



Cyber Resilience Act (CRA) – Updates and current status

Michael Lang, Business Development Cybersecurity

30.09.2026

Your Speaker today

Michael LANG

Business Development Cybersecurity

✉ Michael.lang@nmi-testlab.de

 [Contact me on LinkedIn](#)

 [Contact me on Teams](#)

 [Book a meeting with me](#)

☎ Phone: +49-5235-9500-217

📱 Mobile: +49-151-54796845

<http://www.nmi-testlab.de/>





**Your accredited
Partner for
Qualification,
Testing and
Certification.**

www.nmi-testlab.de



Our Services

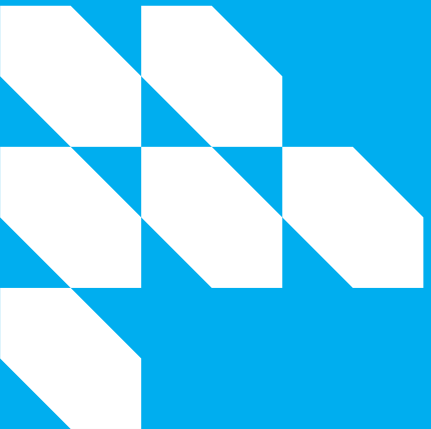
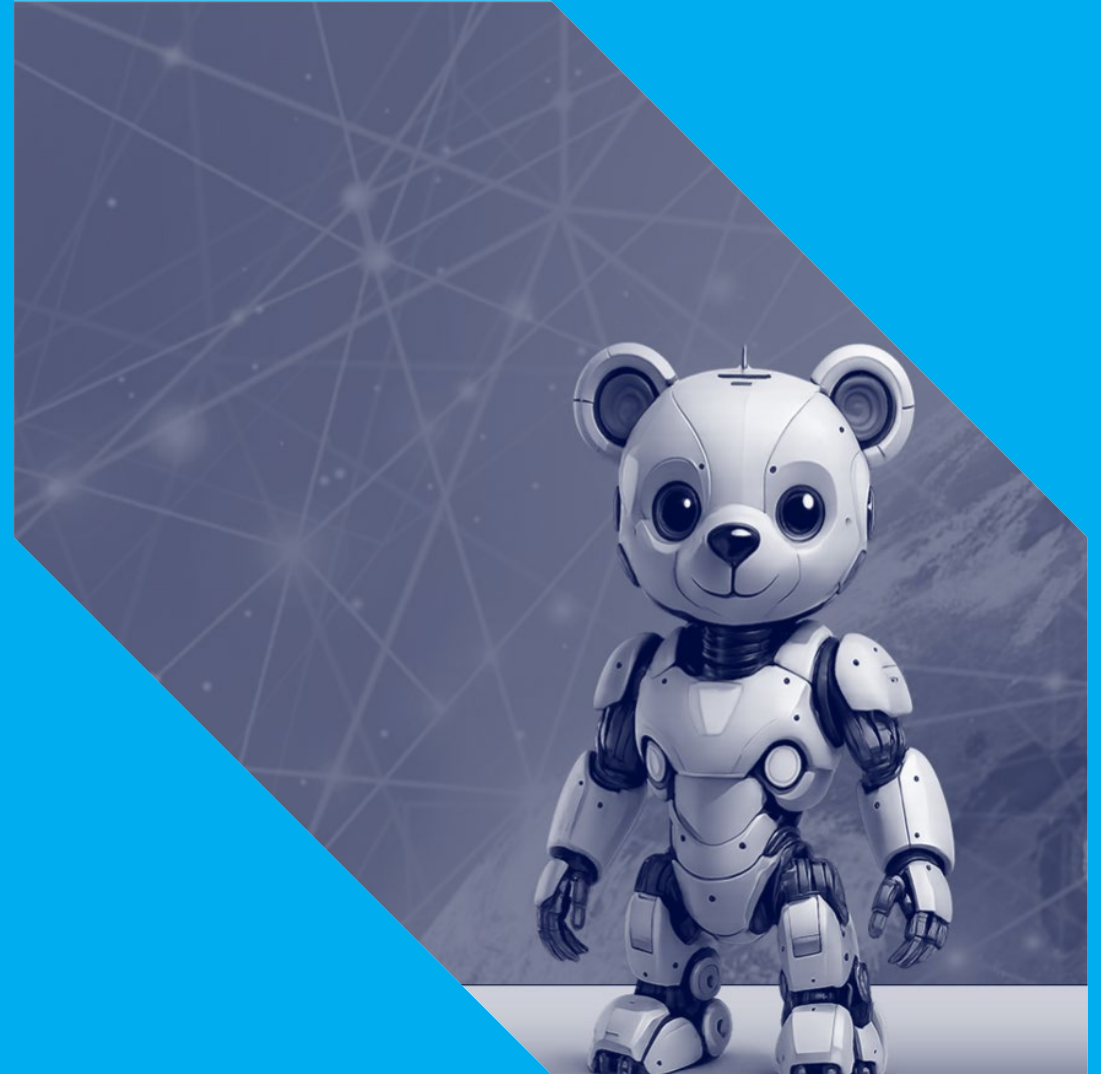
Product Testing

- ✦ EMC
- ✦ Environmental Simulation
- ✦ Electrical Device Safety
- ✦ Battery Testing
- ✦ Radio
- ✦ Cybersecurity
- ✦ Fieldbus

Market Access

- ✦ International Type Approval
- ✦ Notified Body EMC EU
- ✦ Notified Body MED EU
(Marine Equipment Directive)
- ✦ Shipbuilding Classifications
- ✦ Product Certification Radio
 - ✦ Notified Body RED EU
 - ✦ TCB FCC USA
 - ✦ FCB ISSED Canada
 - ✦ RCB MIC Japan

Cyber Security – Regulatory Overview



2016: The trigger for stricter cybersecurity in the EU

My Friend Cayla: Vernichten Sie diese Puppe



[My Friend Cayla: Vernichten Sie diese Puppe | DIE ZEIT](#)

The Bright-Eyed Talking Doll That Just Might Be a Spy

Share full article



[The Bright-Eyed Talking Doll That Just Might Be a Spy - The New York Times](#)

Regulator tells parents to destroy 'spy' doll

A German regulator has warned parents of the dangers of a children's toy called My Friend Cayla. The doll, capable of revealing personal data, is a de facto "espionage device," a federal agency said.

Depending on who you ask, there will either be one less doll to play with or [one less spy device in kids' rooms](#).

Germany's Federal Network Agency, or Bundesnetzagentur, said on Friday it was prohibiting retailers from selling My Friend Cayla, which garnered controversy last year over built-in technology that experts said allowed it to effectively spy on children. The government forbids illicit radio transmission equipment in toys.

[DW: Regulator tells parents to destroy 'spy' doll](#)

JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht

Home | Suche | JurPC in der Wikipedia | JurPC in der Rechtsprechung | Autoren | Statistik | Impressum

Home | JurPC Web-Dok. 13/2017

"My friend Cayla" - eine nach § 90 TKG verbotene Sendeanlage?

Gericht:	Stefan Hessel *
Typ:	Beitrag
Fundstelle:	JurPC Web-Dok. 13/2017
Autor(en):	Hessel, Stefan
Zitiervorschlag:	Stefan Hessel *, JurPC Web-Dok. 13/2017, Abs. 1

["My friend Cayla" - eine nach § 90 TKG verbotene Sendeanlage? – JurPC](#)

[EU & US consumer take action against flawed connected toys | BEUC](#)

My Friend Cayla



© myfriendcayla.de



EU market access

Cybersecurity is a market access criterion in the EU.

Increasing connectivity of products (IoT, industry, wireless)

New binding EU regulations

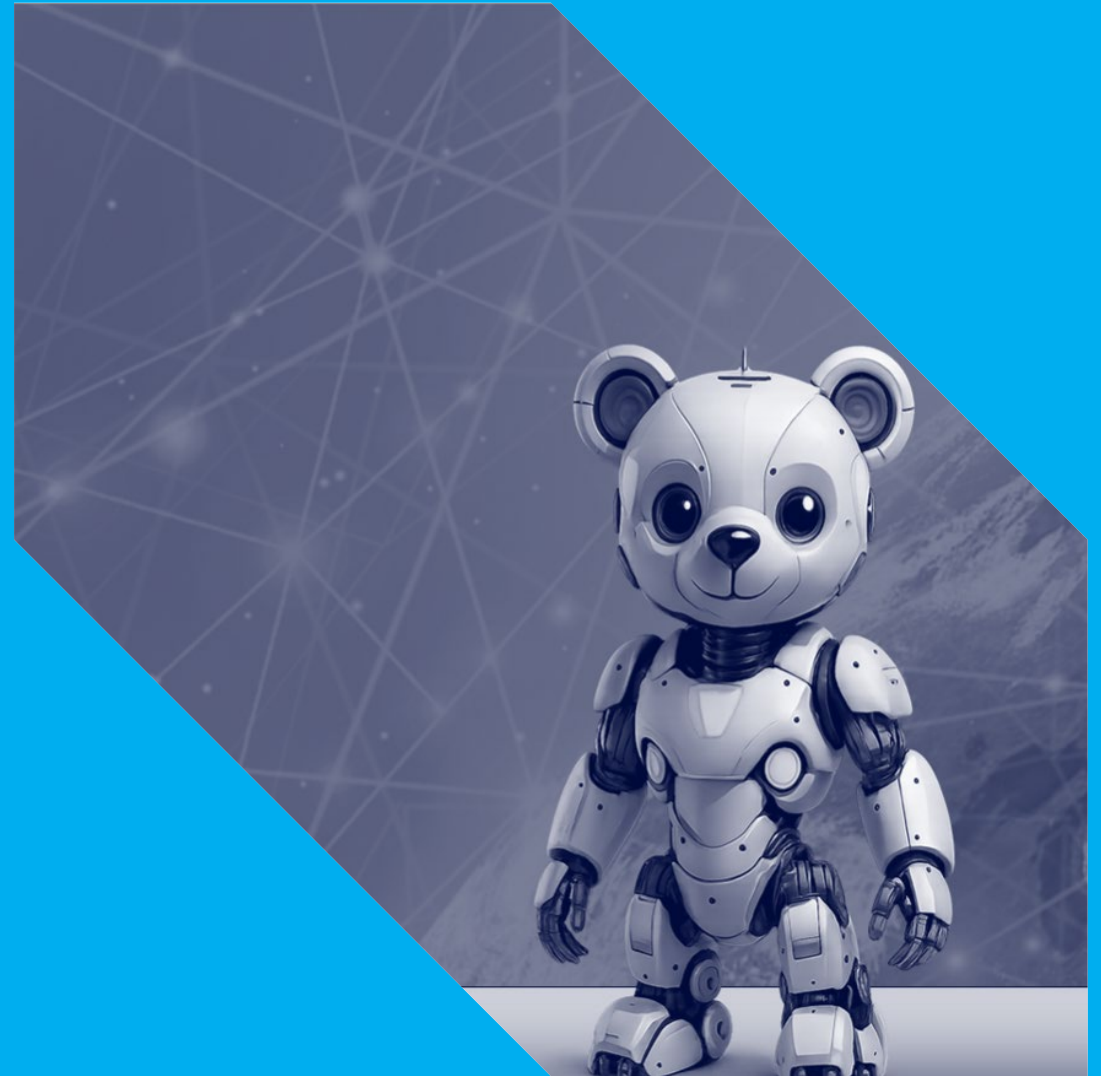
- Radio Equipment Directive (RED) – Active since 01.08.2025
- Cyber Resilience Act (CRA) – Active from 11.12.2027

High risks associated with

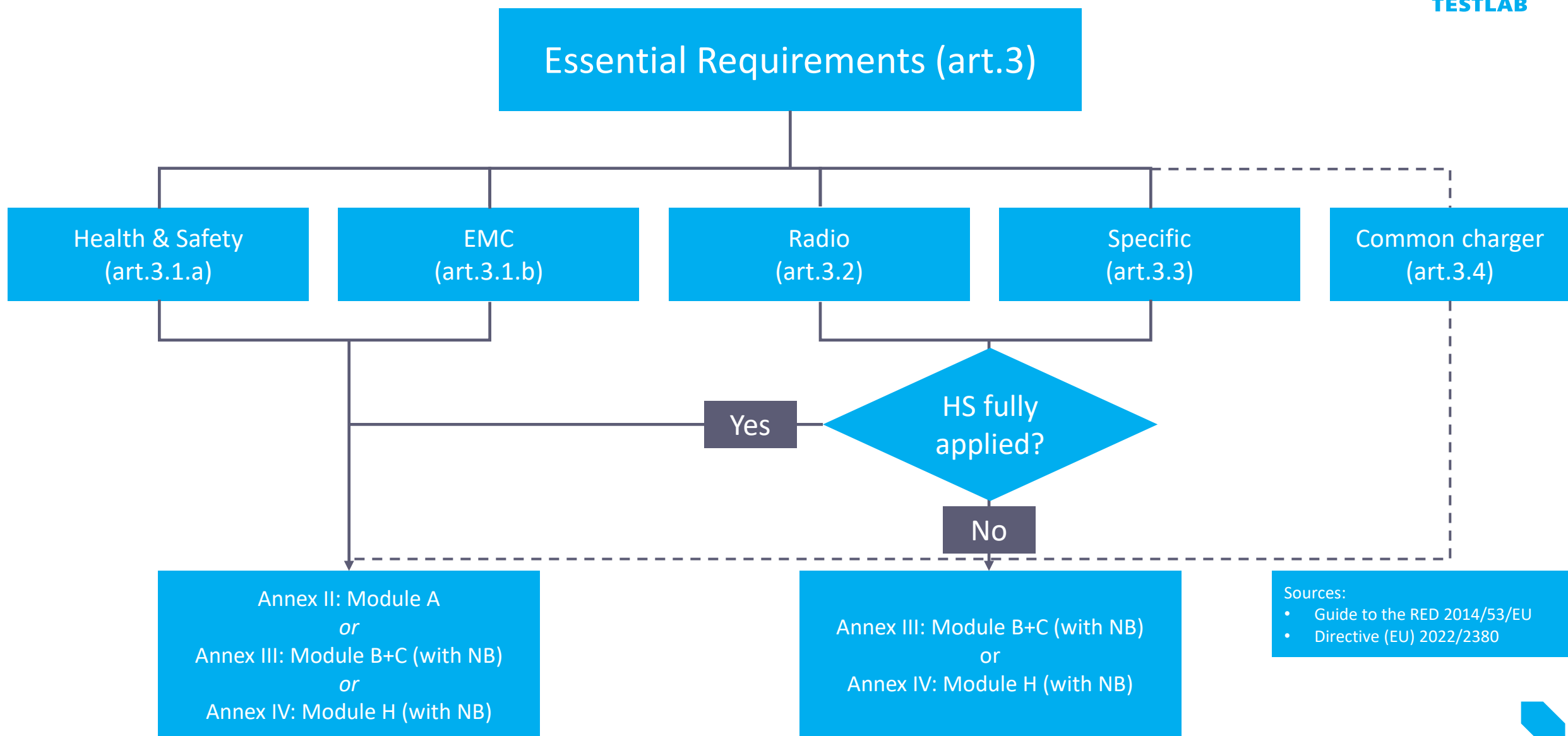
- Unclear requirements
- Late-stage security assessment
- Delayed or failed market access



Cyber Security – Radio Equipment Directive (RED)



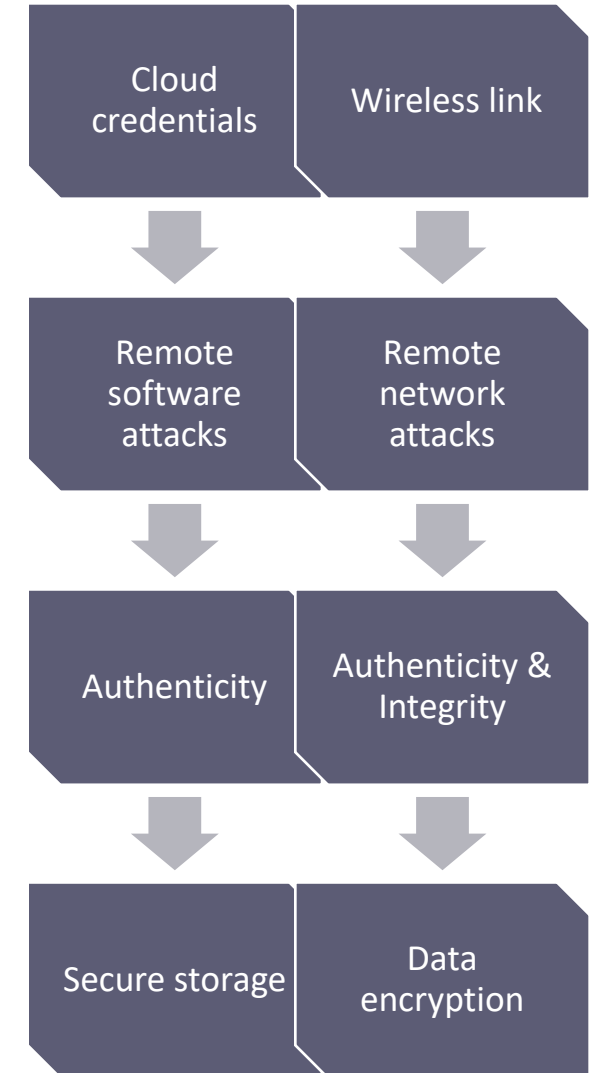
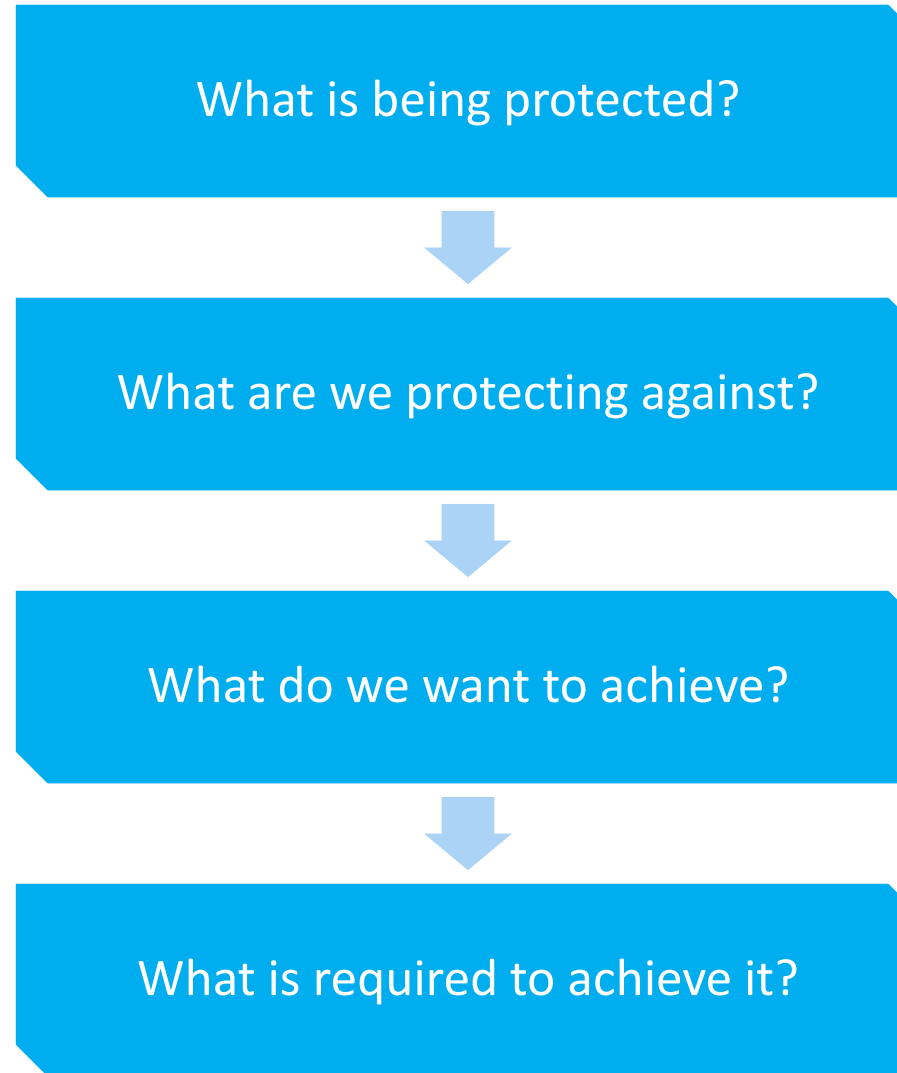
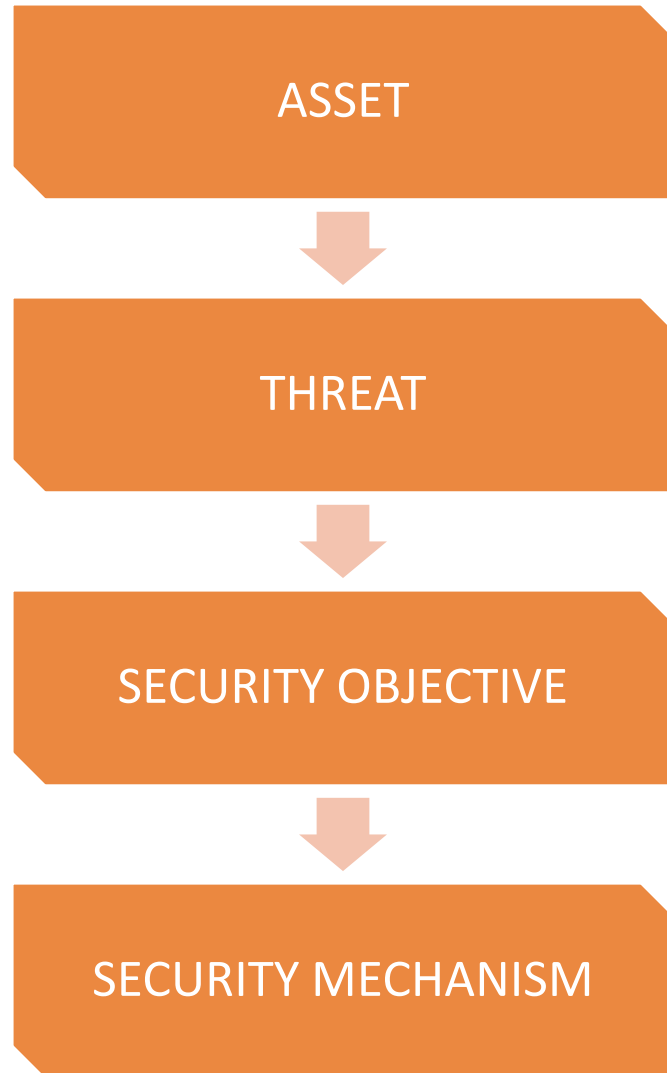
RED-Aspects = Essential Requirements = Risks!



Radio Equipment Directive and Cybersecurity



RED logic



Standard EN 18031-X

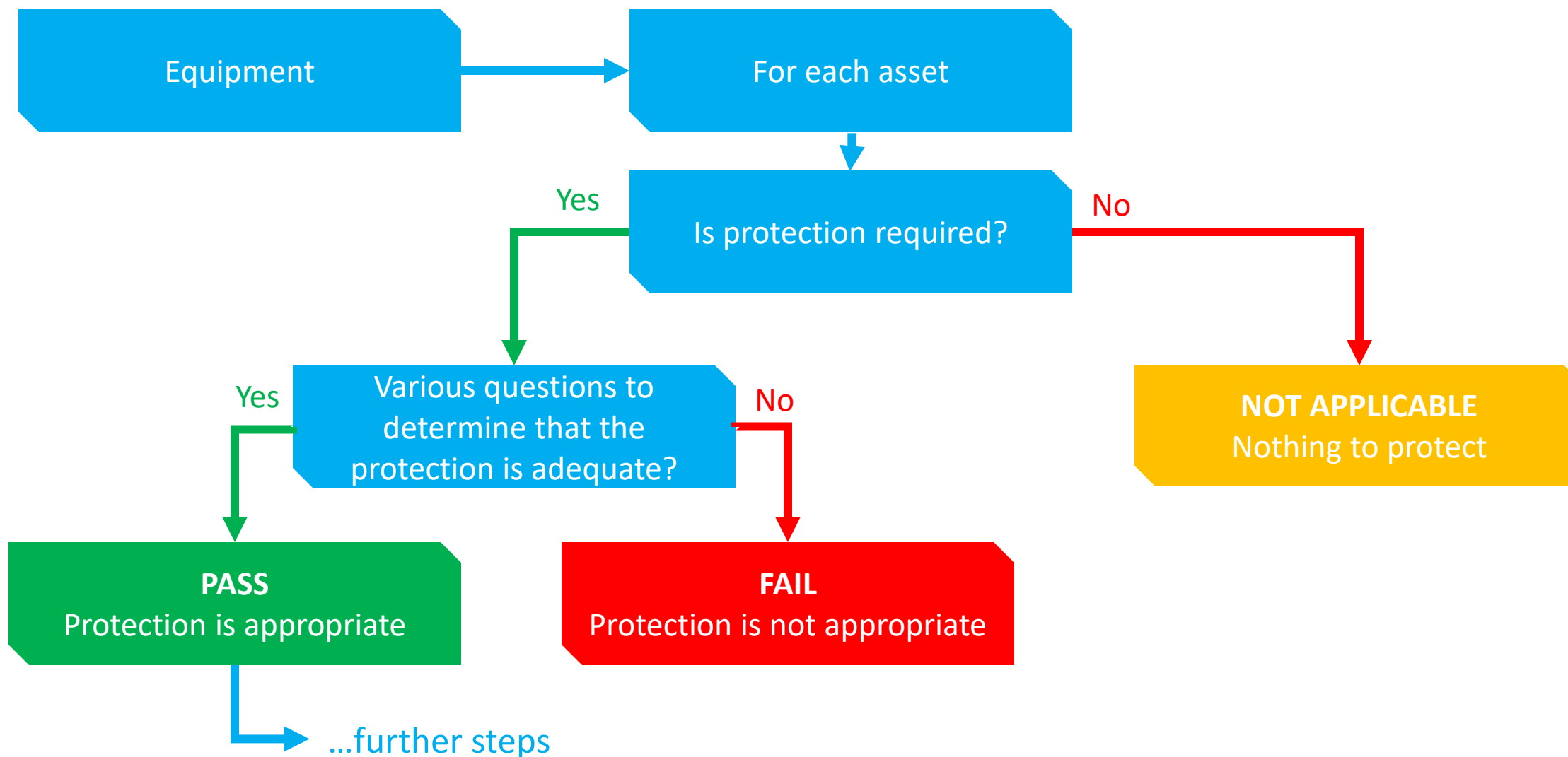
To ensure that the requirements can be harmonised, assets have been introduced as the main targets to which the requirements are to be applied.

Essential requirements	EN 18031-1 RED 3.3 (d)	EN 18031-2 RED 3.3 (e)	EN 18031-3 RED 3.3 (f)
Security asset	☒	☒	☒
Network asset	☒	☒	☒
Privacy asset	☒	☒	☒
Financial asset	☒	☒	☒

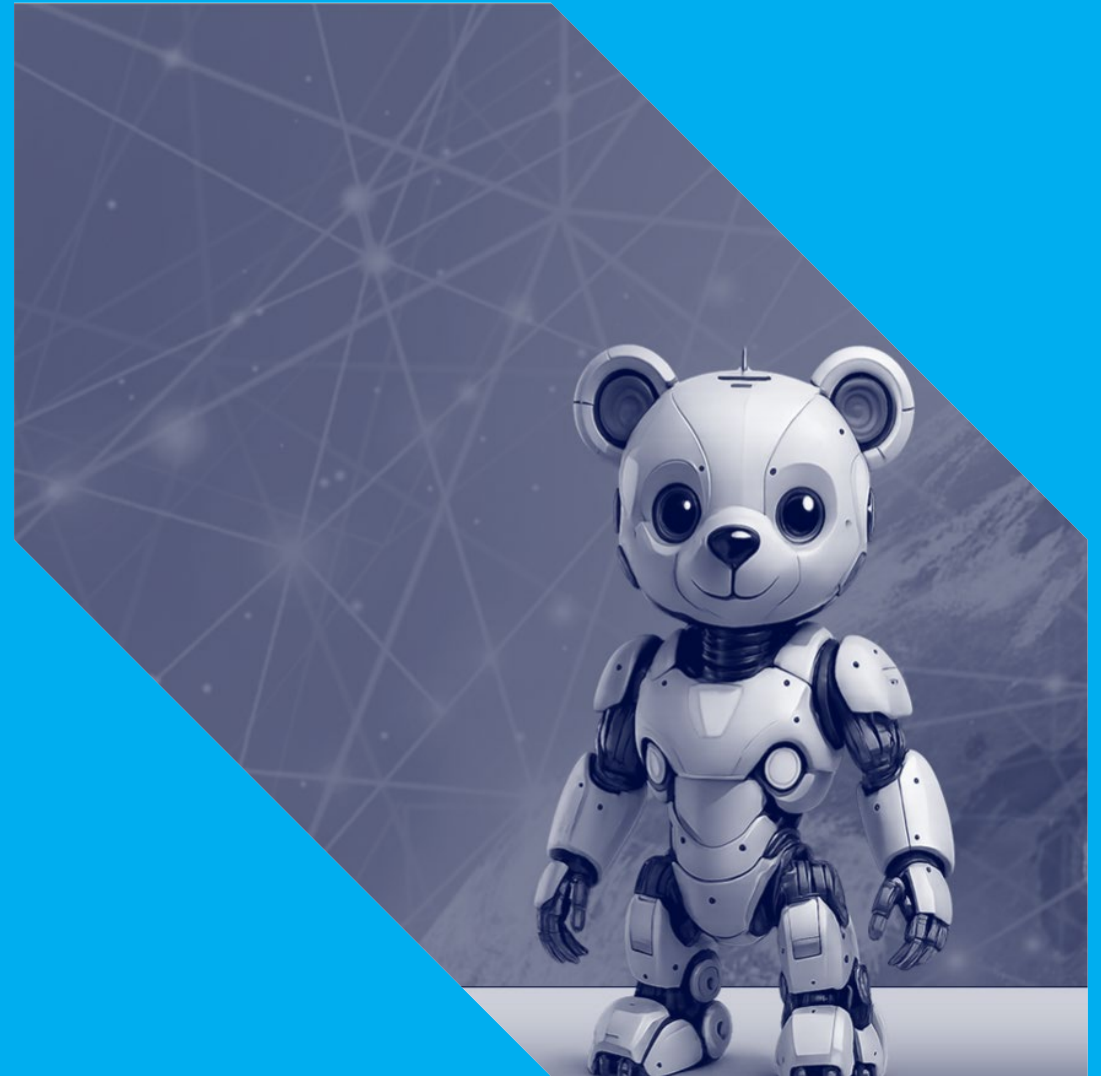
Requirements of EN 18031-X

Abbreviation	Mechanism	EN 18031-1	EN 18031-2	EN 18031-3
ACM	Access control mechanism	✓	✓	✓
AUM	Mechanism for authentication	✓	✓	✓
SUM	Secure update mechanism	✓	✓	✓
SSM	Secure storage mechanism	✓	✓	✓
SCM	Mechanism for secure communication	✓	✓	✓
RLM	Resilience / Fail-safe mechanism	✓	✗	✗
LGM	Mechanism for logging	✗	✓	✓
NMM	Network monitoring mechanism	✓	✗	✗
DLM	Mechanism for deleting data	✗	✓	✗
TCM	Traffic control mechanism	✓	✗	✗
UNM	Mechanism for notifying users	✗	✓	✗
CCK	Confidential cryptographic keys	✓	✓	✓
GEC	General equipment features / capabilities	✓	✓	✓
CRY	Cryptography	✓	✓	✓

Decision Trees



Cyber Security – Cyber Resilience Act (CRA)





CRA

Concept

The CRA is a Regulation, not a certification framework

WHAT IT IS

A legal requirement for every product with digital elements on the EU market

Defines

- **essential requirements** in Annex I Part I
- **vulnerability handling** in Annex I Part II

Classifies products into

- Default,
- Important I,
- Important II and
- Critical

WHAT IT IS NOT

- **No harmonised standards**
None of the well-known standards satisfy all CRA requirements; IEC 62443 is not harmonised under the CRA
- **Not a certification scheme**
certification schemes (e.g. EUCC, etc.) can be used to support it
- **Not optional** if your product with digital elements is or existing on the EU market. (Products with digital elements on the market before 12/11/2027 are subject to the CRA only if they undergo a substantial modification from that date onwards.)

The CRA tells you what your product must achieve. Conformity modules tell you how to verify it

Scope: "Products with digital elements"



Hardware products (including components already on the market)
(laptops, smart devices, mobile phones, network equipment, or CPUs...)



Software products (including components already on the market)
(operating systems, word processing, games or mobile apps, software libraries...)

... including their **remote data processing solutions!**



Outside the scope of application



Non-commercial products
("hobby products")



Services, particularly standalone "Software as a Service" (SaaS) services (websites, purely web-based offerings...)



Complete exclusions for certain products:

▀ vehicle type approval [EU 2019/2144]

▀ aviation equipment [EU 2018/1139]

▀ medical devices [EU 2017/745]

▀ marine equipment [EU 2014/90]

▀ in vitro diagnostics [EU 2017/746]



Annex I, Part I – Essential cybersecurity requirements

1

Products with digital elements are designed, developed and manufactured to ensure an adequate level of cybersecurity in the face of the risks.

2

Based on the cybersecurity risk assessment referred to in Article 13(2), products with digital elements, where applicable, shall comply with the following requirements:

a	With no known exploitable vulnerabilities	b	Secure default configuration	c	Security Updates
d	Protection against unauthorized access	e	Confidentiality of data	f	Integrity of data
g	Data minimization	h	Ensure availability	i	Minimization of negative effects
j	Low attack surfaces	k	Mitigating the impact of a security incident	l	Provide security-related information
m	Secure deletion and transmission				

BENEFITS OF THESE REQUIREMENTS: Protection of users and their data · Increasing the trustworthiness and reliability of products · Strengthening society's digital resilience · Supporting a secure and trustworthy Digital Single Market in Europe



Annex I, Part II – Vulnerability Handling Requirements

1

Identify and document vulnerabilities and components

2

Troubleshoot and fix vulnerabilities

3

Test and review security regularly

4

Share and publish information about vulnerabilities that have been eliminated

5

Coordinated vulnerability disclosure strategy

6

Facilitating the exchange of information and providing contact address

7

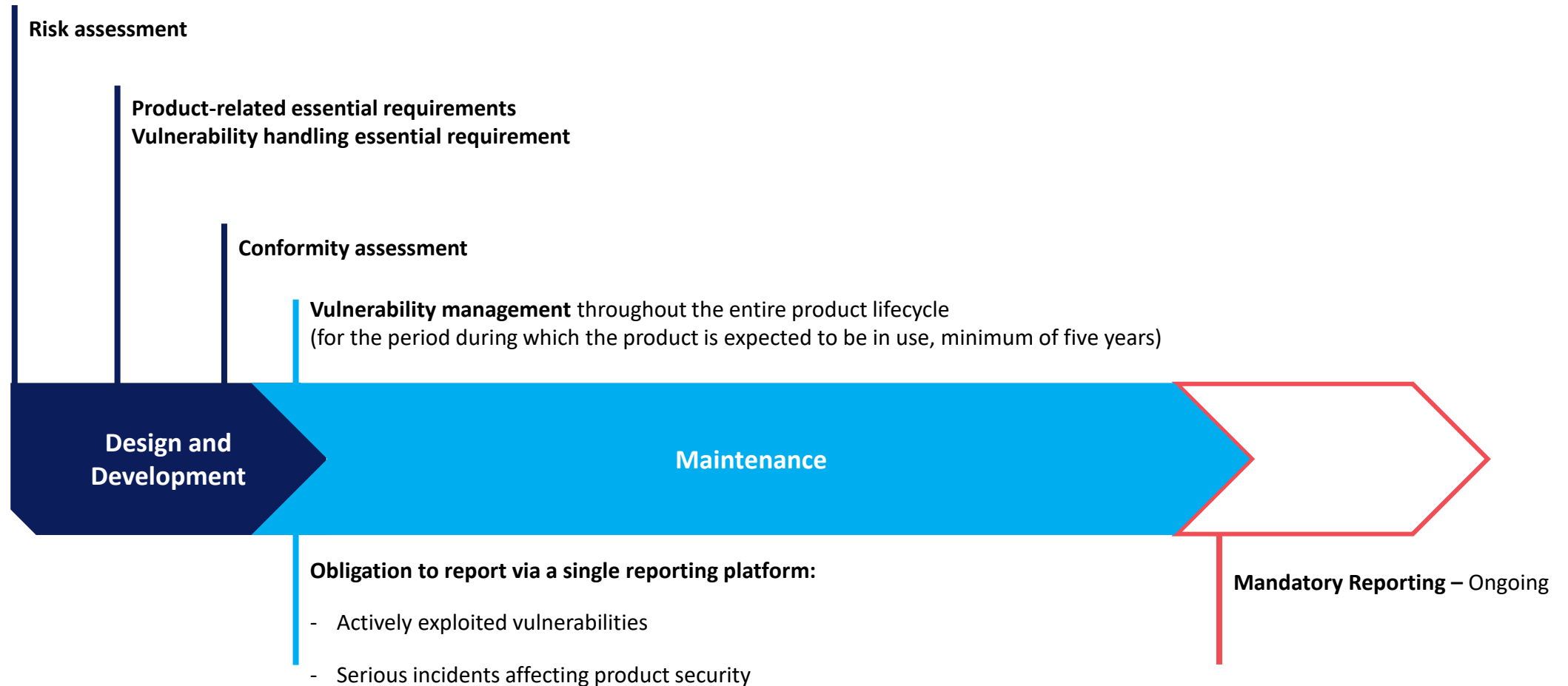
**Security UpdateEnsure secure distribution of updates
Proposals**

8

Provide security updates instantly and free of charge

GOAL: Quickly identify vulnerabilities, remedy them effectively and communicate them transparently – for more security and trust. · Rapid response to risks · Protection of users and data · Strengthening transparency and trust · Secure digital single market and resilient products

Obligations of manufacturers – General



CRA

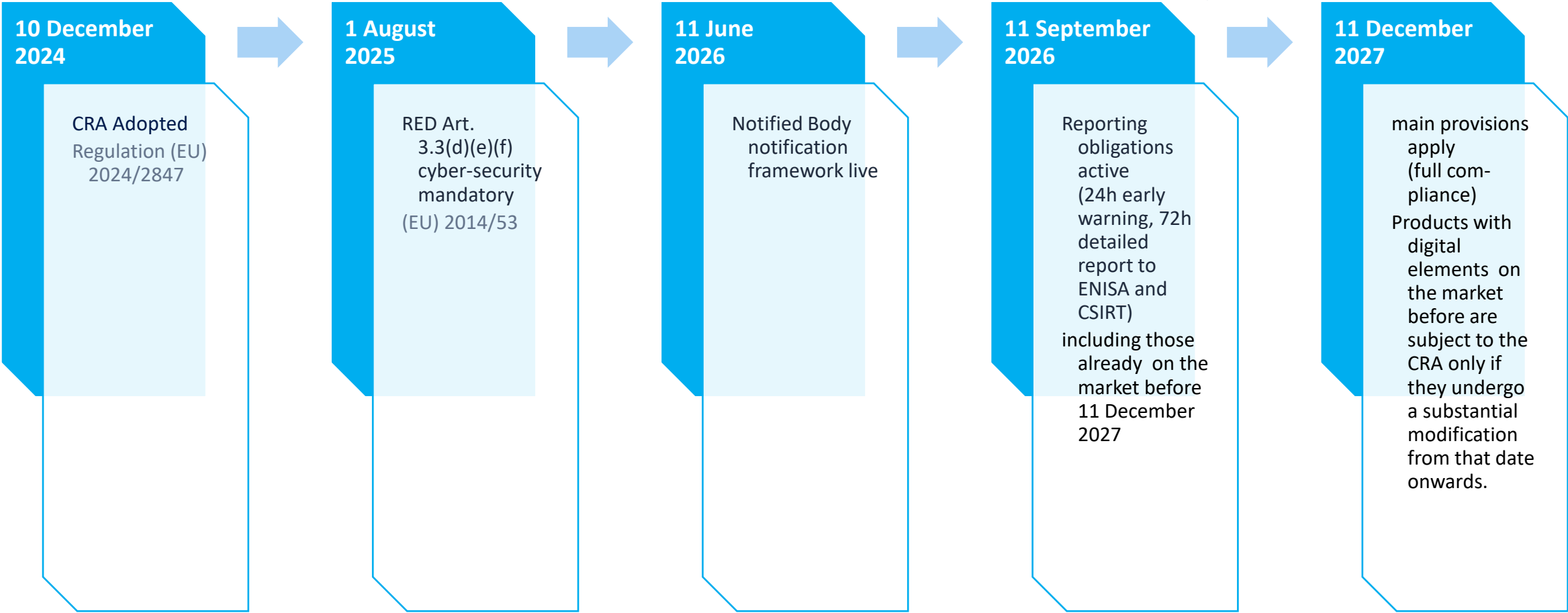
Timeline

The CRA adoption is around the corner

8
Days
active*



438
Days
left*



* Calculation date: 30/09/26

Two dark blue geometric shapes, resembling stylized tabs or flags, positioned at the top left of the white content area.

CRA

The four product classes

How real products map to the four classes

Default

Consumer electronics | Simple embedded devices | Basic software tools

Important Class I

Web browsers | Password managers | VPN software | SIEM systems | etc.

Important Class II

Firewalls, IDS/IPS | Hypervisors / container runtime | Tamper-resistant microprocessors |
Tamper-resistant microcontrollers

Critical

Hardware devices with security boxes (HSMs) | Smart meter gateways | Smart cards and
secure elements

Classification follows the product's core functionality, not incidental features. Integrating a secure element or a browser does not reclassify the product



product categories

Important Class I (19*)	identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
	standalone and embedded browsers
	password managers
	software that searches for, removes, or quarantines malicious software
	products with digital elements with the function of virtual private network (VPN)
	network management systems
	Security information and event management (SIEM) systems
	boot managers
	Public key infrastructure and digital certificate issuance software
	Physical and virtual network interfaces
	Operating systems
	Routers, modems intended for the connection to the internet, and switches
	Microprocessors/Microcontrollers with security-related functionalities
	Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
	Smart home general purpose virtual assistants/ Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
	Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (social interactive features (e.g. speaking or filming) or that have location tracking features
	Personal wearable products to be worn or on a human body that have a health monitoring (such as tracking) purpose, or personal wearable products that are intended for the use by and for children

Important Class II (4*)	Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
	Firewalls, intrusion detection and prevention systems
	Tamper-resistant microprocessors/ microcontrollers
Critical (3)	Hardware Devices with Security Boxes
	Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
	Smartcards or similar devices, including secure elements

*some entries are merged





CRA

Requested Standards

Requested standards

Horizontal standards (1–15)

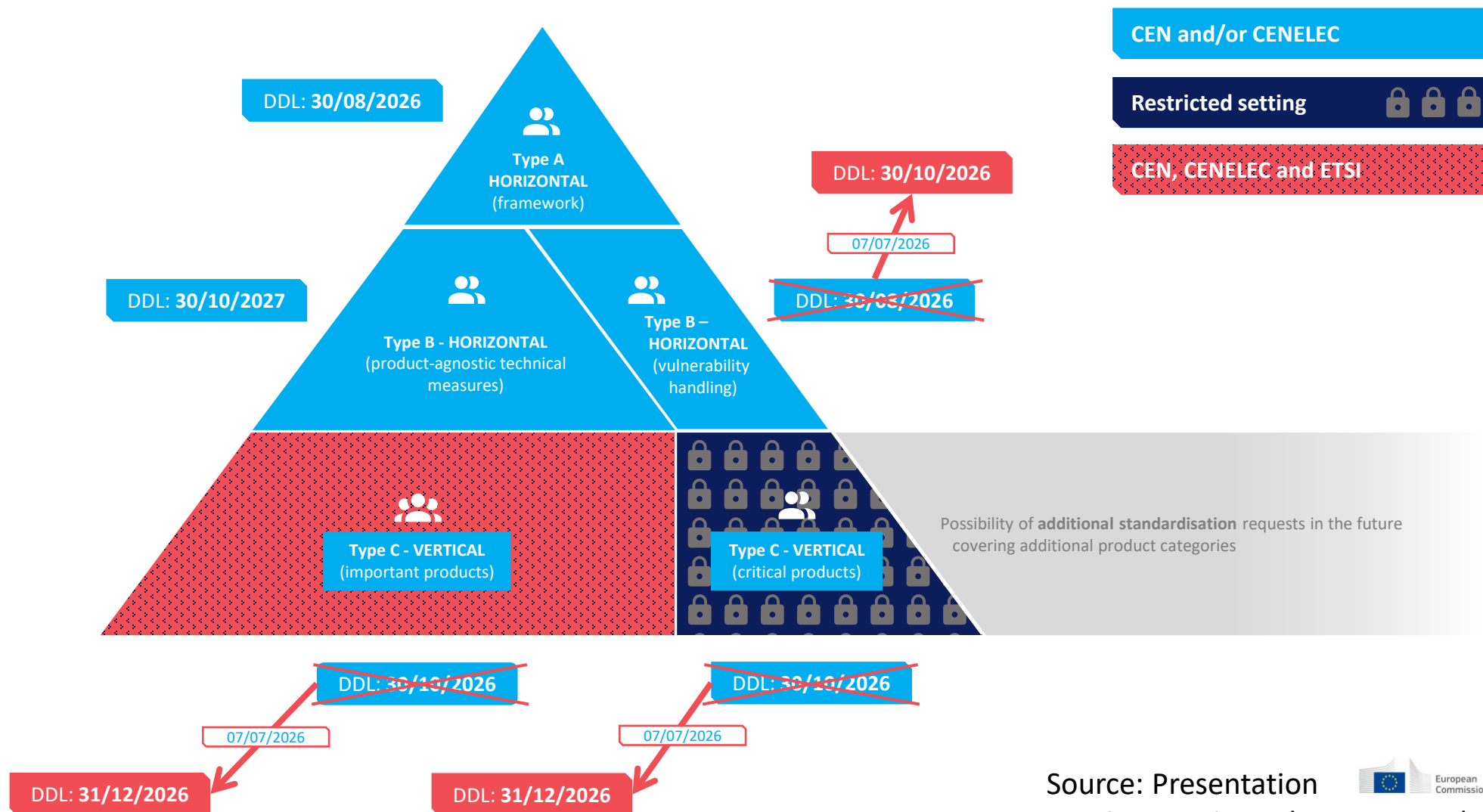
- Risk-based approach (CRA Annex I)
- Essential requirements (CRA Annex I, Part 1)
- Handling of vulnerabilities (CRA Annex I, Part 2)

Vertical standards (16–41)

- Important products – Class 1 (CRA Annex III)
- Important products – Class 2 (CRA Annex III)
- Critical products (CRA Annex IV)



CRA standardisation request in a nutshell



Harmonised standards give presumption of conformity (But so far no standard is harmonised on CRA)

Standard	Scope	Status	Deadline
EN 40000-1-1	Vocabulary	Drafting	30 Oct 2026
EN 40000-1-2	Principles for Cyber Resilience (Annex I Part I)	Drafting	30 Oct 2026
EN 40000-1-3	Vulnerability Handling (Annex I Part II)	Drafting	30 Oct 2026
EN 40000-1-4	Generic Security Requirements	Drafting	30 Oct 2027
ETSI EN 304 6xx series	Class I verticals (browsers, password mgrs, etc.)	Drafting	31 Dec 2026
EN 18031-1/2/3	RED cybersecurity (radio equipment)	Published	Active now (but not on CRA)

If you apply a harmonised standard correctly, you have presumption of conformity with the CRA.

Note:

EN 18031 is harmonised under RED, not CRA. It serves as a bridge standard until standards published.

Mapping RED Art. 3.3 → CRA

RED	CRA
[GEC] General equipment capabilities	(a) No known vulnerabilities
No mapping	(b) Secure default configuration
[SUM] Secure update mechanism	(c) Security updates
[ACM] Access control mechanism	(d) Authorized access
[AUM] Authentication mechanism	
[SSM] Secure storage mechanism	
[SCM] Secure communication mechanism	(e) Confidentiality
[CCK] Confidential cryptographic keys	
[CRY] Cryptography	
[SSM] Secure storage mechanism	(f) Integrity
[SCM] Secure communication mechanism	
No mapping	(g) Data minimization
[RLM] Resilience mechanism	(h) Availability of products functions
[GEC-8] General equipment capabilities	(i) Availability of environment
[LIM] External impact limitation	(i) Attack surface minimization
[GEC] General equipment capabilities	(k) Incident impact reduction
No mapping	
[LGM] Logging mechanism	
INMM] Network monitoring mechanism	(l) Recording and monitoring
[CM] Traffic control mechanism	
[MON] Recording and monitoring	
[DLM] Deletion mechanism	(m) Secure deletion

Vertical Standards

1	EN18 304-617 V1.0.0 2026-08-12 Browsers Enquiry-draft.pdf	2026-08-13 12:52
2	EN 304-618 V0.2.2 2026-06-22 Password-managers Enquiry-draft.pdf	2026-06-22 16:15
3	EN 304-619 V1.0.0 2026-07-15 Antivirus-Enquiry-draft.pdf	2026-07-16 7:45
4	EN 304-620 v1.0.0 2026-08-12 Virtual-Private-Networks Enquiry-draft.pdf	2026-08-12 13:19
5	EN 304-621 V1.0.5 2026-08-12 Network-Management-Systems Enquiry-draft.pdf	2026-08-12 7:53
6	EN 304-622 V1.0.0 2026-08-12 Security-Information-Event-Management Enquiry-draft.pdf	2026-08-12 13:22
7	EN 304-623 V0.1.3 2026-06-17 Boot Managers Enquiry-draft.pdf	2026-06-22 16:15
8	EN 304-624 V1.0.0 2026-08-05 PKI certificate issuance software Enquiry-draft.pdf	2026-08-05 14:34
9	EN 304-625 V1.0.0 2026-08-10 Network-Interfaces Enquiry-draft.pdf	2026-08-10 9:06
10	EN 304-626 V1.0.1 2026-08-12 Operating-Systems Enquiry-draft.pdf	2026-08-12 13:24
11	EN 304-627 V1.0.1 2026-07-06 Routers-modems-switches Enquiry-draft.pdf	2026-07-06 16:19
12	EN 304-631 V1.0.0 2026-07-20 Smart-home-virtual-assistants Enquiry-draft.pdf	2026-07-29 17:57
13	EN 304-632 V1.0.0 2026-07-20 Smart-home-security-products Enquiry-draft.pdf	2026-07-29 17:56
14	EN 304-633 V1.0.0 2026-07-20 Internet-connected-toys Enquiry-Draft.pdf	2026-07-29 17:55
15	EN 304-634 V1.0.0 2026-07-24 Personal-wearables Enquiry-draft.pdf	2026-07-29 17:48
16	EN 304-635 V1.0.1 2026-06-24 Virtualization Container Enquiry-draft.pdf	2026-06-24 7:44
17	EN 304-636 V1.0.0 2026-07-09 Firewalls Enquiry-draft.pdf	2026-07-09 14:49

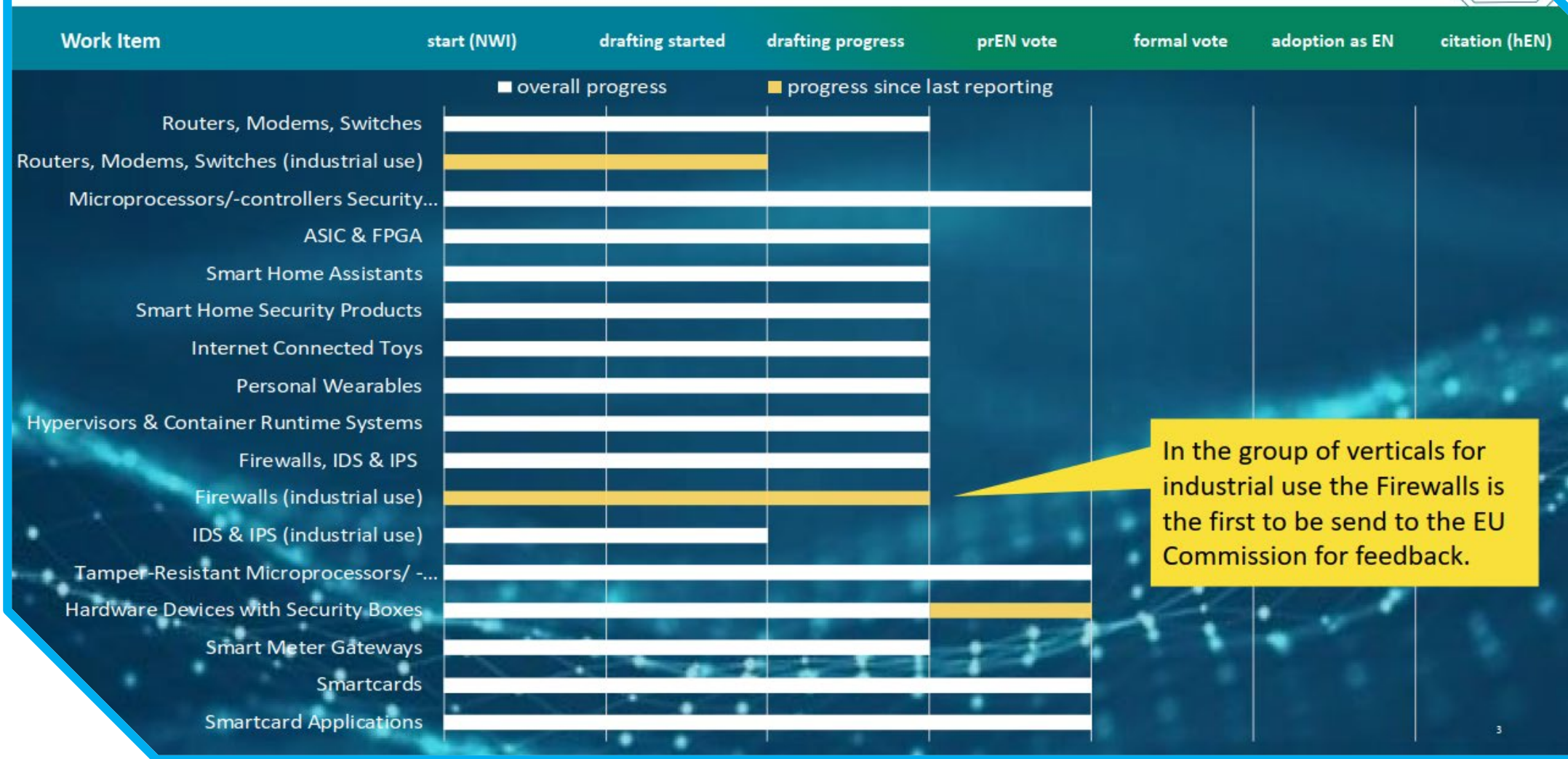
CRA Standardisation Dashboard

Reporting period: 04-06/2026 (last reporting 01-03/2026)



CRA Standardisation Dashboard

Reporting period: 04-06/2026 (last reporting 01-03/2026)



new guidance to support timely CRA implementation

07/27/2026 – EU Commission

[Commission publishes new guidance to support timely Cyber Resilience Act implementation | Shaping Europe's digital future](#)



[C\(2026\) 5252 - Communication on the Cyber Resilience Act \(CRA\) guidance](#)



[C\(2026\) 5252 - Annex - Commission guidance on the application of the Cyber Resilience Act \(CRA\)](#)



IEC 62443 is not harmonised under the CRA

WHAT IT GIVES YOU

- IEC 62443-4-1: a strong secure **development lifecycle process** framework
- IEC 62443-4-2: technical security **requirements for components** (SL1 through SL4)
- IEC 62443-6-2: a security **evaluation methodology** for IEC 62443-4-2
- A defensible narrative for your secure **development practices**
- Strong fit for IACS and OT products that are Important Class II

WHAT IT DOES **NOT** DO

- Provide **presumption of conformity** with the CRA on its own
- Replace a Notified Body** conformity assessment for Class II
- Cover vulnerability handling** to the depth Annex I Part II requires
- Satisfy** CVD (Article 14) or reporting (Article 14) **obligations automatically**

Use IEC 62443 as evidence alongside the CRA route. Do not present it as the CRA route.



CRA

Vulnerability Handling

From 11 September 2026 you have hours, not days

24h

EARLY WARNING

Notify [ENISA](#) and national CSIRT once you become aware of an actively exploited vulnerability or severe incident

72h

DETAILED REPORT

Provide initial assessment, severity, exploitation status, and corrective measures taken or planned

14d

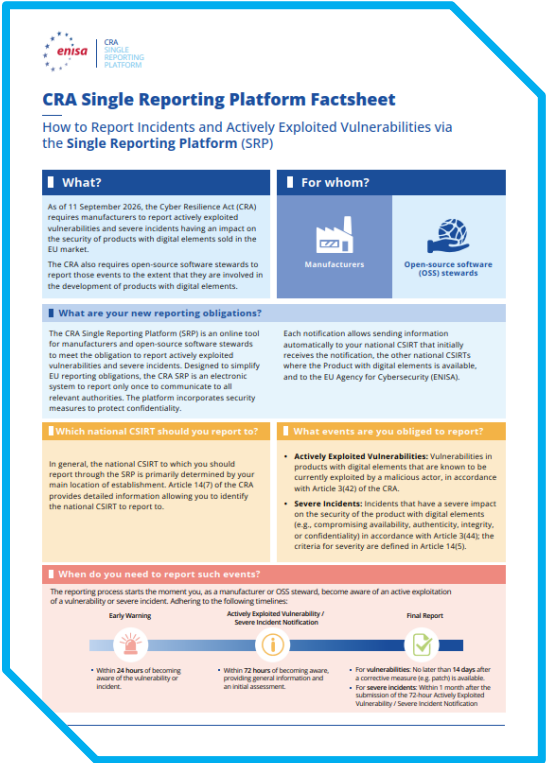
FINAL REPORT

Root cause, mitigation, and long-term corrective actions applied to the product and similar products

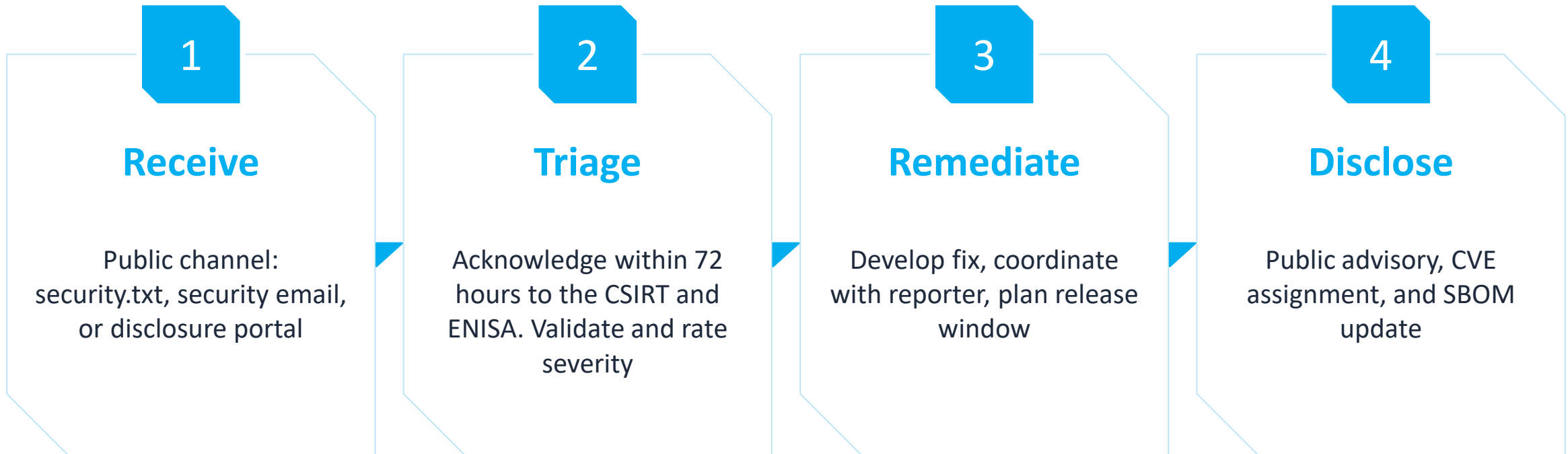
Article 14 reporting applies to actively exploited vulnerabilities and severe incidents.



CRA Single Reporting Platform (SRP)



Coordinated Vulnerability Disclosure is a process, not a document



Annex I Part II (6) requires a public disclosure channel, timely acknowledgment, and coordinated handling.



Two dark blue geometric shapes, resembling stylized tabs or flags, positioned at the top left of the white content area.

CRA

Conformity

Four routes, chosen by classification and applicable standards

MODULE A	MODULE B+C	MODULE H	EUCC SCHEME
Internal production control	Type examination + conformity	Full quality assurance	EU Common Criteria-based cybersecurity certification
WHO Default, Class I with harmonised standards	WHO Class I without harmonised, Class II	WHO Class I without harmonised, Class II	WHO Critical (Annex IV) products
EVIDENCE Manufacturer self-declares. Full technical file still required.	EVIDENCE Notified Body examines a type sample. Manufacturer ensures serial conformity.	EVIDENCE Notified Body audits the full QMS. Surveillance audits ongoing.	EVIDENCE Scheme under Regulation (EU) 2019/881 with ‘basic’, ‘substantial’ or ‘high’ assurance level. EUCC adopted today; others in development. ITSEF required.



Classification determines the conformity route

MODULE A Internal production control	MODULE B+C Type examination + conformity	MODULE H Full quality assurance	EUCC SCHEME EU Common Criteria-based cybersecurity certification
LOW RISK DEFAULT Annex I Conformity route Module A (self-declaration) recommended is a harmonised standard Module B+C or H	MEDIUM RISK IMPORTANT CLASS I Annex I + Annex III Part I Conformity route Module B+C or H, Application of existing Standard or 3rd party Assessment	HIGH RISK IMPORTANT CLASS II Annex I + Annex III Part II Conformity route Module B+C or H Notified Body	VERY HIGH RISK CRITICAL Annex I + Annex IV Conformity route Must have EU cybersecurity certification scheme, Notified Body

Two dark blue geometric shapes, resembling stylized triangles or chevrons, positioned in the top left corner of the white content area.

CRA

What to do now?

Cost of compliance vs cost of non-compliance

COST OF COMPLIANCE

Investable, predictable

- ▮ **Advisory** and programme management
- ▮ **Internal** FTE over 18 to 24 months
- ▮ Testing and certification **fees**
- ▮ Tooling: **SBOM**, CVD, reporting platform
- ▮ Ongoing **post-market** retainer

COST OF NON-COMPLIANCE

Existential, unpredictable

- ▮ Fines up to 15M EUR or 2.5% of global **turnover** (whichever is higher)
- ▮ Product **withdrawal** from the EU market
- ▮ Delayed or blocked new product **launches**
- ▮ Lost **tenders** where CRA compliance is required
- ▮ **Reputation** damage after a public incident

Finance teams respond to the right-hand column. Technical teams respond to the left. Both are true.

Our recommendation

-  Review and update your business processes and activities.
-  Analyse the general risks associated with your products (e.g. STRIDE).
-  Inventory your software and hardware components.
-  Check whether your suppliers provide all the necessary information.
-  If a vertical standard for your product is not (yet) available: Assess basic conformity against the existing standards like EN 18031-x or, alternatively, IEC TS 62443-6-2.



Kostenloses Webinar

**Cyber Resilience Act
in der Praxis -
Umsetzungsschritte für Hersteller**

13. Oktober 2026 | 09:00 Uhr - 12:30 Uhr



Personal contact

NMi TESTLAB GmbH

Königswinkel 10
32825 Blomberg, Germany

Phone: +49-5235-9500-0
info@nmi-testlab.de
<http://www.nmi-testlab.de/>

Michael LANG

Business Development Specialist

✉ Michael.lang@nmi-testlab.de

[in](#) [Contact me on LinkedIn](#)

[Contact me on Teams](#)

[Book a meeting with me](#)

☎ Phone: +49-5235-9500-217

📱 Mobile: +49-151-54796845





Security Decisions First, Not Checklists

WÜRTH ELEKTRONIK MORE THAN YOU EXPECT

YOUR SPEAKER TODAY

Adithya Madanahalli

IoT Engineer

Adithya.Madanahalli@we-online.com

 [Connect with me on LinkedIn](#)



SMART TEMPERATURE/HUMIDITY SENSOR

Let's dive in!

- **Product type:** Indoor WiFi temperature / humidity sensor with LCD display
- **Interfaces:** USB-C (charging only) · WiFi 2.4 GHz (station mode)
- **Cloud dependency:** Yes — telemetry + remote monitoring via manufacturer cloud (remote data processing solution)
- **Configuration:** Authenticated changes: WiFi credentials, thresholds, reporting interval, account binding
- **Update mechanism:** Over-the-air (OTA) firmware updates via WiFi / cloud
- **Support period:** 10 years (declared)



“APPROPRIATE” IS THE WHOLE ASSIGNMENT

The intent of CRA one sentence

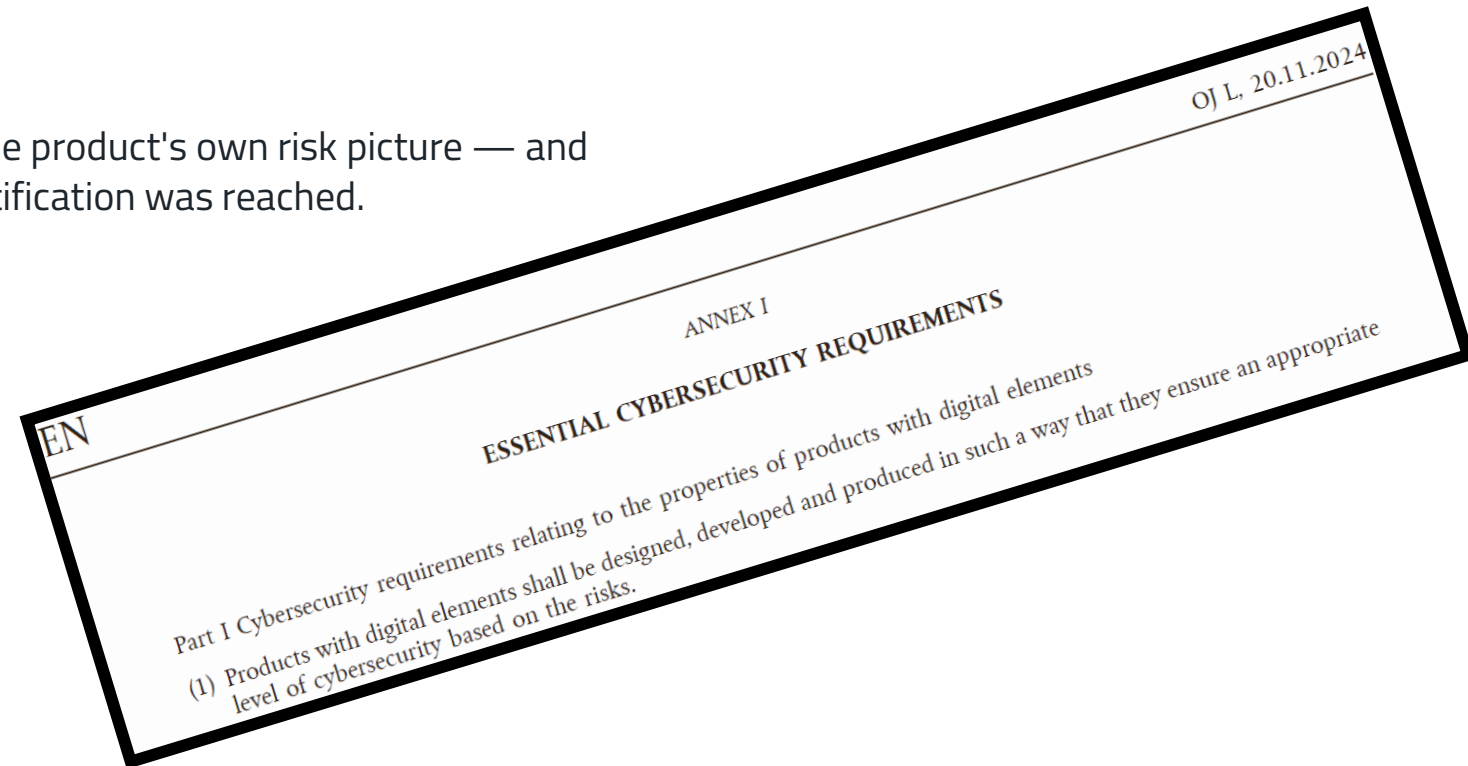
*Products with digital elements shall ensure an **appropriate** level of cybersecurity **based on the risks**.*

Myth: CRA means maximum security everywhere.

Reality: CRA requires a level of security justified by the product's own risk picture — and the manufacturer must be able to show how that justification was reached.

What “appropriate” depends on:

- Intended purpose
- **Foreseeable use and misuse**
- Exposure and interfaces
- Assets and impact
- Lifetime and support commitment



WHY THIS IS THE MANUFACTURER'S JOB

Three myths that don't survive contact with the regulation

- **Myth**

The CRA standards will give us clear requirements.

- **Reality**

The organisation must learn how to apply a security development lifecycle.

- **Myth**

Someone will tell you what to do.

- **Reality**

The CRA places substantial responsibility on the manufacturer, who must also manage regulatory uncertainty.

- **Myth**

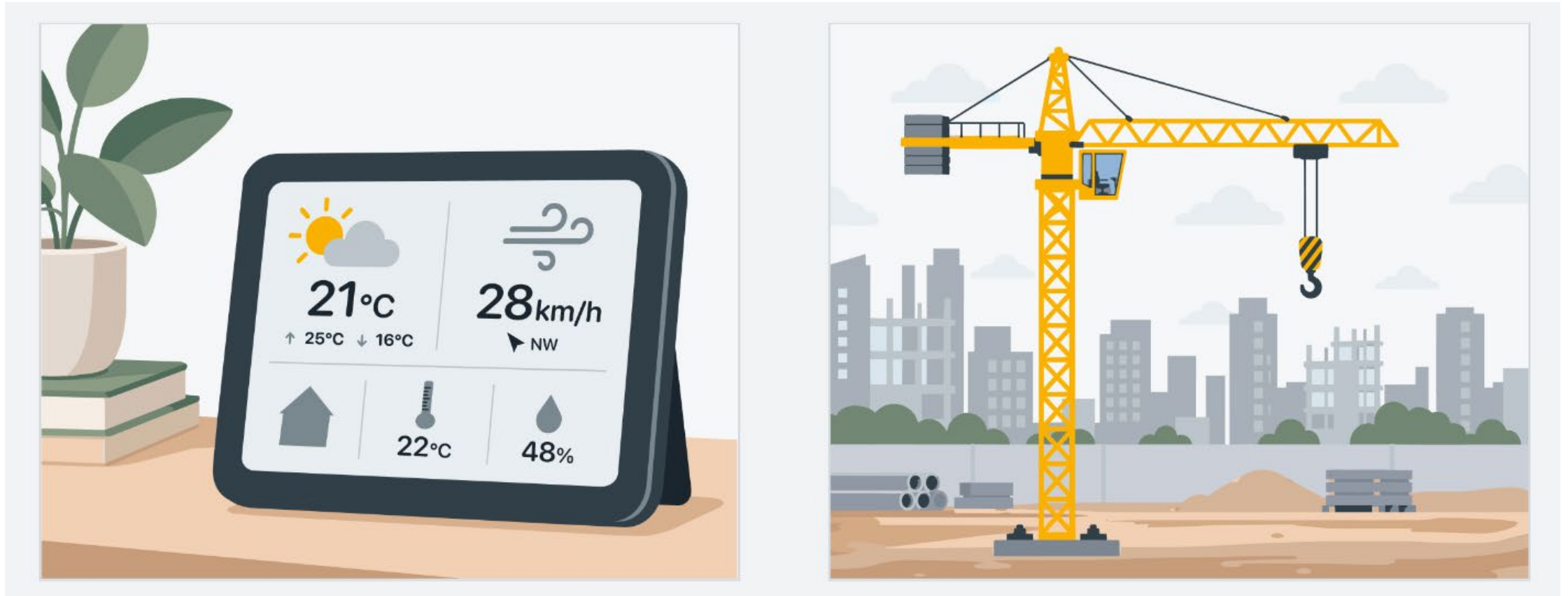
Our suppliers/customers are responsible for that.

- **Reality**

Manufacturers remain responsible for their entire product.

SAME COMPONENT: DIFFERENT RISK PROFILE

Wireless link: Indoor monitor vs Crane control



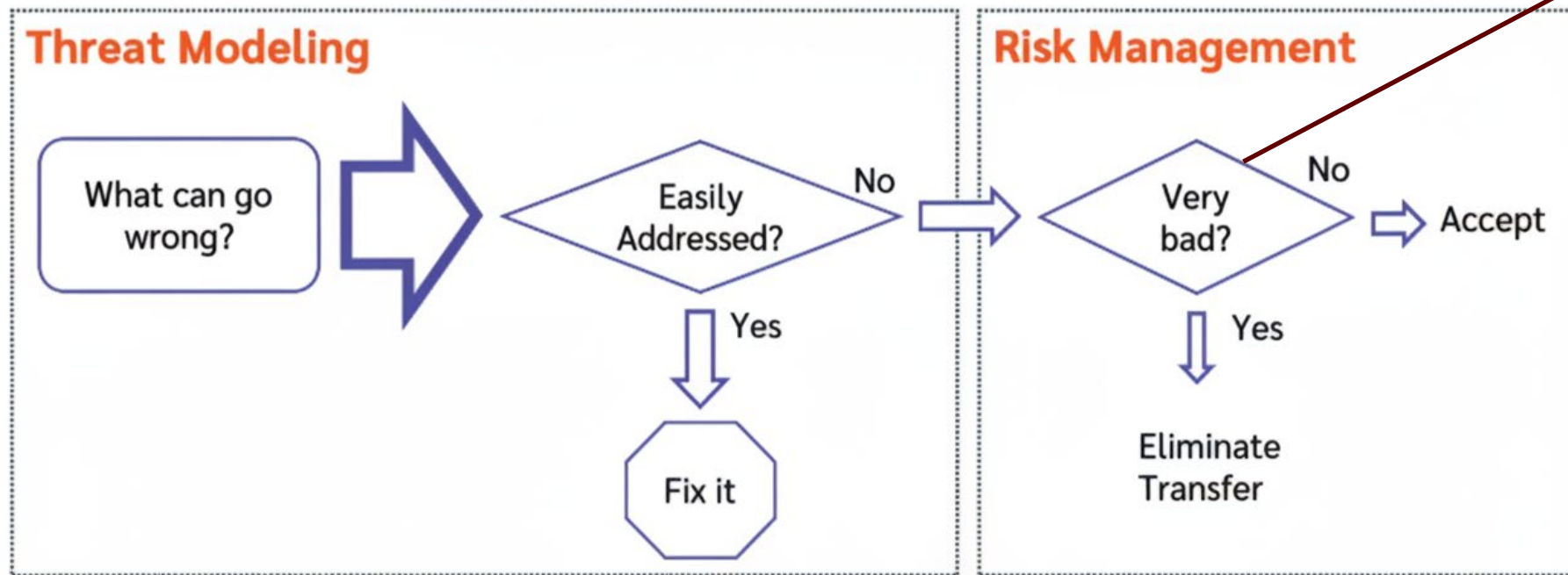
AI

What is „appropriate“ depends on the risk profile of your application.

A PRACTICAL APPROACH TO RISK ASSESSMENT

What can go wrong → fix it or decide

Risk = Likelihood X Impact



<https://shostack.org/blog/risk-management-and-threat-modeling/>

RISK ASSESSMENT WORKFLOW

A simple 4-step process

01



ASSETS

What needs
protection

Wireless module firmware, keys,
OTA channel

02



THREATS

What can go wrong

Remote code execution, tampering,
spoofed updates

03



RISK SCORE

How serious it is

Likelihood x impact

04



TREATMENT

What we do about it

Secure boot, signed OTA, key
rotation

STEP 1 - ASSET IDENTIFICATION

What do we need to protect? Structured inventory of hardware, firmware, cryptographic, interface and functional assets

Hardware

- WiFi radio / antenna
- USB-C port & power circuit
- Sensing element & LCD display
- SoC (incl. JTAG/SWD), battery

Cryptographic

- Firmware signing key
- Device identity key / certificate
- WiFi credentials on device
- Cloud session tokens, pairing secret

Firmware

- Bootloader / secure boot chain
- Application firmware (sensor, display, WiFi stack)
- OTA update client / agent

Interface & Functional

- WiFi station link · Cloud API / TLS channel
- Mobile app config interface · Local display
- Sensor telemetry · Config state · User account data

STEP 2 - THREAT IDENTIFICATION (STRIDE)

What are we protecting against? STRIDE applied per asset group

S	Spoofing	Insecure WiFi provisioning lets an attacker capture credentials or clone device identity	Wi-Fi credentials, device identity
T	Tampering	Unsigned/malicious firmware installed via compromised OTA or MITM injection	Bootloader, application firmware
R	Repudiation	No audit trail of configuration changes or firmware version at time of incident	Configuration state, update logs
I	Information Disclosure	Cloud token theft or multi-tenant misconfiguration exposes account/device data	Cloud tokens, telemetry, user data
D	Denial of Service	WiFi jamming/death flood or brute-forced pairing PIN disrupts reporting	WiFi link, local pairing interface
E	Elevation of Privilege	Firmware parsing vulnerability allows code execution beyond intended scope	Application firmware

STEP 3 - RISK SCORING

Qualitative 5x5 matrix: Risk Score = Likelihood x Impact

Impact (I)		1	2	3	4	5
5	5	10	15	20	25	
4	4	8	12	16	20	
3	3	6	9	12	15	
2	2	4	6	8	10	
1	1	2	3	4	5	
		1	2	3	4	5
		Likelihood (L) →				

Worked examples

Unsigned firmware install

$$L3 \times I5 = 15$$

Enclosure opened → debug access

$$L3 \times I4 = 12$$

OTA update interrupted → bricking

$$L3 \times I3 = 9$$

Battery circuit manipulation

$$L1 \times I5 = 5$$

STEP 4 - RISK TREATMENT

Mitigate / Transfer / Accept decision for each threat, with a named action owner

Threat	Decision	What we build	What it costs us
Malicious firmware	Mitigate	Signed images, secure boot	<i>Boot time, and a signing key you now have to protect for 10 years</i>
Stolen identity	Mitigate	Encrypted onboarding, no open provisioning mode	<i>Key injection in production. Your factory process changes</i>
Vulnerable component	Mitigate	SBOM, monitoring, A/B update with fallback	<i>Somebody owns this after launch. Forever</i>
Debug access	Mitigate	Lock JTAG, disable data lines	<i>Field returns get harder to diagnose</i>
Battery circuit tampering	Accept	Protection IC already in place	<i>Nothing. Documented and moved on</i>

Full register: 10 High, 14 Medium, 1 Low across 25 scored threats — documented in technical documentation per Art. 13(3)-(4)

BEYOND RELEASE

The lifecycle never fully stops.

SBOM visibility

Keeps the picture of what's inside the product current.

Vulnerability monitoring

Turns a disclosure into the same asset → threat → risk scoring → risk treatment exercise with a potential security patch.

End of support

Is a security decision, not just a commercial one.

NONE OF THIS IS NEW ENGINEERING

All of it is new ownership

BEFORE	NOW	WHAT THAT CHANGES COMMERCIALY
Security was the user's problem	The manufacturer is responsible	<i>You cannot point at the integrator. Expect it in the RFQ.</i>
Security ended at release	Security runs the whole lifecycle	<i>A support period is a commitment, not a marketing number.</i>
Dependencies were somebody else's job	You own your supply chain	<i>Customers will ask for an SBOM. Have an answer ready.</i>
Compliance was a point in time	Compliance is continuous	<i>The technical file is living. It is also a sales asset.</i>

THREE QUESTIONS YOUR CUSTOMERS WILL ASK YOU

Not from an auditor. From procurement, during evaluation

- 1** How long is the support period, and what happens the day after it ends?
- 2** Can you send me the SBOM for this firmware version?
- 3** Who do I call when a vulnerability is found, and how fast do you ship a fix?

If you can answer all three today, the CRA is a formality. If you cannot, it is a project.

KEY TAKEAWAYS

- 1** Decide first, document second. Paperwork is the output, not the work.
- 2** Every control has a bill. Know who pays it before you commit.
- 3** Appropriate is your call. Nobody is coming to make it for you.

THANK YOU



Short Survey German



Short Survey English

Start with the CRA Scorecard - free, 15 questions, 5 minutes

What you get

- Red / Amber / Green readiness score
- Four domains:
 - Digital Exposure,
 - Risk Category,
 - Security Readiness,
 - Organisation
- Indicative product classification
- Recommended next steps mapped to NMI services
- Downloadable report

CRA SCORECARD

Free online assessment

- 15 questions
- 5 minutes
- instant result



training.nmi-testlab.de/cra-scorecard

Time for your questions!

With Support from our specialist

Tobias Vogler

Section Manager Cybersecurity

NMi TESTLAB GmbH
Königswinkel 10
32825 Blomberg, DE

tobias.vogler@nmi-testlab.de
www.nmi-testlab.de





Kostenloses Webinar

**Cyber Resilience Act
in der Praxis -
Umsetzungsschritte für Hersteller**

13. Oktober 2026 | 09:00 Uhr - 12:30 Uhr



Thank you

