Bird & Bird

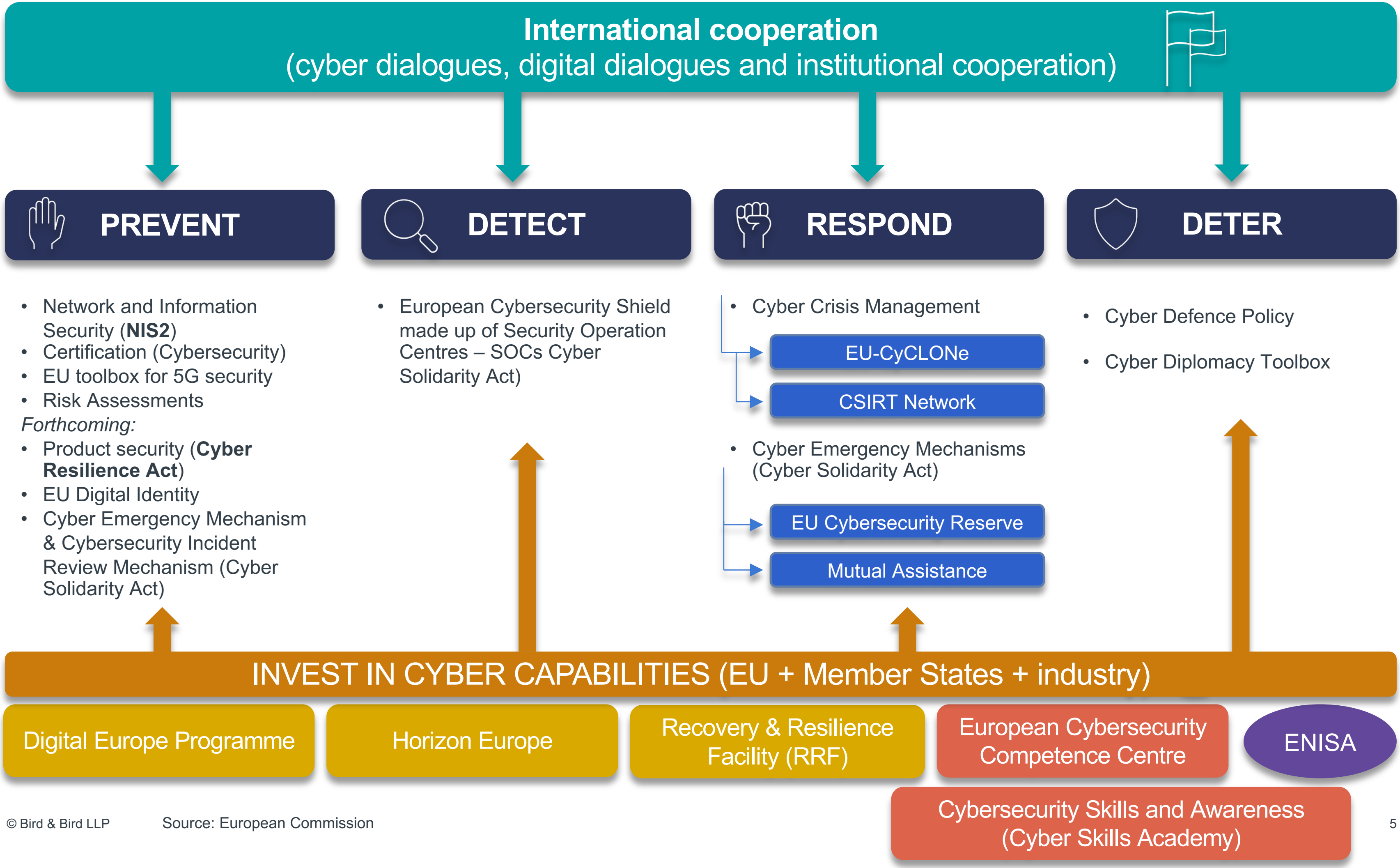
NIS2 and CRA

Current status and what companies need to do to prepare for toughened cybersecurity requirements

Head of EU Cybersecurity Group

Feyo.Sickinghe@twobirds.com

Craiyon - Your FREE AI image generator tool: Create AI art!



International cooperation

(cyber dialogues, digital dialogues and institutional cooperation)

PREVENT

- Network and Information Security (**NIS2**)
- Certification (Cybersecurity)
- EU toolbox for 5G security
- Risk Assessments

Forthcoming:

- Product security (**Cyber Resilience Act**)
- EU Digital Identity
- Cyber Emergency Mechanism & Cybersecurity Incident Review Mechanism (Cyber Solidarity Act)

DETECT

- European Cybersecurity Shield made up of Security Operation Centres – SOCs Cyber Solidarity Act)

RESPOND

- Cyber Crisis Management
  - EU-CyCLONe
  - CSIRT Network
- Cyber Emergency Mechanisms (Cyber Solidarity Act)
  - EU Cybersecurity Reserve
  - Mutual Assistance

DETER

- Cyber Defence Policy
- Cyber Diplomacy Toolbox

INVEST IN CYBER CAPABILITIES (EU + Member States + industry)

Digital Europe Programme

Horizon Europe

Recovery & Resilience Facility (RRF)

European Cybersecurity Competence Centre

ENISA

Cybersecurity Skills and Awareness (Cyber Skills Academy)

Source: European Commission

European cybersecurity legislation

Interplay

NIS2 Directive

Aims at ensuring a high level of cybersecurity of services provided by essential and important entities

Proposal for a Cyber Resilience Act

Focuses on products with digital elements (would also apply to radio equipment)

CER Directive

Focuses on reducing vulnerabilities and strengthening physical resilience of critical entities (=highly critical in NIS2)

Cybersecurity Act – provides an EU-wide cybersecurity certification framework for ICT products, services and processes

Proposal for a Cyber Solidarity Act – the actions proposed under this act cover situational awareness, information sharing, as well as support for preparedness and response to cyber incident

DORA – aims at ensuring secure operational resilience in financial services sector

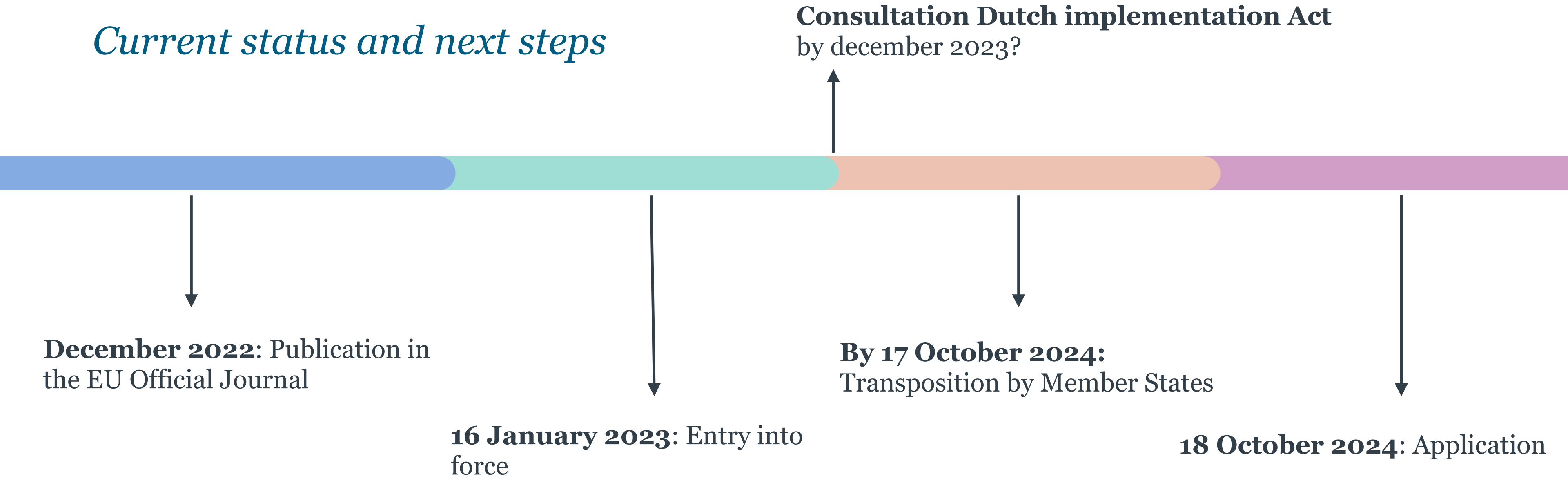
Other sector-specific legislation (e.g., telecomminication, automotive sectors, etc.)

01

NIS2 Directive

NIS2 Directive

Current status and next steps



December 2022: Publication in the EU Official Journal

16 January 2023: Entry into force

Consultation Dutch implementation Act
by december 2023?

By 17 October 2024:
Transposition by Member States

18 October 2024: Application

What will NIS2 change?

Key takeaways

- Replaces and extends the current NIS regime;
- Strengthens cybersecurity obligations
- Companies must align compliance with other regulatory obligations (e.g. CER, GDPR)
- Service providers and vendors will need to facilitate compliance
- Trend towards mandatory deployment of certified ICT products, ICT services and ICT processes
- Essential entities face higher fines than important entities, but the obligations are the same
- Articles 40 and 41 of the European Electronic Communications Code (EECC) will be withdrawn and the ECN/ECS will now be dealt with under the NIS2
- Member States supplement the NIS2 with additional national measures

Who is in scope under NIS2?

NIS2 modifies and expands the organisations that fall under the NIS Directive

- NIS2 eliminates the distinction between operators of essential services and digital service providers
- Size-cap rule: all medium and large enterprises fall within its scope
- Micro or small entities fulfilling specific criteria that indicate a key role for the economies or societies or for particular sectors or types of services are covered, either as essential or important entities
- All entities of the type listed in Annexes I and II which do not qualify as essential pursuant to paragraph 1 (≥ medium-sized enterprises and certain types of entities regardless of their size) are important entities
- Member States must produce a list of essential and important entities

Who is in scope under the NIS2?

NIS 1 Annex II - Operators of Essential Services	NIS 2 Annex 1 - *SECTORS OF HIGH CRITICALITY*
1. Energy: electricity, oil, gas	1. Energy: electricity, district heating and cooling, oil, gas, hydrogen
2. transport: air, rail, water, road	2. Transport: air, rail, water, road
3. Banking	3. Banking
4. Financial market infrastructures	4. Financial market infrastructures
5. Health	5. Health
6. Drinking water supply and distribution	6. Drinking water
7. Digital infrastructure: IXPs, DNS service providers, TLD name registries	7. Waste water
	8. Digital infrastructure: IXPs, DNS service providers***, excluding operators of root name servers,*** TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, trust service providers, providers of public electronic communications networks and/or services
NIS 1 Annex III - Digital services: Online marketplace, online search engine, cloud computing service	9. ICT-service management (B2B): managed service providers (MSP), managed security service providers (MSSP)
	10. Public administration entities, excluding the judiciary, parliaments and central banks
	11. Space

Who is in scope under the NIS2?

NIS 1	NIS 2 Annex 2 – *OTHER CRITICAL SECTORS*
	1. Postal and courier services
	2. Waste management
	3. Manufacture, production and distribution of chemicals
	4. Food production, processing and distribution
	5. Manufacturing
	6. Digital providers: Providers of online marketplaces, providers of online search engines, providers of social networking services platform
	7. Research

Who is in scope under the NIS2?

In-depth analysis is often required to assess applicability - example

‘Cloud computing service’ means

- A digital service
- that enables on-demand administration and broad remote access to
- a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations.

© Bird & Bird LLP

Who is impacted by NIS2?

Impacts will flow across supply chains

- *Take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems used*
- *Ensure a level of security of network and information systems appropriate to the risks*
- *Take an 'all-hazards' approach to protect network and information systems including dealing with supply chain security, and security-related aspects concerning the relationships between each entity and its direct suppliers or service providers*

What will change in terms of obligations?

Overview

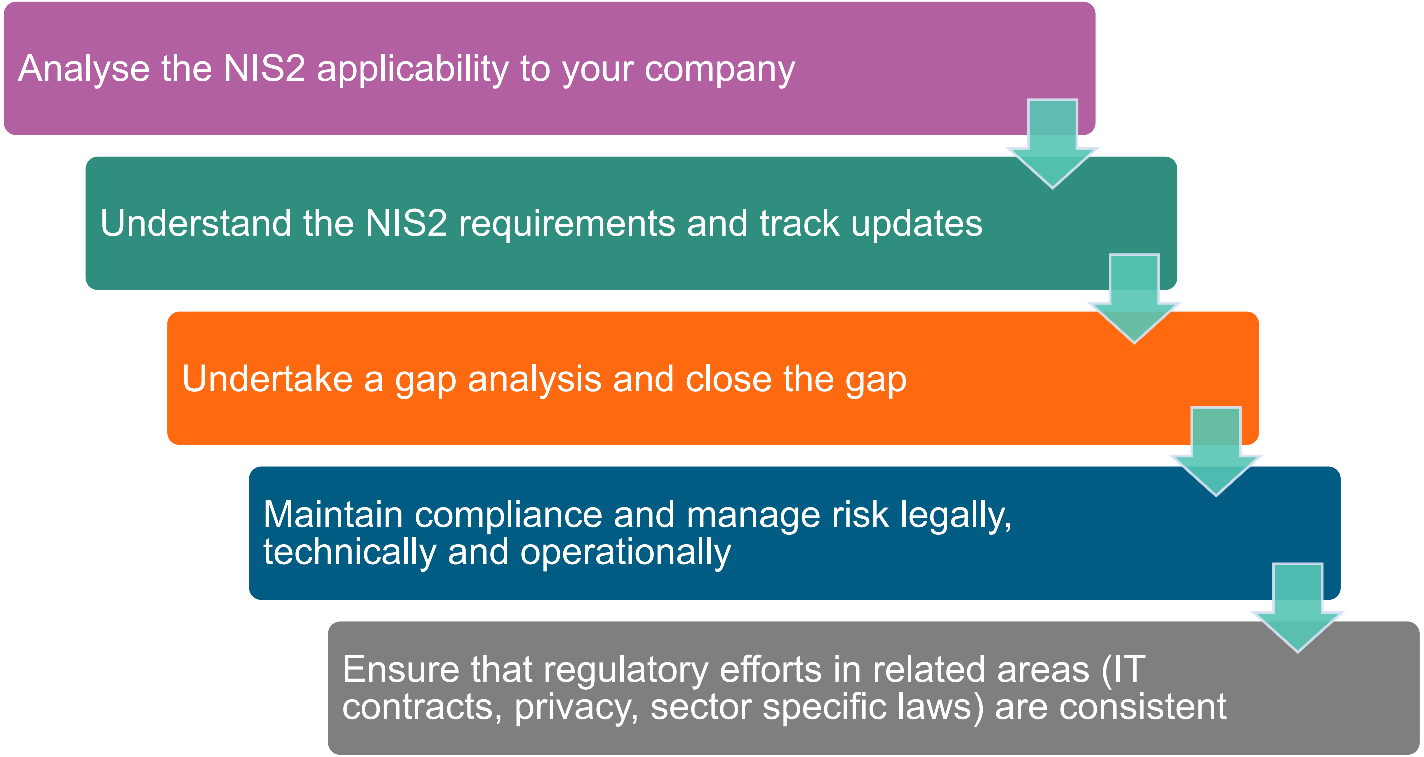
- More specific, strengthened cybersecurity risk management requirements, including addressing:
  - risk analysis and information system security policies;
  - security and incident response requirements;
  - business continuity, such as backup management and disaster recovery, and crisis management;
  - supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
  - security in network and information systems acquisition, development and maintenance; and
  - policies and procedures to assess the effectiveness of cybersecurity risk management measures
- Stronger reporting obligations
- Express governance requirements, including training obligations
- Cybersecurity certification
- Personal liability of management

NIS2 enforcement

What will change?

- NIS2 introduces stronger enforcement powers and provides Member States with broad discretion to implement their own national rules on penalties;
- Investigatory/enforcement options: include (amongst other things) the right for competent supervisory authorities to undertake on-site inspections, perform security audits, request information, order the cessation of certain conduct and, under certain conditions, temporal suspensions and prohibitions;
- Penalties:
  - Essential entities: fines of a maximum of at least 10 000 000 EUR or of a maximum of at least 2% of the total worldwide annual turnover of the group, whichever is higher
  - Important entities: fines of a maximum of at least 7 000 000 EUR or of a maximum of at least 1.4 % of the total worldwide annual turnover of the group, whichever is higher.

What should companies do to prepare for toughened requirements?



Analyse the NIS2 applicability to your company

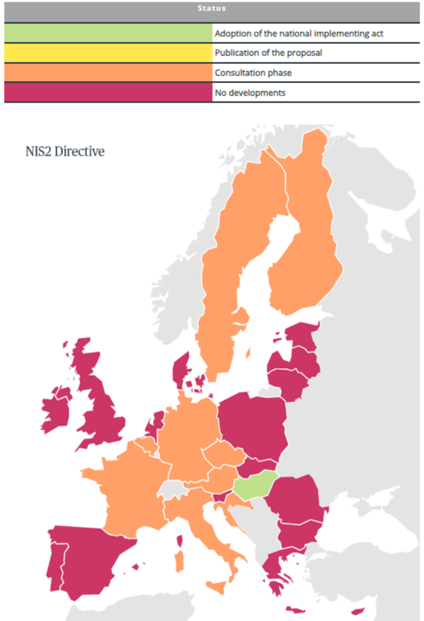
Understand the NIS2 requirements and track updates

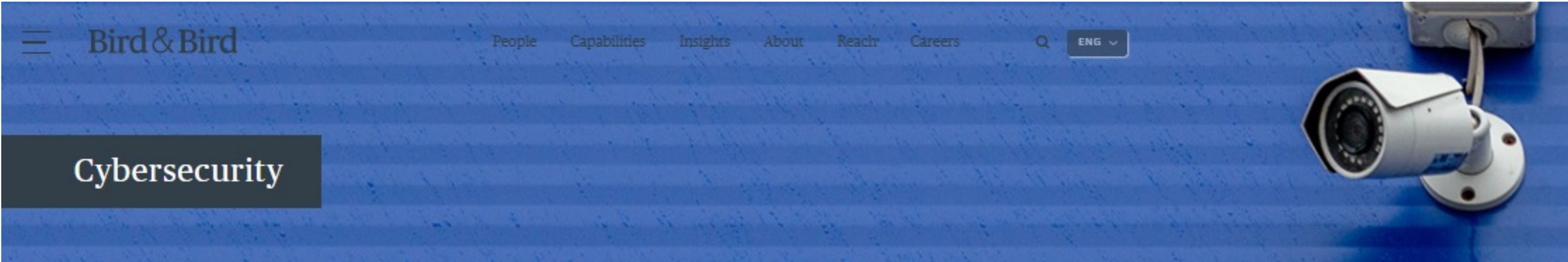
Undertake a gap analysis and close the gap

Maintain compliance and manage risk legally, technically and operationally

Ensure that regulatory efforts in related areas (IT contracts, privacy, sector specific laws) are consistent

Check the NIS2 tracker on twobirds.com


Status
Adoption of the national implementing act
Publication of the proposal
Consultation phase
No developments
NIS2 Directive



Cybersecurity

Craiyon - Your FREE AI image generator tool: Create AI art!

02

Cyber Resilience Act

Key elements

'first ever EU-wide legislation of its kind'

Mandatory cybersecurity requirements for products with digital elements, throughout their whole lifecycle

Cybersecurity by design: Increasing the responsibility of manufacturers by obliging them to provide security support and software updates; report vulnerabilities and incidents

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

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

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

Rules on market surveillance and enforcement on Member State level

Maximum harmonisation, however:

Member States may subject products with digital elements to additional cybersecurity requirements for the procurement or use of those products for specific purposes

(*i.e. purchasing hardware or software for government agencies for military, defence or national security purposes*)

SaaS

Digital services like Software-as-a-Service (SaaS) are not in scope

Example: smart home devices

*Remote data processing solutions **are** in scope:*

"any data processing at a distance

- for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer
- and the absence of which would prevent the product with digital elements from performing one of its functions"

'Placing on the market' obligations

Only place products with digital elements on the market if:

- This complies with the essential cybersecurity requirements in Annex I
- The manufacturer has set up appropriate Annex I processes to effectively resolve vulnerabilities
- Starting point: self-assessment with national supervision afterwards.
- Essential requirements will be set in European standards (harmonized standards):
  - Products listed in Annex III, Class II, subject to a prior third party conformity assessment
  - Similar essential requirements in Annex I apply to all products.

Annex I Essential security requirements	Annex I Vulnerability handling requirements	Annex II – User information and instruction
• Appropriate level of cybersecurity based on the risks • No known exploitable vulnerabilities • secure by default configuration • protection from unauthorised access protect processed data • protect integrity of processed data • minimisation of data • resilience against and mitigation of denial of service attacks • minimise negative impact on other services • limit attack surfaces • reduce the impact of an incident • provide security related information • vulnerabilities addressed through security updates	• Manufacturers need to: • identify and document vulnerabilities • address and remediate vulnerabilities without delay, including by providing security updates • apply effective and regular tests and reviews • publicly disclose information about fixed vulnerabilities • put in place and enforce a policy on coordinated vulnerability disclosure • take measures to facilitate the sharing of information about potential vulnerabilities • provide for mechanisms to securely distribute updates • security patches or updates disseminated without delay and free of charge	• Manufacturer details • point of contact • the identification of the product • the intended use and security properties • any known or foreseeable circumstance which may lead to significant cybersecurity risks • access to software bill of materials EU declaration of conformity • type of technical security support offered • instructions on ensure secure use, how changes to the product can affect the security of data, how security-relevant updates can be installed, secure decommissioning of the product, including information on how user data can be securely removed

Products with digital elements listed in class 1 of Annex III

These products either have

a) a cybersecurity-related functionality, or

b) a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation, such as a central system function

Products listed in class II of Annex III meet both criteria:

Annex III - PRODUCTS WITH DIGITAL ELEMENTS

Class 1	Class 2
1. Software that searches for, removes, or quarantines malicious software 2. Public key infrastructure and digital certificate issuance software 3. General purpose operating systems not covered by class II; 4. Physical and virtual network interfaces; 5. Routers, modems intended for the connection to the internet, and switches, not covered by class II 6. Microprocessors not covered by class II; 7. Microcontrollers; EP: add home automation systems and products that enhance private security, such as cameras and smart locks	1. Products with digital elements that support virtual private network (VPN) functions such as VPN servers and clients; 2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments 3. Firewalls, intrusion detection and/or prevention systems intended for industrial use

Third party conformity assessment +EUCC

Annex III class 2

1. Products with digital elements that support virtual private network (VPN) functions such as VPN server and clients;
2. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;
3. Firewalls, intrusion detection or prevention systems

Annex IIIa

1. Hardware Devices with Security Boxes;
2. Smart meter gateways within smart metering systems and other devices for advanced security purposes, including for secure crypto-processing;
3. Smartcards or similar devices, including secure elements.

Commission may add or withdraw through delegated act.
Implementing act to specify definitions

Required use of European cybersecurity certification schemes

The Commission may decide (in a delegated act) that products in certain categories require a Cyber Security Act certificate, if

- Appropriate CSA schedule is established and available
- Prior impact assessment addressing
  - potential market impact
  - consultation
  - a need for CSA certification among users
  - Member States are ready and have sufficient capacity to implement the relevant CSA scheme
- As long as no CSA certificate is required, class II is applicable

Open Source software

- Non-commercially offered (Open Source) software is not covered
- Commercially offered (Open Source) software is covered
- See definition of 'offering on the market': 'making available on the market' means the provision, in the course of a commercial activity, whether in return for payment or free of charge, of a product containing digital elements with a view to distribution or use on the Union market.
- The supply in the course of a commercial activity might be characterized not only by charging a price for a product, but also:
  - by charging a price for technical support services when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise,
  - by providing a software platform through which the manufacturer monetises other services, or
  - by requiring as a condition for use, the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

EP: developers of open source software should be excluded from the scope if they are not receiving any financial returns for their projects

Conformity assessment procedures

- Products in conformity with harmonised standards or issued under a certification scheme shall be **presumed to be in conformity** with the essential requirements
- Commission may adopt common specifications if no harmonised standards exist

Manufacturers obligations

During expected product life time: time users reasonably expect to be able to use the product specified at the time of purchase

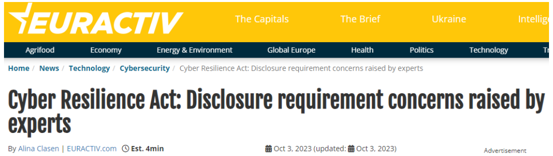
- Check components from **third parties** for security risk (avoid Trojan horses)
- Document risks and vulnerabilities
- Have appropriate security and vulnerability policies and procedures
- Ensure that **vulnerabilities** of that product are handled effectively
- EU declaration of conformity
- Instructions shall be in a language which can be easily understood by users
- Technical documentation and the **EU declaration of conformity**, where relevant, at the disposal of the market surveillance authorities and cooperate with them
- Series of production to remain in conformity
- Take the **corrective measures** necessary to bring that product with digital elements or the manufacturer’s processes into conformity, to withdraw or to recall the product, as appropriate
- Inform authorities and end user of ceasing operations
- **Security updates for a minimum duration of 10 years for last free of charge product version only**

Incident & vulnerability notifications

Notify CIRTs of exploited vulnerabilities and incidents, inform users:

- an early warning without undue delay and in any event within **24 hours** of becoming aware of the actively exploited vulnerability
- a notification updating the information without undue delay and in any event within 72 hours of becoming aware of the actively exploited vulnerability

EP: full report within one month (3 step approach). ENISA should become the one-stop entity for reporting. Alignment with NIS2 directive



Home / News / Technology / Cybersecurity / Cyber Resilience Act: Disclosure requirement concerns raised by experts

Cyber Resilience Act: Disclosure requirement concerns raised by experts

By Alina Clasen | EURACTIV.com Est. 4min Oct 3, 2023 (updated: Oct 3, 2023)

Advertisement

Importers

Complement manufacturer's obligations

- Check whether manufacturer has met its obligations
- Do not place on the market or withdraw products without conformity
- Indicate contact details on product packaging or document
- Report vulnerabilities to manufacturer and authorities
- Keep EU declaration of conformity for 10 years
- Demonstrate product conformity on request
- Inform authorities and end user of ceasing operations
- Distributor = importer = manufacturer in case of product placement under own name
- Substantial Product modificator = manufacturer

Distributors

Complement manufacturers and importers obligations

- Check CE marking
- Check whether manufacturer and importer have met their obligations
- Do not place on the market or withdraw products without conformity
- Notify manufacturer and importer about exploited vulnerabilities and incidents, inform users
- Demonstrate product conformity on request
- Inform authorities and end user of ceasing operations

Notifying authorities & bodies

Supervision at member state level

- ✓ Setting up assessment procedures
- ✓ Requirements for conformity assessment bodies
- ✓ Presumption of conformity
- ✓ Dedicated administrative cooperation group (ADCO)
- ✓ Access to manufacturers documentation
- ✓ Corrective measures
- ✓ Coordinated control actions (sweeps) to detect infringements
- ✓ Manufacturers: administrative fines of up to 15 000 000 EUR or 2.5% of total worldwide annual turnover
- ✓ Other: administrative fines of up to 10 000 000 EUR or 2% of total worldwide annual turnover
- ✓ Incorrect information: administrative fines of up to 5 000 000 EUR or up to 1% of total worldwide annual turnover

Support for small and micro enterprises

- Member States may organize specific awareness and training activities for SMEs
- Set up specific communication channels to provide advice and answer questions
- support testing and conformity assessment activities

- The Commission should develop guidance
- Micro and small businesses can use a **simplified format** for technical documentation.
- **EU subsidies** to become available to help SME's meet the costs of conformity assessment (Digital Europe programme) => Commission Priority

Standardisation

NL: harmonised standards to be available at entry into force

- Essential requirements to be detailed in harmonised standards
- CEN/CENELEC working group appointed.
- Draft standardisation request already released by the EC

EP:

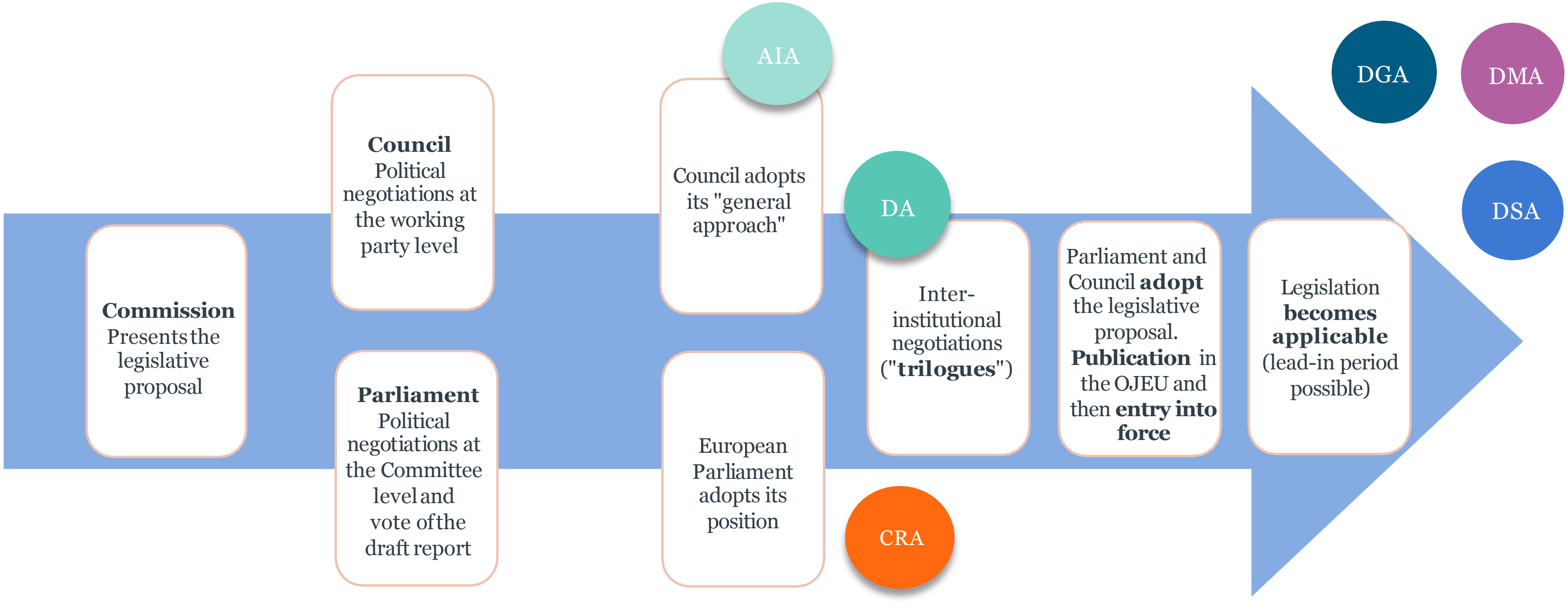
- Harmonised standards, common specifications or European cybersecurity certification schemes should be in place six months before the conformity assessment procedure applies. The Commission should provide guidelines with more details on the implementation.
- Mutual Recognition Agreements (MRAs) with third countries should be concluded to ensure the same level of protection as that provided by the CRA

Timing

- Breach notification requirements to enter into force after **24** months
- Includes products with digital elements already placed on the market
- Other provisions to enter into force after **36/40** months
- EU type-examination certificates and approval decisions remain valid until 42 months after the date of entry into force of the Regulation
- Entry into force not before 2026/2027

What's the status?

Most contentious points: The **reporting obligations** of manufacturers and the **list of critical products**



Commission Presents the legislative proposal

Council Political negotiations at the working party level

Parliament Political negotiations at the Committee level and vote of the draft report

AIA

Council adopts its "general approach"

European Parliament adopts its position

DA

CRA

Inter-institutional negotiations ("**trilogues**")

Parliament and Council **adopt** the legislative proposal. **Publication** in the OJEU and then **entry into force**

Legislation **becomes applicable** (lead-in period possible)

DGA

DMA

DSA

CRA text adopted end 2023/Q2 2024?

Sign up for our *Connected* newsletter for monthly Regulatory & Public Affairs insights

Thank you

twobirds.com

● *Abu Dhabi* ● *Amsterdam* ● *Beijing* ● *Bratislava* ● *Brussels* ● *Budapest* ● *Casablanca* ● *Copenhagen* ● *Dubai* ● *Dusseldorf* ● *Frankfurt* ● *The Hague* ● *Hamburg* ● *Helsinki* ● *Hong Kong* ● *London* ● *Luxembourg* ● *Lyon* ● *Madrid* ● *Milan* ● *Munich* ● *Paris* ● *Prague* ● *Rome* ● *San Francisco* ● *Shanghai* ● *Singapore* ● *Stockholm* ● *Sydney* ● *Warsaw*

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.