, tap "Done".

Thank you!