TÜVNORD

CRA, NIS2 & EU Cybersecurity Certification



Mielke | Regulation | 17.11.2026



Brief notes

- Feel free to ask questions
- You can post questions in the Chat, and I will then answer them for everyone afterwards.
- You are also welcome to send me questions by email, or we can arrange another separate appointment.
- **Email**: tmielke@tuev-nord.de

TÜVNORD

CYPRO



Tobias Mielke

- **PC Head of Cyber Security and Management Systems (TÜV NORD)**
- **Lead Auditor for ISO27001, 27701 and various data protection programs**
- **Participation**
  - ENISA EUCS Guidance (Cloud Certification Scheme)
  - TeleTrust-AK "State of the Art"
  - Task Force CRA (Module H)

CYPRO

Agenda

Regulations & Standards

01 **Reasons for Regulations – European Regulations**

02 **NIS2**

Network and Information System Directive 2

03 **CRA**

Cyber Resilience Act

04 **CER**

Critical Entities Resilience Directive

05 **Standards and certification form the basis.**

TÜVNORD

Reasons for Regulations

Global Risks for 2026

Highest Risks as per the results of the Risk in Focus 2026 Survey (Institute of Internal Auditors - IIA)

Risk area	Average of the regions	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	**73%**	**62%**	**62%**	**82%**	**76%**	**72%**	**86%**
Digital disruption (including AI)	**48%**	**44%**	**39%**	**47%**	**54%**	**50%**	**53%**
Business resilience	**47%**	**49%**	**58%**	39%	35%	**58%**	**46%**
Human capital	**43%**	35%	**56%**	**48%**	**40%**	**38%**	42%
Regulatory change	**41%**	34%	38%	**45%**	**49%**	28%	**51%**

- **Cybersecurity** is the highest ranked risk worldwide by a large margin (73%).

- A technology risk also held second place – **digital disruption** (48%).

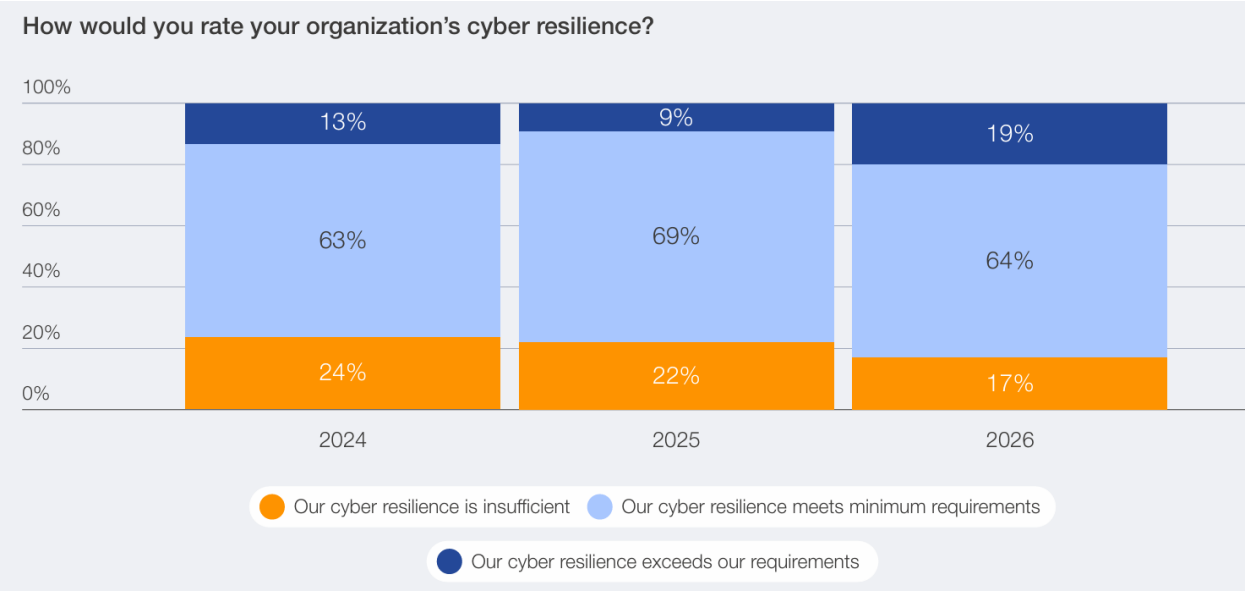
2026 Global Summary Risk in Focus Report English

World Economic Forum

Global Cybersecurity Global Outlook 2026

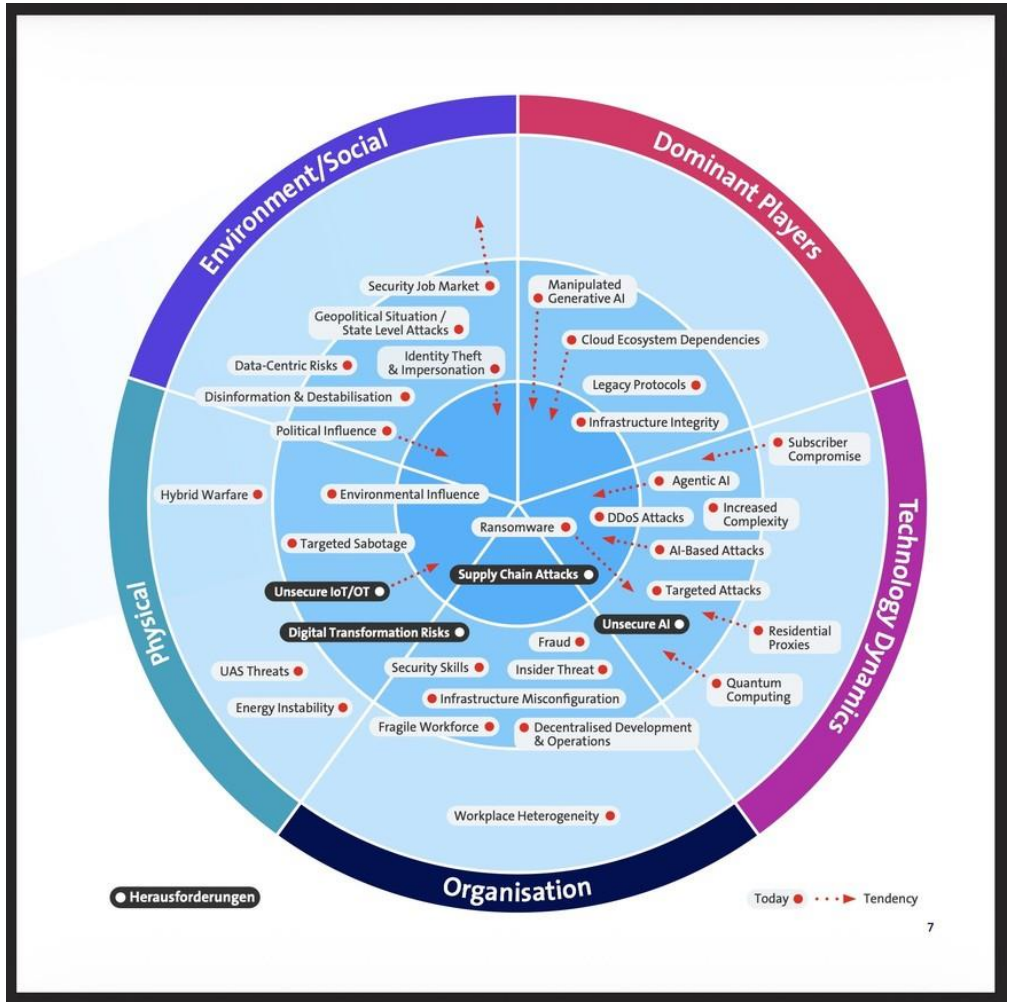
- Cyber resilience underpins an organization's ability to minimize the impact of significant cyber incidents on its primary business goals and objectives.
- Survey data shows increasing confidence in organizational cyber resilience.
- While 64% of organization report having met their minimum cyber resilience requirements, regardless of regional or sectorial variation only 19% claimed that cyber resilience exceeds their requirements.

- Growth in Business Resilience and Security



[Global Cybersecurity Outlook 2026 | World Economic Forum]

Cybersecurity Threat Radar 2026



- Attacks sponsored by states, hybrid influence operations such as **disinformation campaigns**, and **supply chain**, **artificial intelligence** and **industrial system** risks are on the rise.

- **Software supply chains** remain a **key risk**: even a single compromised component or a tampered update can have far-reaching **consequences**. That is why their origin, integrity, and traceability must remain verifiable.

- The issue of **'digital sovereignty'** is becoming increasingly important. Companies need to know where their data is being processed, which **regulations** their providers are subject to, and how dependent they are on individual platforms. Transparency is therefore becoming a prerequisite for effective action.

Fridges/Chiller cabinets in the supermarket

Autumn 2026

What happened

- **October:** France. **Early November:** Germany and further European countries
- Attackers remotely change the settings of supermarket refrigeration systems
- One store in Bavaria: units heated up to **50 °C**, according to the store

The way in

- In one case the attack targeted the **company that maintains the systems remotely** (store operator to dpa)
- The retailer was hit through its **service provider** — not its own IT

Who is behind it

- **France:** Paris attributes the attacks to Iran's Revolutionary Guards (Foreign Minister Barrot, 9 Nov 2026); investigations target their cyber unit
- **Wider wave:** claimed by pro-Russian groups — **not independently confirmed**

The pattern: connected operational technology, reached through a third party's remote access — exactly what NIS2 supply-chain duties and the CRA are designed to address.

What does this mean for Europe?

Cybersecurity in Europe

- Europe faces increasingly sophisticated hybrid attacks with a systematic cyber dimension that can disrupt critical sectors like energy, transport, health, banking and water.
- The cybersecurity laws are intended to enable the EU to address these security risks while strengthening its cybersecurity.

Key Figures and Trends[1]

Global cybercrime costs: exceeded €9 trillion in 2025.

Top 5 targets in the EU: public sector, transport, digital, finance and manufacturing.

Ransomware[2]: most impactful cyber-threat in 2025; attacks every 2 seconds by 2031.

Supply chain attacks: among top 7 threats.

AI and quantum computing: significantly impacting cybersecurity.

Overview of EU legislation in the digital sector

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Finance
Digital Europe Programme Regulation	Recovery and Rexilience Facility Regulation	Frequency Bands Directive	…	Database Directive	Regulation for a Cybersecurity Act	Law Enforcement Directive	Toys Regulation	…	EU Merger Regulation	Common VAT system
Horizon Europe Regulation	InvestEU Programme Regulation	Radio Spectrum Decision	GDPR	Community Design Directive	European Cybersecurity Centre	Directive: combating fraud	European Standardization Regulation	EU accessibility Act (EEA)	Technology Transfer	Administrative cooperation (Tax)
Regulation on a pilot regime distributed ledger tech. Market	Connecting Europe Facility Regulation	Broadband Cost Reduction Directive	Regulation on the free flow of non-personal data	Enforce-ment Directive	NIS-2-Directive	Interoperability between EU information systems in the field of borders and visa	eIDAS Regulation	Geo-Blocking Regulation	Company Law Directive	Payment Service Directive 2
	Regulation on Joint Undertakings under Horizon Europe	Open Internet Access Regulation	Open Data Directive	Directive on the protection of trade secrets	Information Security Regulation	Regulation on terrorist content online	Radio Equipment Directive	Regulation on cooperation for the enforcement of consumer protections laws	Market Surveillance Regulation	Digital Operational Resilience Act (DORA)
	Decision on a path to the Digital Decade	EECC	Data Governance Act (DGA)	Design Directive	Cybersecurity Regulation	Temporary CSAM Regulation	Regulation for a Single Digital Gateway	Digital content Directive	P2B Regulation	Crypto-assests Regulation (MiCAR)
	European Chips Act	EU-top-level-domain Regulation	Data Act (DA)	Compulsory licensing of patents	Cyber Resilience Act (CRA)	E-evidence Regulation	General Product Safety Regulation	Directive on certain aspects concerning for the sale of goods	Single Market Programme	Financial Data Access Regulation
	European critical raw materials Act	Roaming Regulation	European Health Data Space	Standard essential patents	Cyber Solidarity Act	Directive on combating violence against women	Machinery Regulation	Digital Services Act (DSA)	Vertical Block Exemption Regulation	Payment Services Regulation
	Net Zero Industry Act	Secure Connectivity Programme Regulation	Data collection for short-term rental Regulation			Digitalization of travel documents	AI Act	Political Advertising Regulation	Digital Markets Act (DMA)	Digital euro
	STEP	RSPP 2.0	Interoperable Europe Act				(New) Product Liability Directive	Rights to repair Directive	Regulation on distortive foreign subsidies	Regulation on combating late payment
	EU Space Law	Digital Networks Act	ePrivacy Regulation				AI Liability Directive	e-invoicing Directive	Platform Work Directive	EU-Business Wallet
	European supercomputer capacity to AI-start-ups		Digital Networks Act					Multimodal digital mobility services	Single Market Emergency Instrument	

Quelle: https://www.bruegel.org/

Applicable law	Published in the Official Journal of the EU
Under negotiation	Proposal by the Commission entered the legislative process
Planned initiative	Mentioned by the Commission as potential legislative initiative
Abandoned	Negotiations failed

- What's missing?

Critical Entities Resilience Directive, EU 2022/2557

Types of legislation

Regulation vs. Directive

Regulation

GDPR -> European regulation,

- directly applicable,
- legal character,
- also transposed into with additional national rules

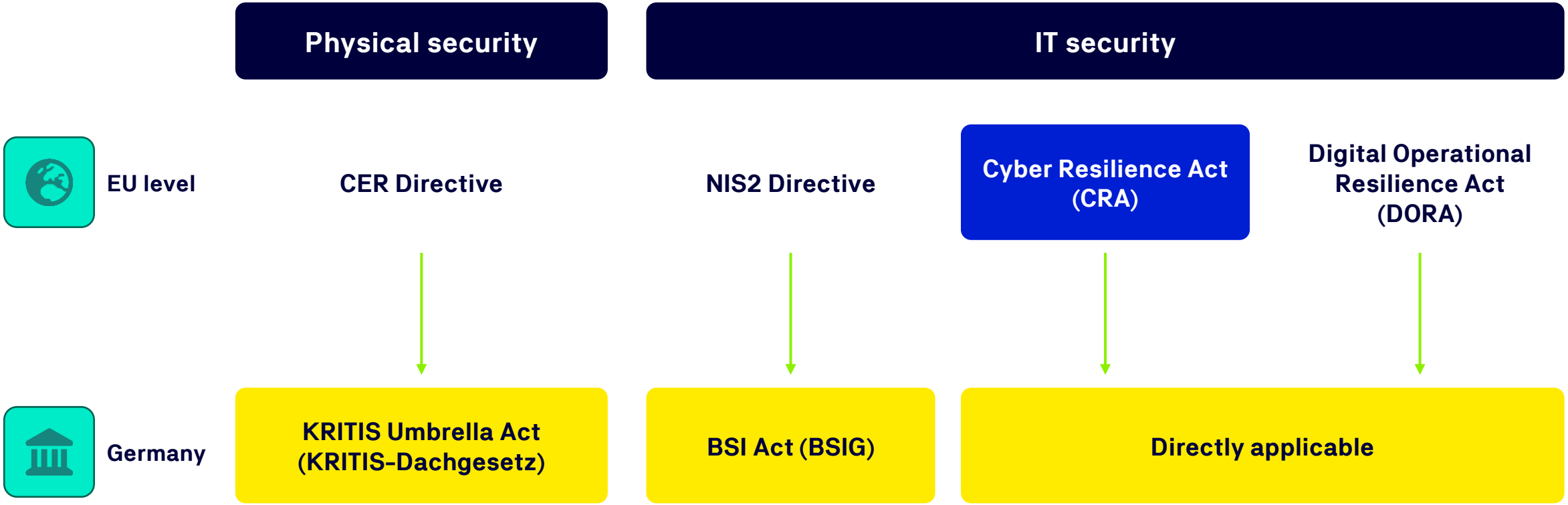
Guideline

NIS-2 -> European directive,

- must be cast in national laws,
- only then legally applicable

EU cybersecurity strategy

Example Germany



Three regulatory layers, one EU framework

THE EUROPEAN CONTEXT

Organisations & operators

Are your operations resilient?

- **NIS2** — cybersecurity of essential & important entities
- **CER** — physical resilience of critical entities
- **DORA** — ICT risk in the financial sector

Products with digital elements

Is the product secure by design?

- **CRA** — horizontal rules, CE marking from Dec 2027
- **RED** — connected radio equipment (bridge to CRA)
- **EUCC** — voluntary EU product certification

Cloud & ICT services

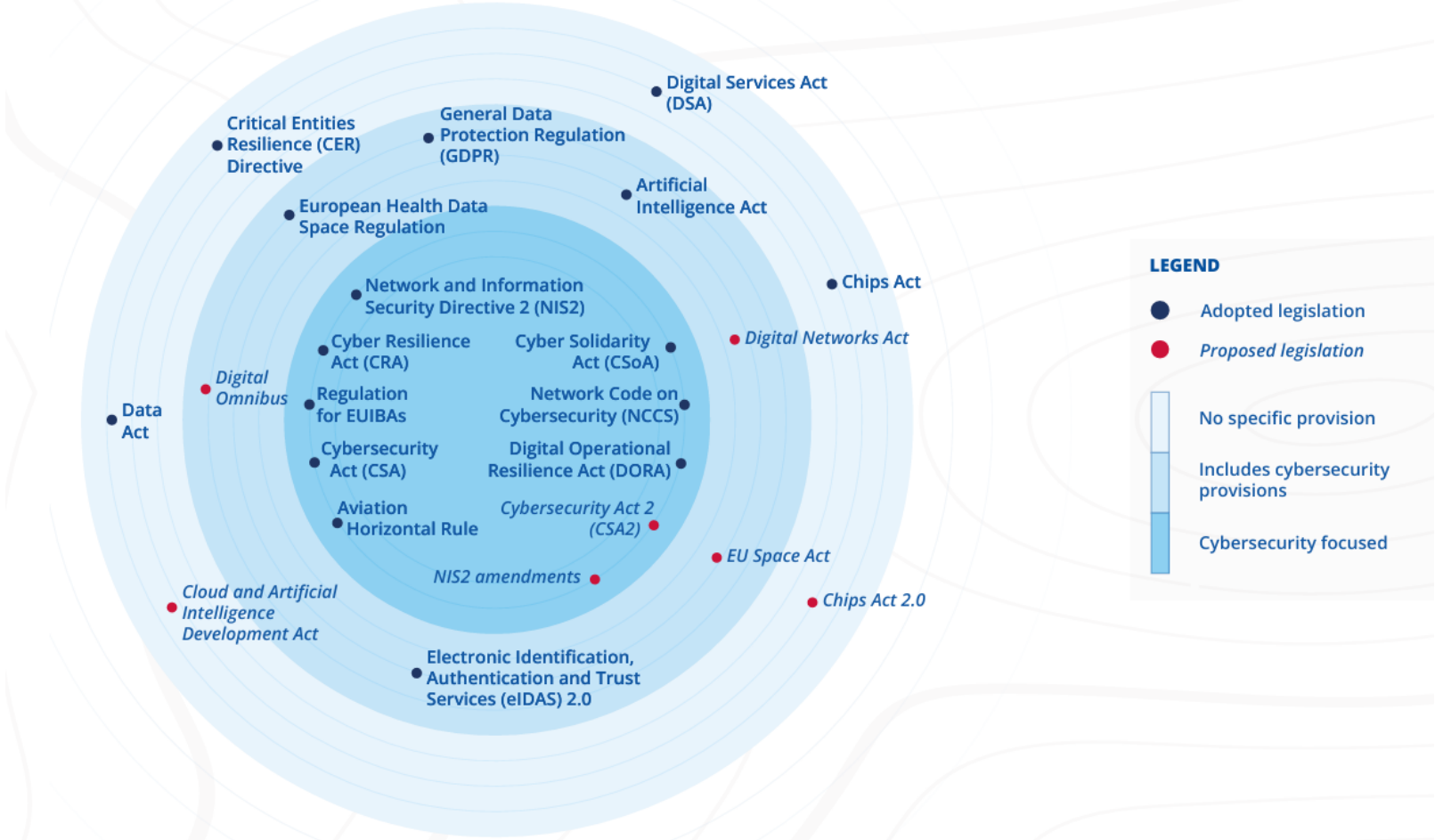
Can customers trust the service?

- **EUCS** — EU cloud scheme, still a candidate
- **BSI C5** — attestation, de-facto benchmark in Germany
- **ISO/IEC 27001 + 27017/27018** — international baseline

The **Cybersecurity Act (CSA, 2019)** provides the EU-wide certification framework behind EUCC, EUCS and future schemes — one certificate, recognised in all 27 Member States.

EU Policy Landscape

ENISA 2026 Report On The State Of Cybersecurity In The Union



- Implementation: EU, national bodies and companies are focused on implementing key legislation, above all NIS2
- New initiatives: Cybersecurity Act 2 (CSA2) with a trusted ICT supply chain security framework, plus the Action Plan on Cybersecurity and AI
- EUCC as the bridge to the CRA: a delegated act is expected to establish a presumption of conformity based on the EU Common Criteria scheme (EUCC)

TÜVNORD

CYPRO

Poll 1

Which regulation affects your organisation most in the next 12 months?

- NIS2
- CRA
- CER
- More than one
- Still assessing

NIS2

Network & Information Security Directive 2



CYPRO

NIS-2 Directive

Uniform IT security throughout Europe

NIS2 → Network and Information Security

EU NIS 2 is the European framework for operators of critical infrastructures and defines minimum cyber security standards in the EU.

The deadline for implementation of the NIS 2 Directive by the EU member states **was** October 17, 2024.

E.g. In Germany, the implementation is carried out by the NIS-2 Implementation Act.
and Cybersecurity Reinforcement Act (NIS2UmsuCG - BSIG)

TÜVNORD

Introduction to NIS 2

NIS 2 standardizes the EU-wide resilience of critical infrastructure against cyber threats, supports cross-border cooperation, and ensures secure digitalization in the single market.

2015 — **IT Security Act 1.0**
- Enhancing the security of critical information technology systems

2016 — **NIS Regulation**
- Establishment of basic standards for essential services

2021 — **IT Security Act 2.0**
- Expansion of the sectors and powers

2022 — **NIS 2 – Directive**
- An expanded version of NIS 1 that covers more sectors and establishes uniform cybersecurity standards across the EU

2024 — **NIS 2 Transposition Deadline**
- All EU member states are required to incorporate NIS 2 into their national laws

2024 — **NIS 2 Implementing Regulation**
- List of technical and methodological requirements

In Germany, approximately 30,000 companies will be affected, as they will be designated as critical or highly critical infrastructure under NIS 2.

Responsibility for implementation lies with the management of each individual company.

Requirements:
- Network and Information Security
- Risk management
- Incident management
- Supply chain security

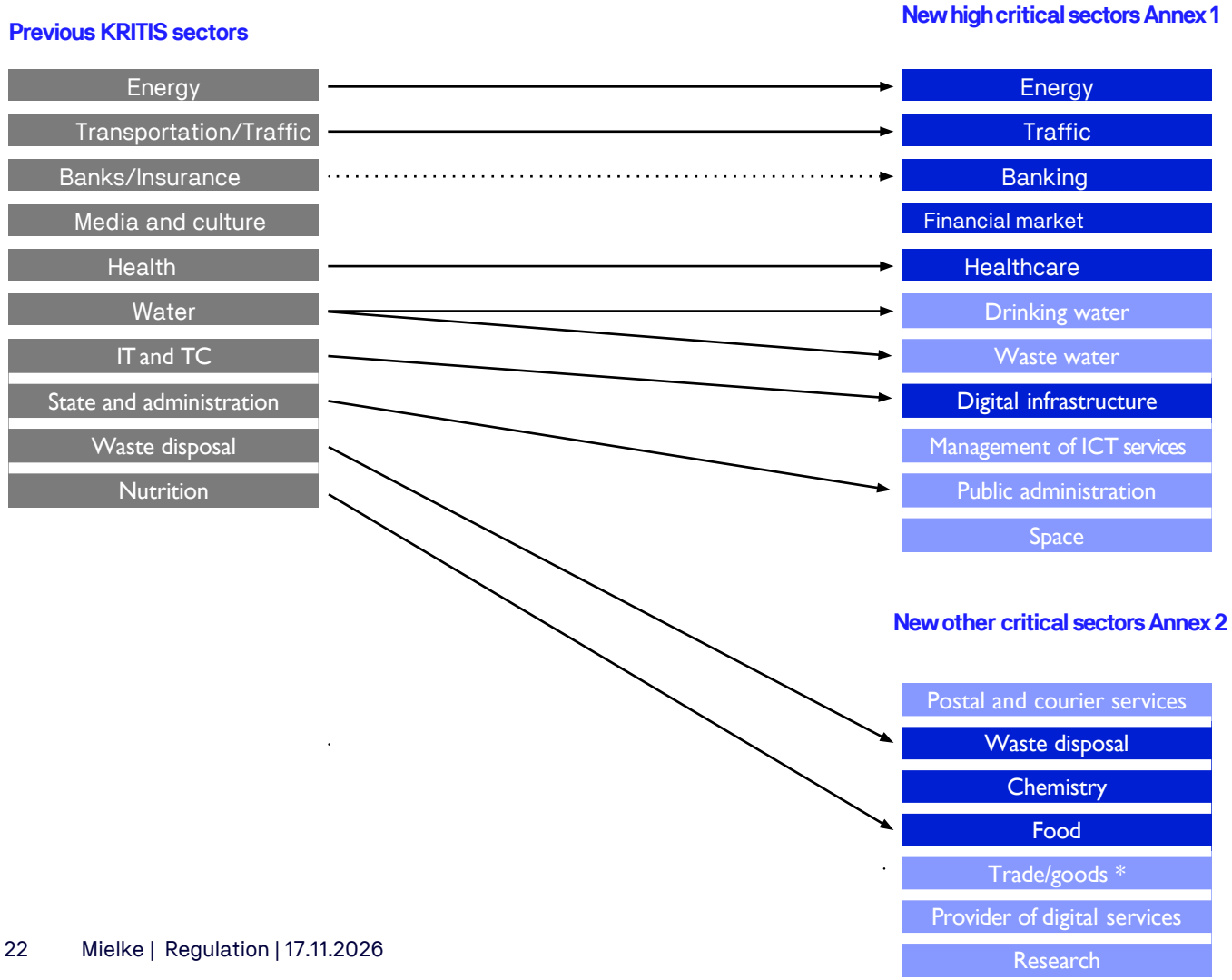
NIS2 Overview

The "Network and Information Security 2" (NIS2) directive

- is the **EU-wide legislation for the protection of critical infrastructures and digital services** of systemic importance in public and private sectors.
- serves to **create a high, common level of security for network and information systems** in the EU.
- contains **legal measures to increase** the overall level of **cybersecurity in the EU** to improve resilience and responsiveness to cyber threats and ensure full functionality even in crises.
- **regulates national cyber security authorities**, the establishment of the Computer Security Incident Response Team (CSIRT), EU-wide initiatives such as the **creation of a vulnerability register** and the role of **ENISA as a central point of contact for** regulated organizations.
- defines **criteria for identifying operators of critical infrastructures and information security requirements.**
- aims to **promote cooperation between all Member States** and strengthen the safety culture in all sectors of critical importance such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.
- is a **revised version** of the existing **NIS1** directive and **expands** it **to include stricter safety requirements, additional sectors** and a **higher number of affected companies**.
- **the obligation for <u>all</u>** Member States **to adopt national cybersecurity strategies**

Sectors and subsectors

Overview of old sectors and new sectors (18)



*Example:
Breakdown into sectors and subsectors using the example of the industry sector = manufacturing/production of goods

a) Manufacture of medical devices and in-vitro diagnostics
b) Manufacture of computers, electronic and optical products
c) Manufacture of electrical equipment
d) Mechanical engineering
e) Manufacture of motor vehicles and parts
f) Other vehicle construction

Requirements & obligations of affected facilities

GOVERNANCE
(Article 20)



CYBERSECURITY RISK MANAGEMENT MEASURES
(Article 21)



INFORMATION/ REPORTING OBLIGATIONS
(Article 23)



USE OF EUROPEAN CYBER SECURITY CERTIFICATION SCHEMES
(Article 24)



Essential cybersecurity risk-management measures

Risk-management measures – Article 21

- **Article 21 a** policies on risk analysis and information system security
- **Article 21 b** Incident handling
- **Article 21 c** business continuity, such as backup management and disaster recovery, and crisis management
- **Article 21 d** supply chain security
- **Article 21 e** security in acquisition, development and maintenance of systems
- **Article 21 f** policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- **Article 21 g** basic cyber hygiene practices and cybersecurity training
- **Article 21 h** policies and procedures regarding the use of cryptography
- **Article 21 l** HR security, access control policies, asset management
- **Article 21 j** MFA, secured/emergency communication

Additional "formal" duties

- Registration of the entity
- Timely reporting of significant incidents (24h)
- Ensuring compliance with additional local NIS2 requirements
- (Regular) executive management training
- Management governance: awareness of the cybersecurity posture

Requirements & obligations of affected facilities

GOVERNANCE
(Article 20)



Top management has governance responsibility and is obliged to implement and enforce NIS2!

Governance requirements

- Approval of risk management measures
- Monitoring the implementation
- Training of the management bodies
- Responsibility for violations

Requirements & obligations of affected facilities

CYBERSECURITY RISK MANAGEMENT MEASURES
(Article 21)



Measures* to manage the risks to the security of their network and information systems and to prevent or minimize the impact of security incidents. Includes at least:

a. Risk analysis and security guidelines for information systems
b. Management of security incidents
c. Maintaining operations and crisis management
d. Security of the supply chain
e. Security measures for the acquisition, development and maintenance of network and information systems
f. Guidelines and procedures for assessing the effectiveness of cybersecurity risk management measures
g. Basic cyber hygiene procedures and cyber security training
h. Policies and procedures regarding the use of cryptography and encryption
i. Personnel security, access control concepts and asset management
j. Use of MFA, authentication solutions, emergency communication systems

** Appropriate + proportionate technical, operational and organizational measures*
- *Consideration of the state of the art and the costs of implementation*
- *Consideration of the extent of risk exposure and the size of the company*
- *Consideration of the probability of the occurrence of security incidents and their severity (incl. social and economic impact)*

Supply Chain

NIS2 Supply Chain Impact for the Companies (Art. 21 NIS2)

Supply chain security, including security-related aspects of the relationships between individual entities and their immediate suppliers or service providers

- Modern attacks begin in the supply chain (e.g., SolarWinds)
- Extending the requirements to other companies

Suppliers and service providers of affected EU customers must adhere to fundamental principles such as security by design and security by default.

Implementation of an Information Security Management System (ISMS) using existing standards (ISO/IEC 27001:2022 etc.). An ISMS establishes the structures and methods necessary for an effective Supply Chain. Without an ISMS, many of these foundational elements would have to be created from scratch, which significantly increases the effort and risk involved.

Overview of implementation in Europe

Publications on the EU Commission website

Österreich	Italien
Belgien	Lettland
Bulgarien	Litauen
Kroatien	Luxemburg
Zypern	Malta
Tschechische Republik	Niederlande
Dänemark	Polen
Estland	Portugal
Finnland	Rumänien
Frankreich	Slowakei
Deutschland	Slowenien
Griechenland	Spanien
Ungarn	Schweden
Irland	

Source:
https://digital-strategy.ec.europa.eu/de/policies/nis-transposition

NIS2 Directive implementation in the Czech Republic

This page gives state of play of the implementation of the NIS2 Directive in the Czech Republic and points of contact.

Share

The content will be updated progressively as information will be made available to the Commission, without prejudice to the formal assessment of the compliance of transposition measures with the requirements of the NIS2 Directive.

Status of transposition

On 7 May 2025 the Commission sent a reasoned opinion for failure to notify full transposition.

National strategy on the security of network and information systems

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020

Single point of contact

National cyber and information security agency

Address: Mučednická 1125/31, 616 00 Brno t
Email: nckb@nukib.cz
Phone: +420 541 110 777

National competent authority for DSPs

CZ.NIC

Address: Milešovská 1136/5, 130 00 Praha 3
Email: kontakt@nic.cz

National competent authorities for OES

Same as single point of contact (see above).

CRA

Cyber Resilience Act

Cyber Resilience Act

Introduction

The CRA implements a post-market enforcement model for the placing of products on the EU market from a cybersecurity perspective

The manufacturer ensures that the product complies with the essential requirements set out in the CRA and places it on the market under its sole responsibility.

All products sold in the EU that contain “digital elements” must comply with the requirements of the CRA.

This includes not only low-cost consumer products but also B2B software and complex high-end industrial systems.

The CRA defines “products with digital elements” as products—including remote data processing solutions—that can be connected directly or indirectly to a device or a network.

Cyber Resilience Act

How do the CRA and the CE marking requirement relate to each other

The CRA is an EU regulation (like the GDPR) aimed at strengthening digital security for "products with digital elements" in the EU.

These are physical or virtual products (including backend systems, where applicable) that contain digital components and are connected in any way to the internet or other networks. These products can include both hardware and software.

CE Marking

CE marking in general:

- **A prerequisite for market entry** in the EEA* for most products, unless other regulations apply. The goal is to ensure product safety.
- The marking requirement stems from **EU directives and regulations**, such as the "General Product Safety Directive," the "CE Marking Regulation," or the **CRA**.
- Marking requirement does not apply to all products.



Relation to the CRA:

- Without compliance with the CRA, **"products with digital** elements" cannot be CE marked (Article 27 et seq.).
- Manufacturers must demonstrate/confirm that they comply with the CRA (effective **December 11, 2027**)
- **Without a CE marking,** products may not be placed on the market or sold in the EEA* as of December 11, 2027. An exception applies only to replacement parts for products already in the field.

*EEA: European Economic Area

Most interesting questions for manufacturers

Impact for international companies – also outside of the EU

1. Are my products affected by the CRA?
2. What is the timeline for my products?
3. How can I achieve presumption of conformity?
4. Which conformity assessment procedures can I choose from for my product?
5. Can I still export my existing product into the European Union?
6. What is the progress of standardization and which standards should I use for my product?
7. Where do I find more and up-to-date information on the CRA?

The CRA applies to **all manufacturers** who **place products with digital elements on the EU market**, regardless of whether their place of business is located within or outside the EU.

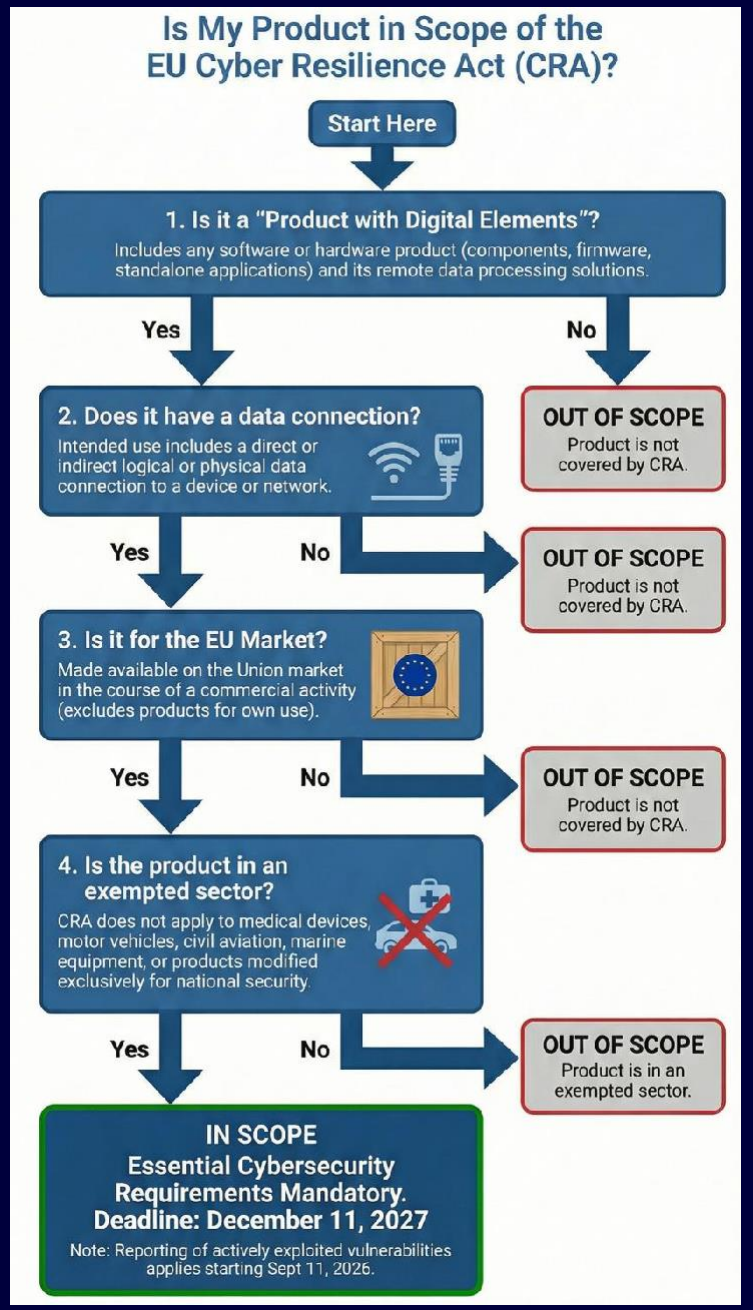
For example, the CRA applies to a Japanese manufacturer wishing to sell its game consoles on the EU market just as much as it does to a U.S. manufacturer selling antivirus software in the EU. In addition, distributors and importers of related products must also ensure compliance with the regulations.

Am I affected by the CRA?

1. Follow the definition of „product with digital elements“
2. Look at the intended use, which also includes the capability (e.g. deactivation must be permanent) and foreseeable use
3. Include Remote Data Processing Solution (e.g. App)
4. Identify the time of when the product will be placed on the market (for **every** product – no batch/model view)

Rule of thumb: Expect that every software or hardware product with a data connection sold

in Europe after Dec. 11th, 2027 is going to be in scope.



Products with digital elements, Art. 3(1) CRA

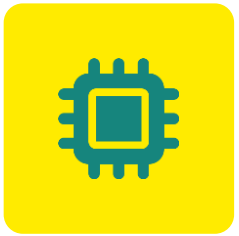
*'Product with digital elements' means a **software or hardware product** and its **remote data processing solutions**, including software or hardware **components** being placed on the market separately*



1 Hardware



2 Software



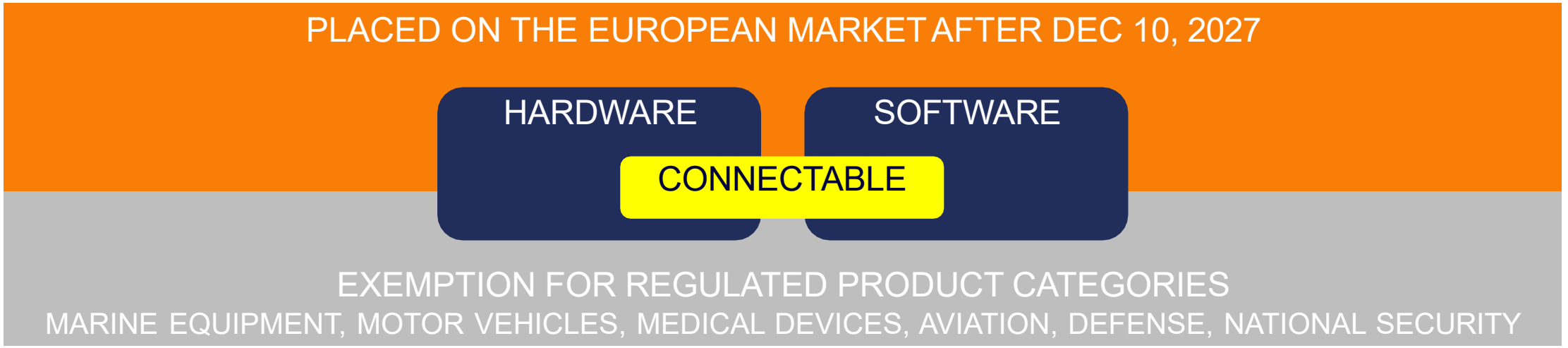
3 Components



4 Remote data processing

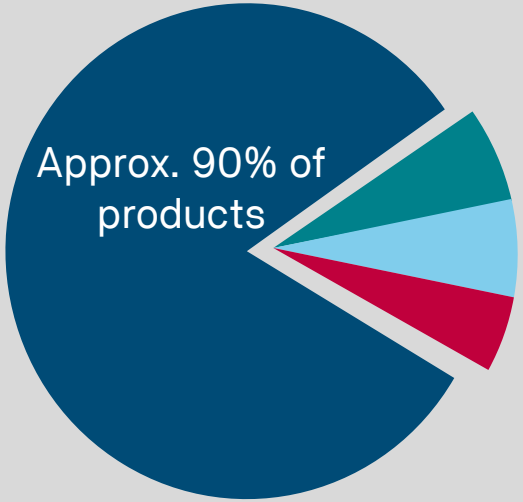
CRA – Examples of product affected

Component	Product to be integrated	Product placed on the EU market	Affected by CRA?
Network interface	PLC	Machine tool	Yes
Network interface	PLC	PLC	Yes
Display	Embedded System	Coffee machine	No, if no connectivity
Embedded Controller	ECU	Car	No, exempted



Key provisions of the Cyber Resilience Act

Classification, requirements, and evidence of conformity



Essential safety requirements for all products containing digital elements (horizontal requirements)

Product requirements

- Products with digital elements → Modules A or B/C or H or CSA
- Important products with digital elements, Class I → Modules A[1], or B/C, or H, or CSA
- Important products with digital elements Class II → Modules B/C or H or CSA
- Critical products with digital elements → Modules B/C[2], or H[2], or CSA

This classification allows for a differentiated approach to the scope and depth of **the essential safety requirements** and the **demonstration of conformity** with the CRA.

Classification of products

Depending on the classification, different procedures (**modules**) for demonstrating conformity are possible or required (Article 32).

Proof of conformity

[1]Permitted only when using a harmonized European standard
[2]Permitted only if a CSA certificate is not required

Horizontal and vertical standards

Horizontal standards establish a common baseline for all products with digital elements, while **vertical** standards address the specific risks of individual product categories.

Aspect	Horizontal standards	Vertical standards
Scope	Product-agnostic	Product-specific
Applicability	Every product with digital elements, regardless of category	Important (Annex III) and critical (Annex IV) product categories only
Content	Common framework, terminology, risk management method, lifecycle activities, vulnerability handling and generic security requirements	Concrete security requirements and assessment criteria for one product type, such as routers, password managers or smartcards
M/606 type	Type A (framework) and Type B (product-agnostic requirements)	Type C (product-specific)
Developed by	CEN-CENELEC JTC 13	ETSI (EN 304 6xx), CENELEC (prEN 50770, EN 40001-3 to EN 40004-3), CEN/TC 224 (EN 40000-10, EN 40000-11, EN 18330)
Series	EN 40000-1-x	EN 304 6xx, prEN 50770 and related series

Impact on conformity assessment

Harmonised standards also determine which conformity assessment procedures are available

Product tier	Examples	Conformity route	Effect of a cited harmonised standard
Default	Most products with digital elements	Self-assessment (internal control)	Supports the presumption of conformity, self-assessment is available regardless
Important, Class I	Password managers, VPN products, routers, smart home hubs	Self-assessment only where harmonised standards, common specifications or a European certification scheme are applied (Article 32(2)), otherwise a notified body	Opens the self-assessment route
Important, Class II	Hypervisors and container runtimes, firewalls, IDS/IPS, tamper-resistant microcontrollers	Third-party assessment	Supports conformity, does not remove third-party assessment
Critical (Annex IV)	Hardware devices with security boxes, smart meter gateways, smartcards and secure elements	European cybersecurity certification where mandated; otherwise third-party routes	Supports conformity, does not remove certification or third-party requirements

Modul H in the CRA

A conformity assessment procedure based on comprehensive quality assurance.



A process in which not the product itself (as in a type examination), but the manufacturer's quality management and development system is examined by a notified body (third party).

Discussions are currently being held on who will become a notifier, i.e. an accreditor, and what requirements will be placed on the certification bodies to be accredited.

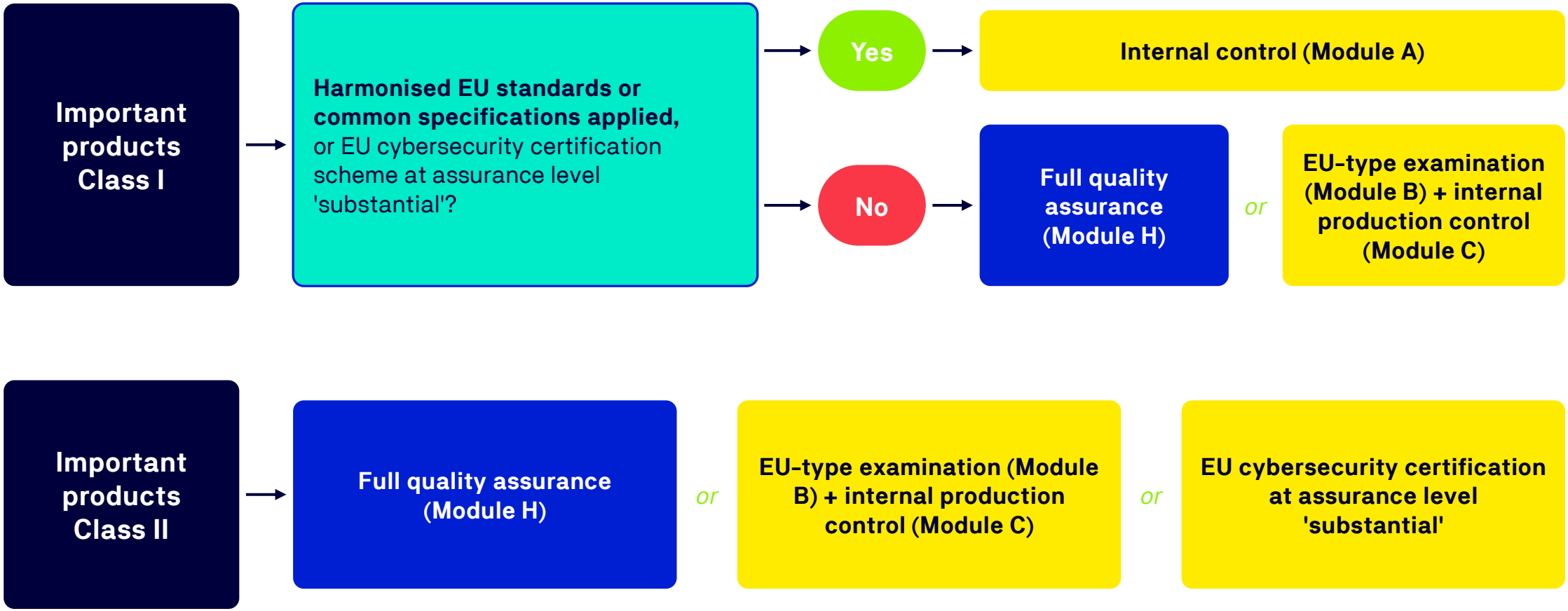
The basis of the management system is also under discussion: ISO 9001 or ISO 27001



The committee is chaired by the German Federal Office for Information Security (BSI), which favours ISO 27001.

Choosing the right conformity assessment

Procedure for important products



TÜVNORD

CYPRO

Poll 2

Which CRA conformity route do you expect for your products?

- Module A (self-assessment)
- Module B+C
- Module H
- EUCC certification
- Not a manufacturer / unsure

CER

Critical Entities Resilience Directive

Critical Entities Resilience Directive

The EU CER Directive is a legislation that protects organizations delivering essential services across the EU.

The Directive specifically addresses **11 critical sectors**, including energy, transport, digital infrastructure, banking, and healthcare, to ensure essential services continue despite any disruption. It does this by enforcing mandatory risk assessments, business continuity planning (e.g. ISO22301), and incident reporting, with a focus on proven operational readiness.

Using an all-hazards approach, the Directive addresses natural disasters, cyber-physical attacks, terrorism, pandemics, and supply chain failures. It recognizes that critical entities don't operate in isolation, making resilience a shared responsibility.

- Resilience measures across supply chains & infrastructure
- Coordination with NIS2 for integrated cyber-physical protection and Incident notification to competent authorities

11 Sectors — and What They Must Do

The 11 CER sectors

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- Public administration
- Space
- Food

Obligations of critical infrastructure

Risk assessment

Every 4 years, all risk types (cyber, physical, supply chain, employees, environment).

Resilience measures

Appropriate and proportionate technical and organizational measures.

Incident reporting

To the competent authority — deadline varies by Member State (DE: typically 24 hours).

Background checks

For sensitive positions (e.g., access to critical facilities).

Crisis management

EU Cyber Security Act

- The Cybersecurity Act grants ENISA its permanent mandate and establishes the framework within which European certification schemes for ICT products, services, and processes will be developed

Five EU schemes — one is operational

Scheme	Subject	Status
EUCC	ICT products based on Common Criteria, e.g. chips, smartcards, security hardware	Adopted by the Commission in 2024; certification possible since February 2025
EUCS	Cloud services at three assurance levels	In development; dispute over sovereignty requirements for the highest level
EU5G	Network equipment and operation of 5G networks	In development; resumption announced
EUDI Wallet	European Digital Identity Wallets	In development
EUMSS	Managed security services, e.g. SOC and incident response providers	In development; legal basis created by amending regulation

Link to the Cyber Resilience Act: a European certificate under one of these schemes can demonstrate a product's conformity with the CRA. For manufacturers, it pays to look at both legal acts together.

EUCC — the EU's product certification scheme

What it is

- First **operational** scheme under the Cybersecurity Act — applicable since **Feb 2025**
- Based on **Common Criteria** (ISO/IEC 15408) and ISO/IEC 18045
- Assurance levels **'substantial'** and **'high'**
- One certificate, valid EU-wide — replaces national SOG-IS/CC schemes (transition until **Feb 2027**)

Why it matters now

- Voluntary today — but the designated hook for **CRA critical products**
- Presumption of conformity & procurement differentiator under NIS2 supply-chain duties
- Issued by accredited certification bodies — [TÜV NORD / TUViT positioning & reference projects]

EUCS is coming — C5 is here

EUCS — the EU cloud scheme

- Candidate scheme under the Cybersecurity Act — **not yet adopted**
- Assurance levels basic / substantial / high
- Adoption delayed by the **sovereignty debate** (data localisation at level ‘high’)

The toolbox available today

- **BSI C5** — attestation (ISAE 3000), de-facto requirement for German public sector & regulated customers
- **ISO/IEC 27001** with 27017 / 27018 cloud & privacy controls
- National peers for context: SecNumCloud (FR), ENS (ES)

Pragmatic strategy: certify ISO/IEC 27001 and attest C5 now — the control sets map heavily onto the draft EUCS, so today’s evidence becomes tomorrow’s head start.

EU Regulation

Role of certifications (business perspective)

Certifications such as

- ISO 27001 (information security),
- ISO 22301 (business continuity),
- ISO 27701 (data protection management) and
- TISAX

are pragmatic tools for covering large parts of the EU requirements in a structured manner and providing external evidence of compliance.

One management system, many proofs

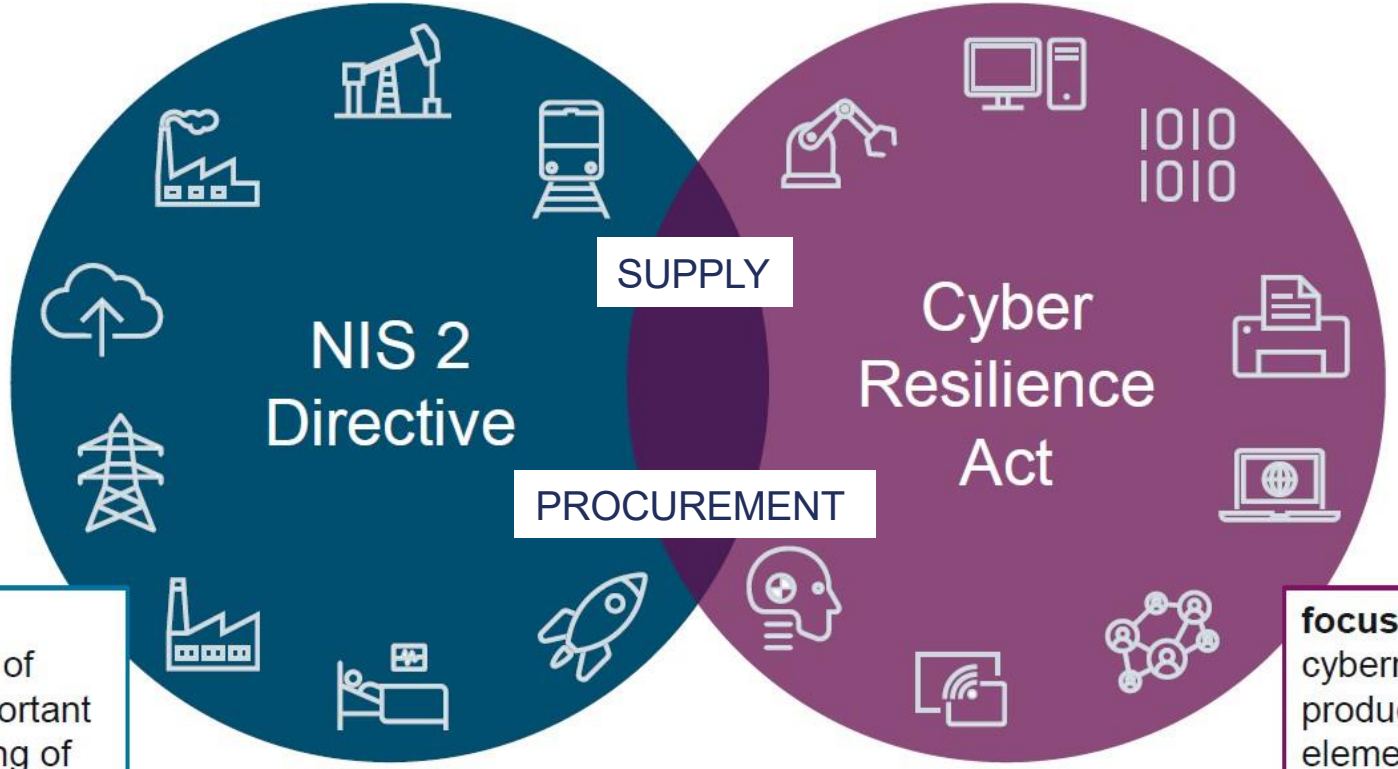
Obligation	Anchor standard	What certification demonstrates
NIS2 Art. 21	ISO/IEC 27001 ISMS	Risk measures, governance, audit-ready evidence for supervision
CER	ISO 22301 BCMS	Continuity, crisis management, all-hazards resilience
CRA Module H	ISO/IEC 27001 / ISO 9001 discipline	Audited quality & security system across the product lifecycle
Cloud (EUCS → today)	ISO/IEC 27001 + BSI C5	Customer assurance, public-sector market access
Privacy add-on	ISO/IEC 27701	GDPR-aligned privacy management

The message: you don’t build five compliance programmes — you build **one integrated management system** and let accredited certification turn it into recognised evidence.

Example Solutions for EU Regulation

NIS 2 and CRA Interplay

- ISO/IEC 27001
- TISAX
- ISA/IEC 62443-2-1
- ISO22301



- (EN 18031-1)
- ETSI EN 303 645
- ISA/IEC 62443-3-3
- ISA/IEC 62443-4-1
- ISA/IEC 62443-4-2
- Modul H (ISO27001/ISO9001)

OPERATOR

MANUFACTURER

CIO, CISO

focus:
cyberresilience of essential & important entities; reporting of cyber incidents; cyber risk mitigating measures

R&D, QA

focus:
cyberresilience of products with digital elements & vulnerability handling of manufacturers of those products

BDI

Source: BDI

What to do now — by role

Action Plan

Operators (NIS2 / CER)

1. Confirm scope & complete registration
2. Gap-assess against Art. 21 measures
3. Build or level up the ISMS to ISO/IEC 27001
4. Prepare evidence & audit readiness

Manufacturers (CRA)

1. Inventory & classify the product portfolio
2. Operate vulnerability handling & SRP reporting — live since Sep 2026
3. Choose the conformity route — evaluate **Module H** early
4. Engage a notified body in good time

Cloud providers

1. Certify ISO/IEC 27001 (+ 27017/27018)
2. Obtain / maintain a **C5 attestation**
3. Track EUCS — map controls when the scheme lands
4. Use attestations proactively in customer assurance

TÜVNORD

CYPRO

Poll 3

Where does your organisation stand on certification today?

- ISO/IEC 27001 certified
- Implementing an ISMS
- C5 / SOC 2 attested
- None yet
- Other

CYPRO

But...

...that's only half the story

TÜVNORD

EU regulations and directives on cyber security



CSA – European Cyber Security Act & European Cybersecurity Certification Framework

RED - Radio Equipment Directive

CRA – Cyber Resilience Act

5G Toolbox

EU RCE Directive

European Chips Act

Cyber Security for Vehicles

MDR - Medical Device Regulation

US IoT Cybersecurity Improvement Act 2020

GDPR - General Data Protection Regulation

Singapore Cyber Security Labeling Scheme

India Guidelines for IoT Security

eIDAS & **EUid** - Biometrics a.o.

MD - Machinery Directive

Digital Services Act

Toy Safety Directive

Finland Cyber Security Label

Japan Cyber-Physical Security Framework

ePrivacy Directive - Cookies and Communication

GPSR - General Product Safety Regulation

PSR – Payment service (former PSD2)

Green Deal: Circular Economy & Sustainability (life cycle of IoT devices)

LGPD Brazilian General Data Protection Law

Japan Basic Cybersecurity Act

EASA Delegated Regulation on unmanned aircraft systems (UAS)

Insurances wrt cybersecurity

Market Surveillance Regulation

AI Liability Directive

AI Act

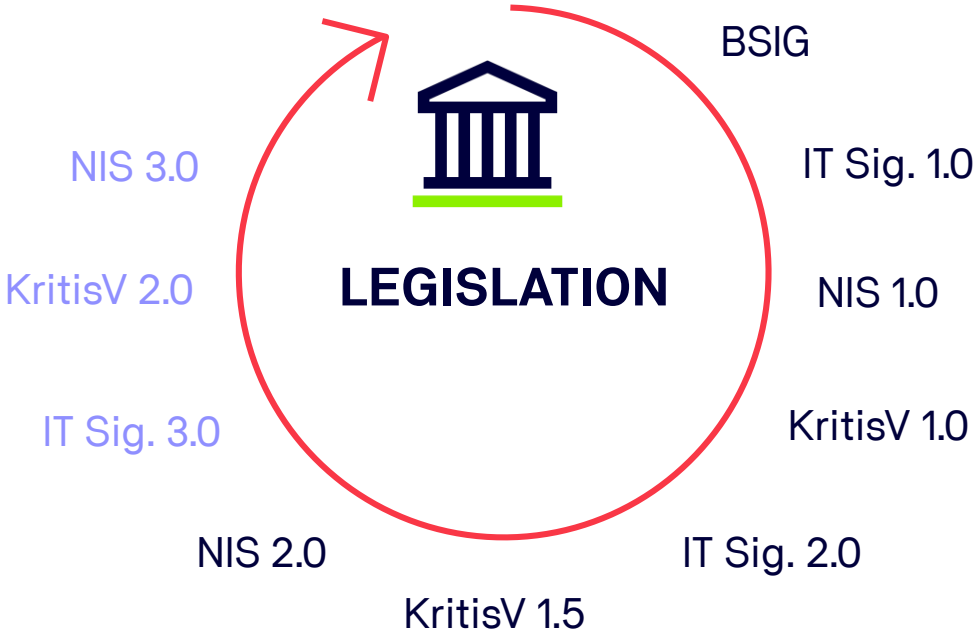
Product Liability Directive

OECD - Recommendation on Digital Security of Critical Activities

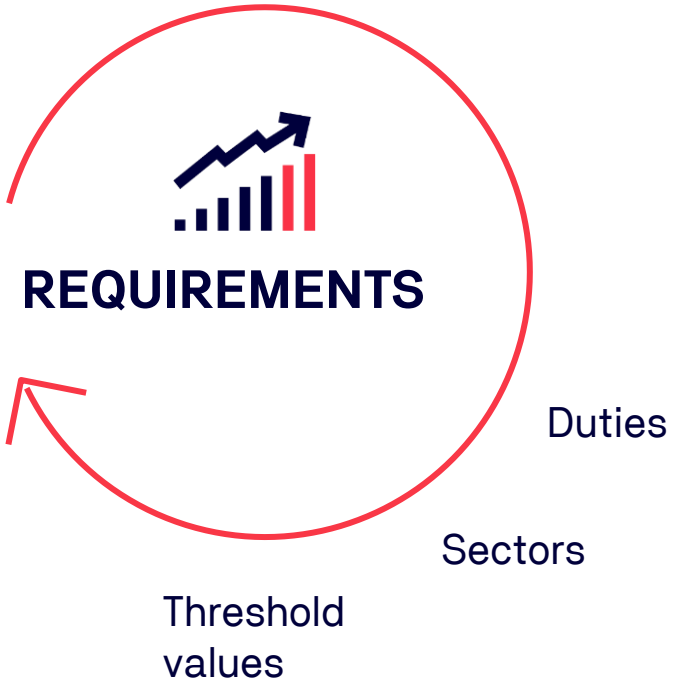
Conclusion

Legislation & IT security requirements/obligations are developing with increasing speed

Legislation is constantly changing...



IT security requirements will increase ....



... and obligations for companies are growing!



What will shape 2027?

Outlook



TÜVNORD

CYPRO

Questions?

tuev-nord.de