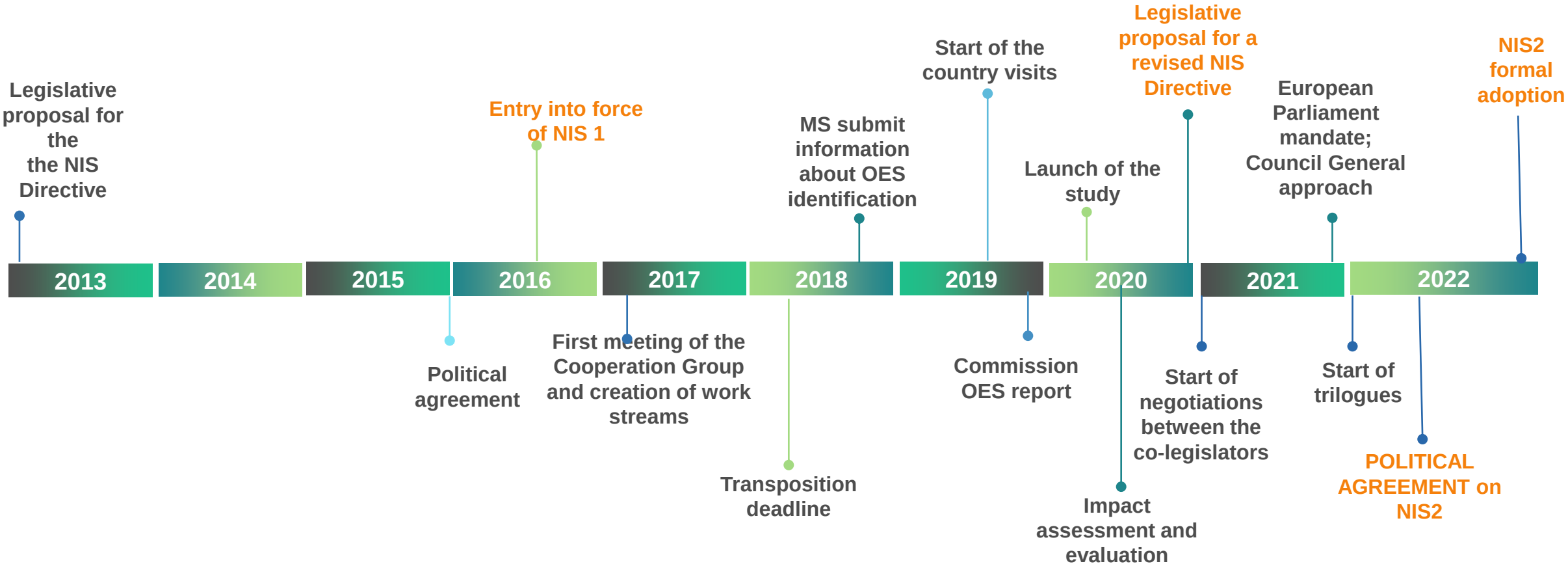
Latest EU cybersecurity legislative initiatives– NIS 2 and CRA

Boryana Hristova-Ilieva, Legal officer
Unit H2 – Cybersecurity and digital privacy policy
DG CONNECT, European Commission

NIS 2 Directive: state of play

Timeline of the NIS Directive



European Commission

Main challenges of NIS 1

Not all sectors that may be considered critical are in scope

Great inconsistencies and gaps due to the NIS scope being *de facto* defined by MS (case by case OES identification)

Diverging security requirements across MS

Diverging incident notification requirements

Ineffective supervision and limited enforcement

Voluntary and ad-hoc cooperation and info sharing between MS and between operators

Three main pillars of the proposal for NIS 2

MEMBER STATE CAPABILITIES

National authorities

National strategies

Coordinated Vulnerability Disclosure (CVD) frameworks

Crisis management frameworks

RISK MANAGEMENT & REPORTING

Size threshold

Accountability for top management for non-compliance

Entities are required to take cybersecurity risk management measures

Entities are required to notify incidents

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability database

Peer-reviews

Biennial ENISA cybersecurity report

European Commission

Which sectors are covered?

Annex I	Annex II
Energy (electricity (incl. new categories of operators such as electricity producers, nominated market participants, operators of recharging points), district heating and cooling, oil (incl. central stocktaking entities), gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	RESEARCH **
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, Content Delivery Networks, electronic communications, trust service providers,)	
ICT Service management**	
Public administration entities	
Space	

** additional sectors or sub-sectors agreed by the co-legislators

European Commission

Two regulatory regimes

	Essential entities	Important entities
Security requirements	Risk-based security obligations, including accountability of top management	
Reporting obligations	Significant incidents	
Supervision	Ex-ante + ex post	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines. Only for essential entities*: ultima ratio* possibility to suspend authorisation or impose temporary ban on managerial duties	
Jurisdiction	General rule: MS where the entities are established Exception: telcos - MS where they provide services; Certain digital infrastructures and digital providers – main establishment in the Union.	

More harmonised security requirements & incident reporting

- Accountability for top management for non-compliance with cybersecurity risk management measures
- Risk-based approach: appropriate and proportionate cybersecurity measures
- Defining a minimum set of measures

(such as risk analysis and information security policy, incident handling, business continuity, supply chain security)

- Reporting of significant incidents
- MS to inform each other and ENISA of incidents with cross-border nature

NIS 2 and SMEs

- Size threshold
- Proportionality: Risk-based approach, supervision and enforcement rules
- Member States to address SME needs in national strategies.

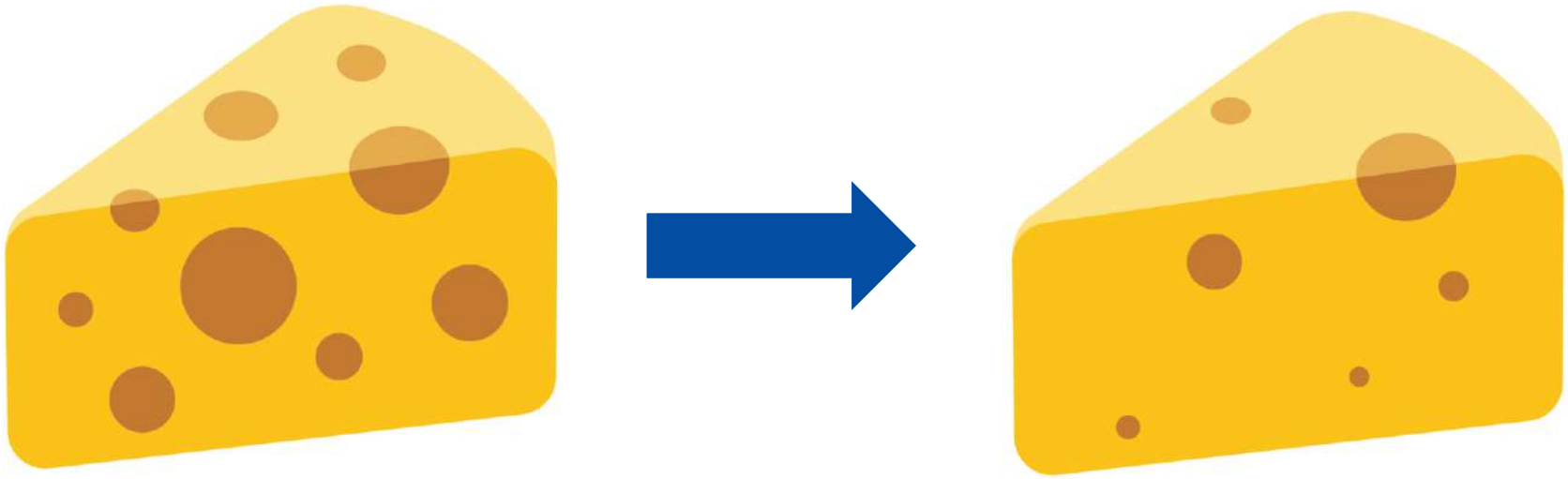
Cyber Resilience Act

Impact of security incidents

- Average cost of a data breach for individual businesses was **EUR 3.5 million in 2018**.
- Statistically speaking, **every 11 seconds** another organisation is hit by a ransomware attack.
- In 2021 alone cybercriminals were able to leverage hacked devices and **launch 9.75 million DDoS attacks** worldwide.
- **57 % of SMEs** say they would go out of business in the event of a cybersecurity attack.
- The aggregate cost of security incidents affecting businesses in Germany amounts to **EUR 220 billion in 2020**.
- **Two thirds** of NIS incidents are the result of a **vulnerability exploitation**. (Other causes are phishing, credential theft etc.)

Sources: Ponemon Institute, Cybersecurity Ventures, Netscout, ENISA, Bitkom

CRA in a nutshell



European Commission

Main elements of the proposal

- **Cybersecurity rules** for the placing on the market of hardware and software
- Based on **New Legislative Framework** (well-established EU product-related legislative setting)
- **Obligations** for manufacturers, distributors and importers
- Cybersecurity **essential requirements** across the life cycle (5 years)
- Harmonised **standards** to follow
- **Conformity assessment** – differentiated by level of risk
- **Market surveillance and enforcement**

Scope

Products with digital elements:

- ✚ **Hardware products** and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- ✚ **Software products** and components placed on the market separately, such as operating systems, word processing, games or mobile apps
- ⓘ The definition of **“products with digital elements”** also includes **remote data processing solutions.**

Not covered:

- ✖ **Non-commercial projects, including open source** in so far as a project is not part of a commercial activity
- ✖ **Services, in particular cloud/Software-as-a-Service** – *covered by NIS2*

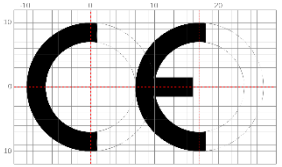
Outright exclusions:

- ✖ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment) under the new and old approach

Obligations of manufacturers

Assessment of the risks associated with a product

(1) Product-related essential requirements (Annex I, Section 1)
(2) Vulnerability handling essential requirements (Annex 1, Section 2)
(3) Technical file, including information and instructions for use (Annex II + V)



Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:

(1) exploited vulnerabilities
(2) incidents having an impact on the security of the product

Reporting obligations to continue

European Commission

Product-related essential requirements

1. Appropriate level of security
2. Products to be delivered without known vulnerability
3. Based on the risk and where applicable:
    - Security **by default**
    - Protection from **unauthorised access**
    - **Confidentiality** and **integrity of data**, commands and programs
    - **Minimisation** of data
    - Availability of **essential functions**
    - Minimise **own negative impact** on other devices
    - Limit **attack surfaces**
    - Reduce **impact of an incident**
    - **Record and monitor** security relevant events
    - Enable adequate **security updates**

Vulnerability handling requirements

- **Identify and document dependencies** and vulnerabilities, including **SBOM**
- No known vulnerabilities and **address vulnerabilities** without delay
- **Test the security** of the digital product
- Publically **disclose information** about fixed vulnerabilities
- **Coordinated vulnerability disclosure** policy
- Facilitate the **sharing of information** about potential vulnerabilities
- Mechanisms allowing the **secure updating**
- Patches are delivered **without delay**, **free of charge** and with **advisory messages**

Information and instructions

- **CE marking**
- **Contact** information for reporting vulnerabilities
- **Intended use**, including the security environment foreseen
- Security **properties** of the product
- Where the **SBOM** can be accessed (if publicly available)
- EU **Declaration of Conformity**
- Type of **support offered** by the manufacturer and for how long
- Instructions on **secure use** and secure removal of data

Which conformity assessment to follow?

90% of products	10% of products		
Default category	**Critical "Class I"**	**Critical "Class II"**	**Highly critical**
Self-assessment	**Application of a standard or third party assessment**	**Third party assessment**	**Mandatory EU certification**
Criteria: **n/a**	**Criteria:** • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact)		**Additional criteria:** • Used by **NIS2** entities • Resilience of **supply chain**
	To be amended/specified via delegated acts		
Examples: Photo editing, word processing, smart speakers, hard drives, games etc.	**Examples (Annex III):** Password managers, network interfaces, firewalls, microcontrollers etc.	**Examples (Annex III):** Operating systems, industrial firewalls, CPUs, secure elements etc.	**Examples:** **n/a** (empowerment to future-proof the CRA)

Market surveillance powers and sanctions

- Tools for checks at the disposal of market surveillance authorities (MSAs): documentary checks, requests for information, inspections, laboratory checks etc.
- **When non-compliance found**, MSAs have powers to:

  1) require **manufacturers to bring non-compliance to an end** and eliminate risk;
  2) to **prohibit/restrict the making available** of a product or to order that the product is **withdrawn/recalled**;
  3) impose **penalties** (including fines up to 15 000 000 EUR or up to 2.5 % of worldwide turnover).

- In exceptional circumstances, COM may require ENISA to conduct an evaluation and, based on the results, establish a **corrective or restrictive measure is necessary at Union level** via an Implementing Act (and following MS consultations).

How will the CRA impact SMEs?

European Commission

Costs & benefits for SMEs

- 99% of the hardware manufacturers and software developers in the EU market
- Targeted outreach during preparatory phase of the proposal (impact assessment)
- Public consultation: Strong support for horizontal approach & level playing field with large companies

Costs & benefits for SMEs

Costs

- Compliance costs *(manufacturers)*
  - Secure product development costs
  - Testing
  - Third-party assessment
  - Documentation costs
  - Reporting
- Possible price increase *(users)*

Benefits

- Positive impact on **competitiveness** and **internal market** *(manufactures)*
- Reduction of **cybersecurity incidents** for businesses between 20 % and 33 % *(users)*
  - 90% of SMEs state that a cyber incidents would have a serious negative impact, for 57% possible bankruptcy (*ENISA survey*)

How will the implementation of the CRA be facilitated?

European Commission

A risk-based approach to the obligations

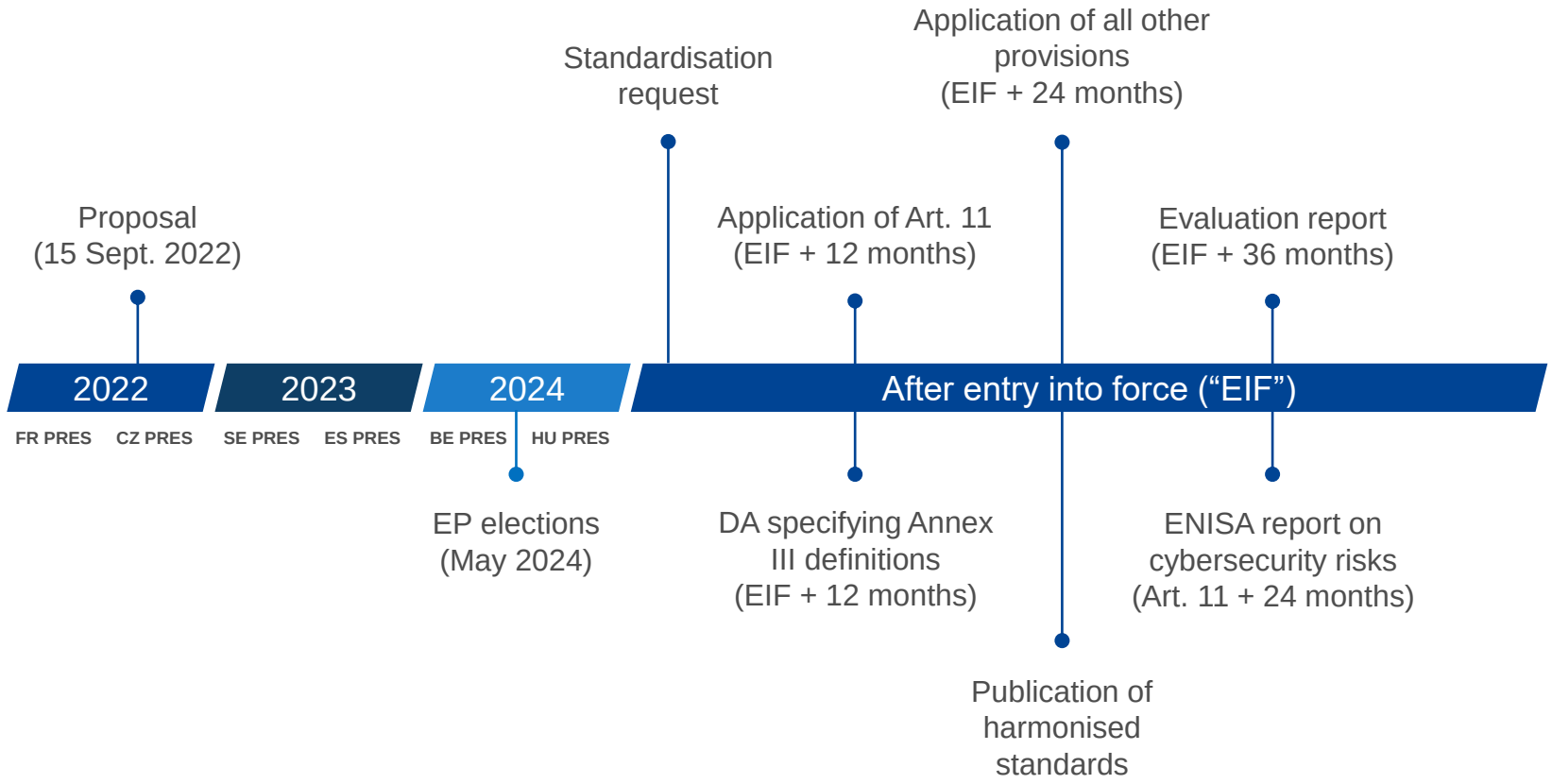
- Objective-driven, technology-neutral and risk-based essential cybersecurity requirements
- Conformity assessment (based on criticality)
- Interplay with other legislation to avoid duplication of regulatory burden
- Alignment with existing standards
  - **Harmonised standards** to be developed by ESOs – CEN / CENELEC / ETSI.
  - **Less burdensome compliance** when following Harmonised Standards : Presumption of conformity.
  - Building on **existing European, national, international standards**
  - Preparatory work has started : mapping, gap analysis …

Funding & guidelines

- Funding, e.g. training and awareness raising, sandboxes, automated compliance tools and supporting platforms
  - ✓ Horizon Europe, Digital Europe programme
  - ✓ Digital innovation hubs & National cybersecurity coordination centres

- Guidelines & templates by the Commission

Tentative timeline



European Commission

Thank you.