



RED | CRA | NIS2

Cybersecurity regulation towards secure development and use of connected products in Europe

As of June 2024
Steffen Zimmermann
VDMA e. V.

Upcoming European Cybersecurity Regulations



Delegated Regulation Radio Equipment Directive (EU) 2022/30 including 2023 amendment

COMMISSION DELEGATED REGULATION (EU) 2022/30

of 29 October 2021

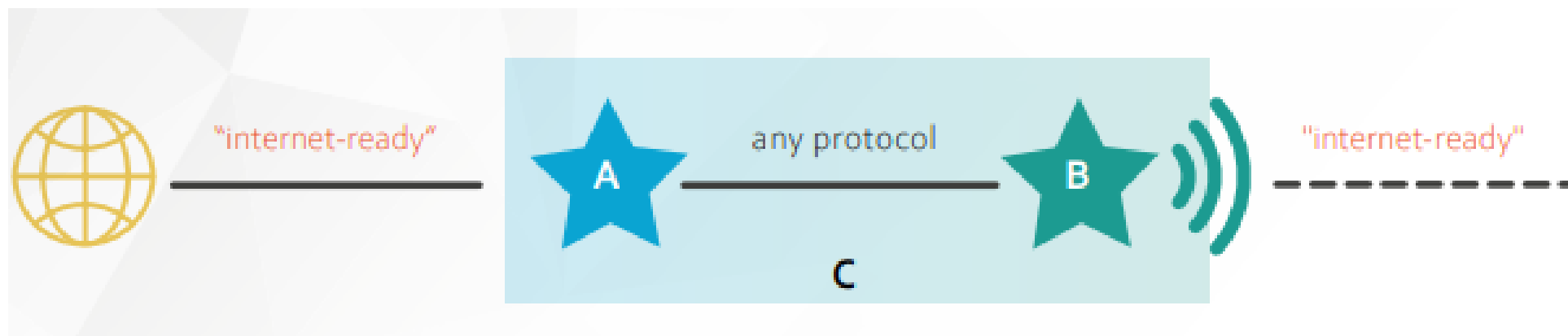
supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive

(RED DA)

RED Delegated Act in a nutshell



- Delegated Act (EU) 2022/30 with additional provisions on cybersecurity
- The regulation "activates" the essential requirements 3(3) d,e,f of the RED ([see SReq](#))
- Original scope of the Radio Equipment Directive 2014/53/EU will not be extended
- Scope: internet-enabled RED products (internet-connected radio equipment) and e.g. toys
- Also applies to "combined equipment" and devices indirectly connected to the Internet
- Implementation period until July 31, 2025 - application mandatory from August 1, 2025
- Manufacturer's declaration only through application of harmonized standards (hEN)
- prEN 18031-1/2/3 under development at CEN/CLC - ENQ was rejected
- Completion of the harmonized standards expected in June 2024 by 30 August 2024
- [Position paper on 9 scenarios from Orgalim - incl. "combined equipment"](#)



Upcoming European Cybersecurity Regulations



Cyber Resilience Act (CRA) Text Adopted (2024)0130

European Parliament

BG ES CS DA DE ET EL EN FR GA HR **IT** LV LT HU MT NL PL PT RO SK SL FI SV

Index < Previous Next > Full text

Procedure : **2022/0272(COD)** Document stages in plenary

Document selected : A9-0253/2023

Texts tabled : A9-0253/2023	Debates :	Votes : PV 12/03/2024 - 8.11 CRE 12/03/2024 - 8.11 Explanations of votes	Texts adopted : P9_TA(2024)0130
---------------------------------------	-----------	---	---

Texts adopted 637k 201k

Tuesday, 12 March 2024 - Strasbourg

Cyber Resilience Act P9_TA(2024)0130 A9-0253/2023

- Resolution
- Consolidated text

CRA in a nutshell – Cyber Resilience Act

- **Cyber Resilience Act (law) applies directly, no national implementation necessary**
- **Product-related regulation on the basis of NLF (CE)**
- **For all "products with digital elements" that are made available on the market**
- **"intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network"**
- **Basic requirements for design, development and production**
- **Requirements for vulnerability management in the product life cycle**
- **3 classes with higher requirements: Important Class I, II, and Critical**
- **Conformity assessment procedure according to NLF**
- **Entry into force expected for October 2024**
- **36 months implementation period (October 2027)**
- **21 months implementation period for reporting incidents, vulnerabilities (July 2026)**



Upcoming European Cybersecurity Regulations



Network and Information Systems Security Directive (EU) 2022/2555

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

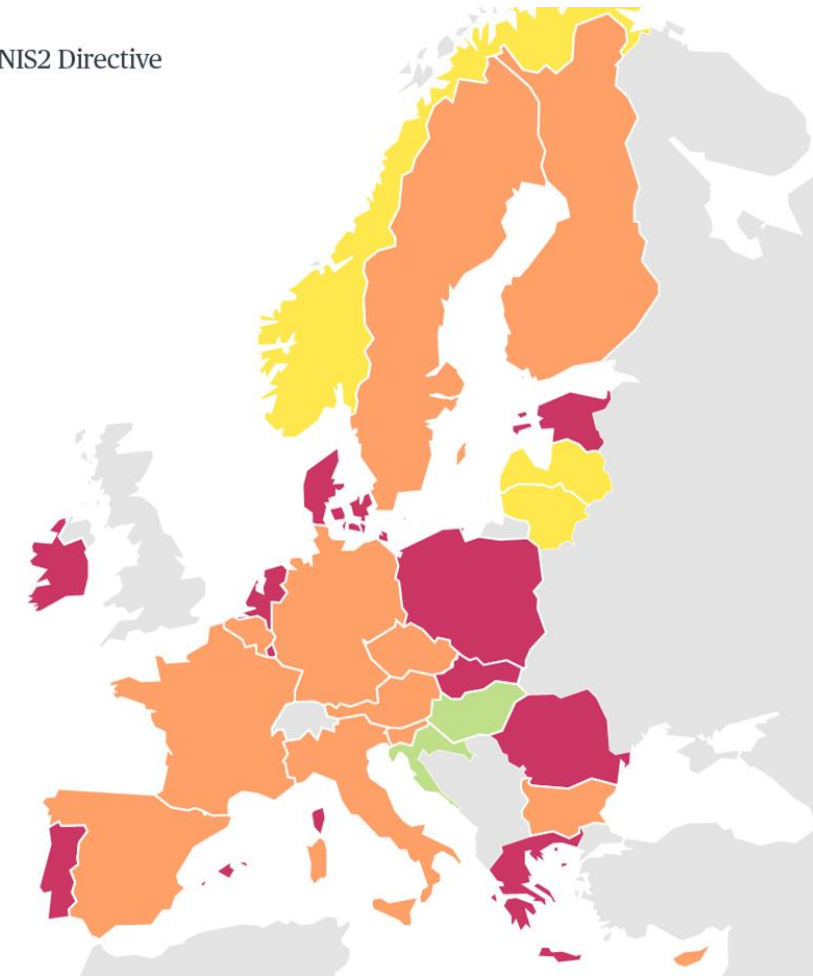
(NIS2 Directive)

NIS 2 in a nutshell





- **Directive = must be transposed into national law**
- **In force since January 16, 2023, implementation by October 17, 2024**
- **Goal: Increasing operational cyber resilience in the EU**
- **Wide scope: industry sectors like machinery, electrical engineering, vehicle construction, managed service providers**
- **Generally from 50 employees, 10 million turnover and balance sheet total**
- **Compliance with "state of the art"**
- **24h/72h reporting obligation for significant incidents**
- **Obligation to register entities to national authorities**

NIS2 Directive



NIS2-Tracker by Bird&Bird:
<https://www.twobirds.com/en/trending-topics/cybersecurity/nisd-tracker>

RED-CRA-NIS2: which areas are involved?

	NIS 2 Directive (NIS2UmsuCG)		Cyber Resilience Act RED Delegated Act
			
Range	IT	OT	Product
Area of application	Own IT infrastructure	Production / Shopfloor	Products for sale
Responsibility	IT department	Management	Product development
Systems	Laptop, e-mail, website, IaaS	MES, PLC, Remote maintenance	"Connected product", IoT services, machine cloud
Operating processes	Own processes		Customer processes
Regulatory role	Users, users, service providers		Manufacturer

RED - CRA - NIS2 cybersecurity requirements*

Secure Development	Secure Manufacturing	Secure Integration	Secure Operation	Secure Maintenance
No known exploitable vulnerabilities	OT risk assessment	Secure by default configuration	Vulnerability management	Secure remote service
Appropriate risk assessment	Awareness training	Hardening guidelines	Patch management	Substantial modification
Patchability, support period definition	Asset management	User manual	Information sharing, CERT	Update availability +10 years
Authentication, IAM, Sign & Encrypt	Business continuity management		Incident, vulnerability reporting	Legacy systems monitoring
SBOM, tests and reviews	Supply chain security		SPOC, PSIRT	

CRA

RED DA

NIS2

CRA

RED DA

NIS2

CRA

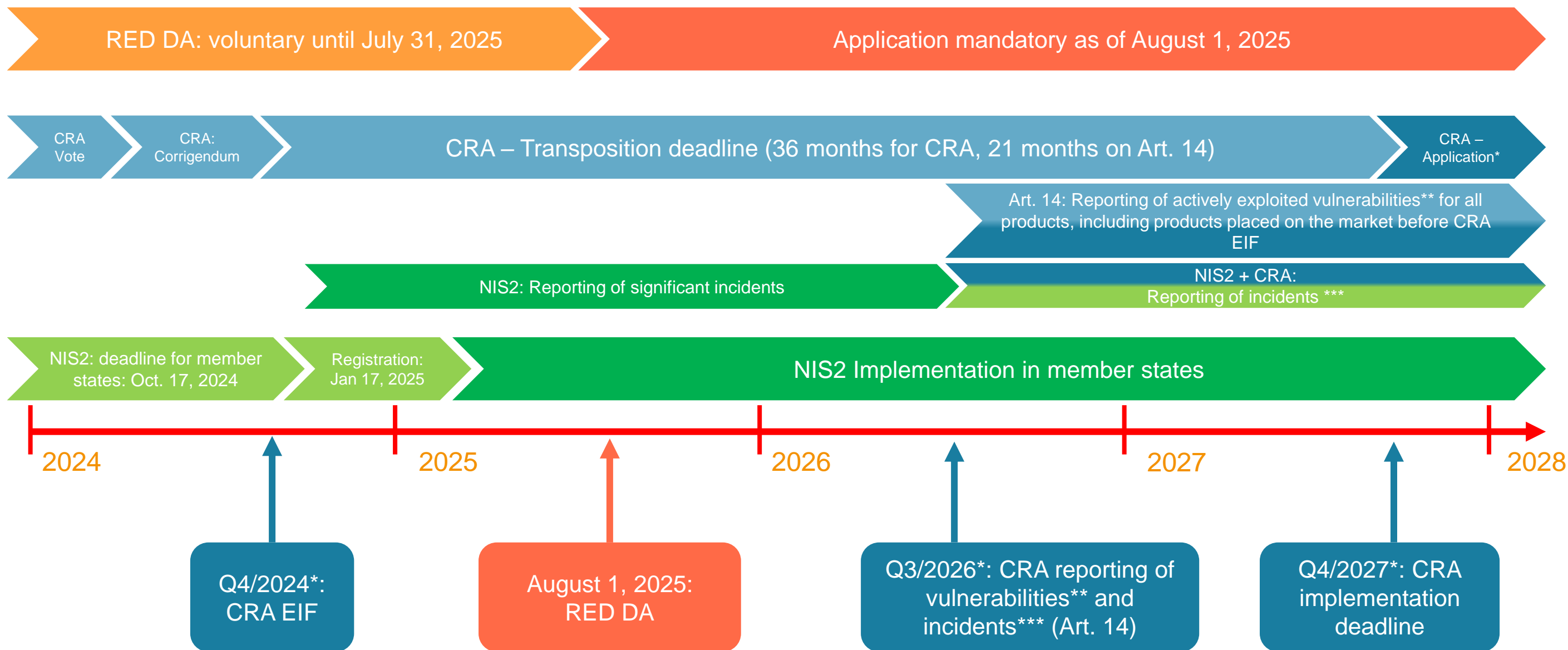
NIS2

CRA

NIS2

*Note: this list does not include all (essential) requirements from RED DA, CRA and NIS2

Timeline NIS2-Transposition*, RED DA, CRA*



CRA: [Cyber Resilience Act: Text Adopted \(2024\)0130](#)
 RED DA: [Delegated Regulation 2022/30 Radio Equipment Directive, including 2023 amendment](#)
 NIS2: [Network and Information Systems Security Directive 2022/2555](#)

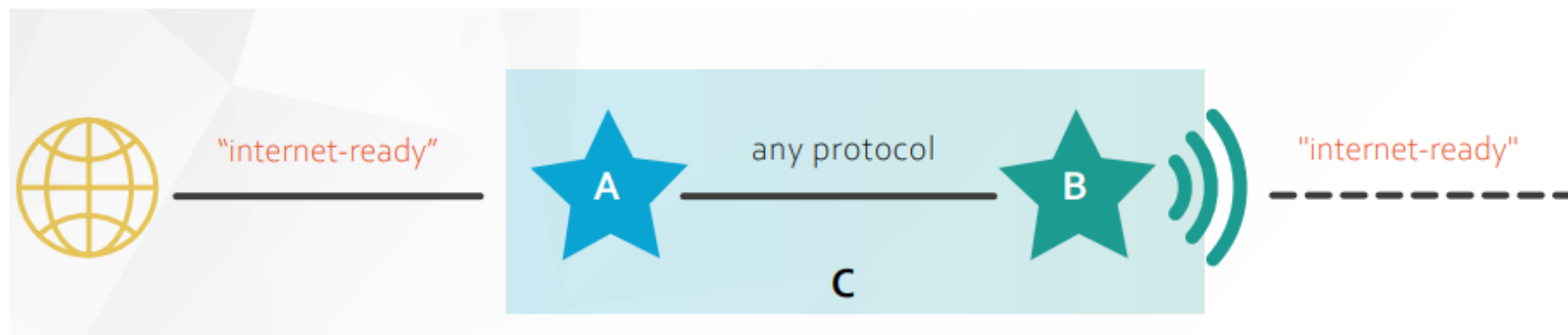
* Not yet final, tentative
 ** actively exploited vulnerabilities
 *** NIS2: significant incidents / CRA: severe incidents with impact on Product Security



Radio Equipment Directive DA

D(EU) 2022/30

RED – Scenario Combined Equipment



PRODUCT C	
Radio equipment according to 2014/53/EU?	<p>YES</p> <p>The product has a radio interface and is radio equipment according to the definition in 2014/53/EU.</p>
"Internet-connected radio equipment"?	<p>YES</p> <p>Regardless, of whether Product A is within the scope of the delegated regulation, the combined equipment itself is capable of communicating over the internet via its radio interface ("wireless") and via its "wired" interface.</p>
Product examples	<p>Combustion engine with a telematic device incorporated remote controllable machinery.</p>

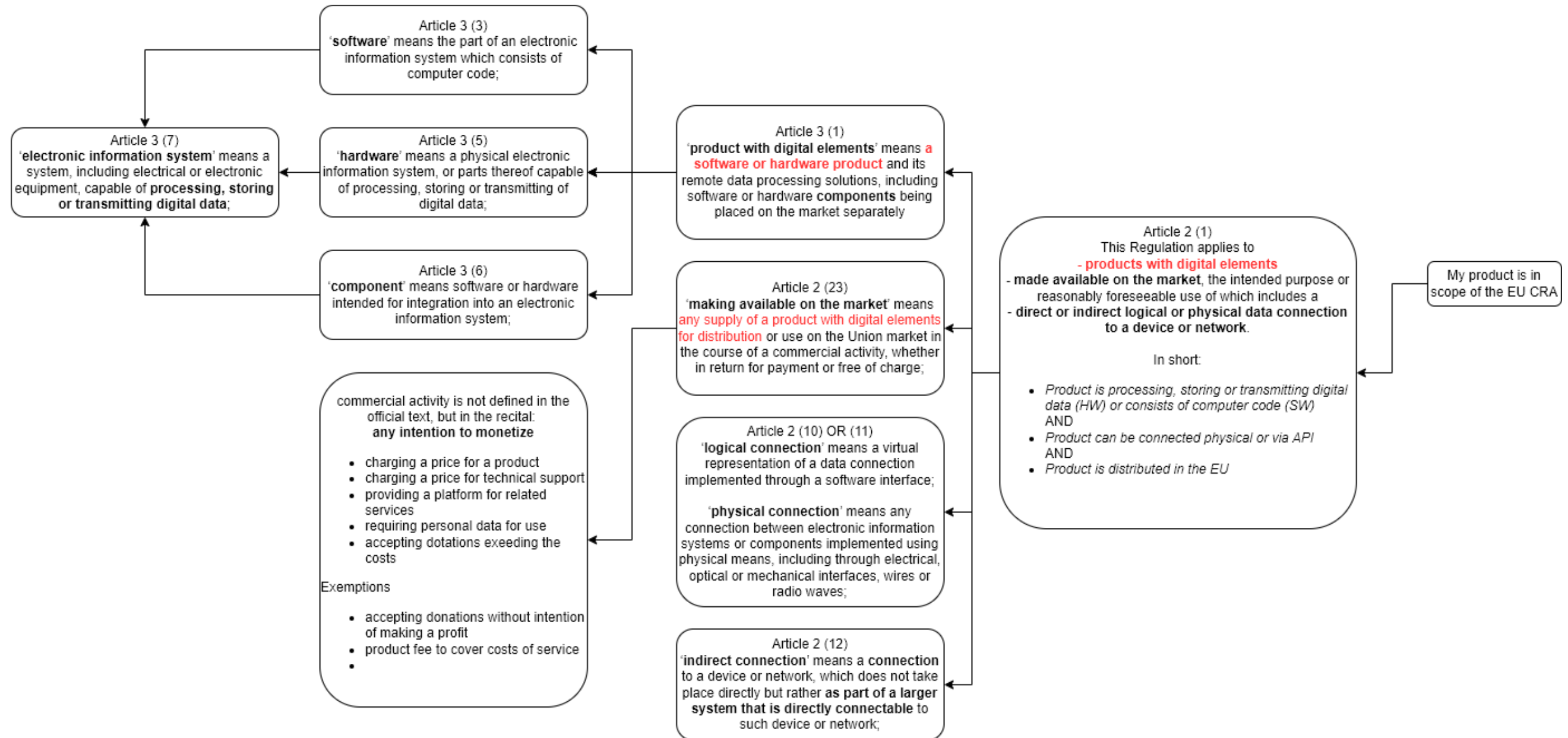
RED Delegated Act - Important Notes

- A manufacturer's self declaration is only possible when using the harmonized standards cited in the Official Journal of the EU
- A citation of EN 18031-1/2/3 for full compliance with the requirements currently seems unlikely
- EN IEC 62443-4-2 covers essential parts of the legal act; for a conformity assessment against the legal act based on EN IEC 62443-4-2, the mandatory involvement of a Notified Body is necessary
- Voluntary compliance with the Cyber Resilience Act (CRA) after its entry into force will not exempt from the RED conformity assessment
- The Commission has not found any scenario in which the essential requirements of the RED DA are not covered by the CRA
- The Commission has held out the prospect of withdrawing the delegated act, but there is no timetable yet

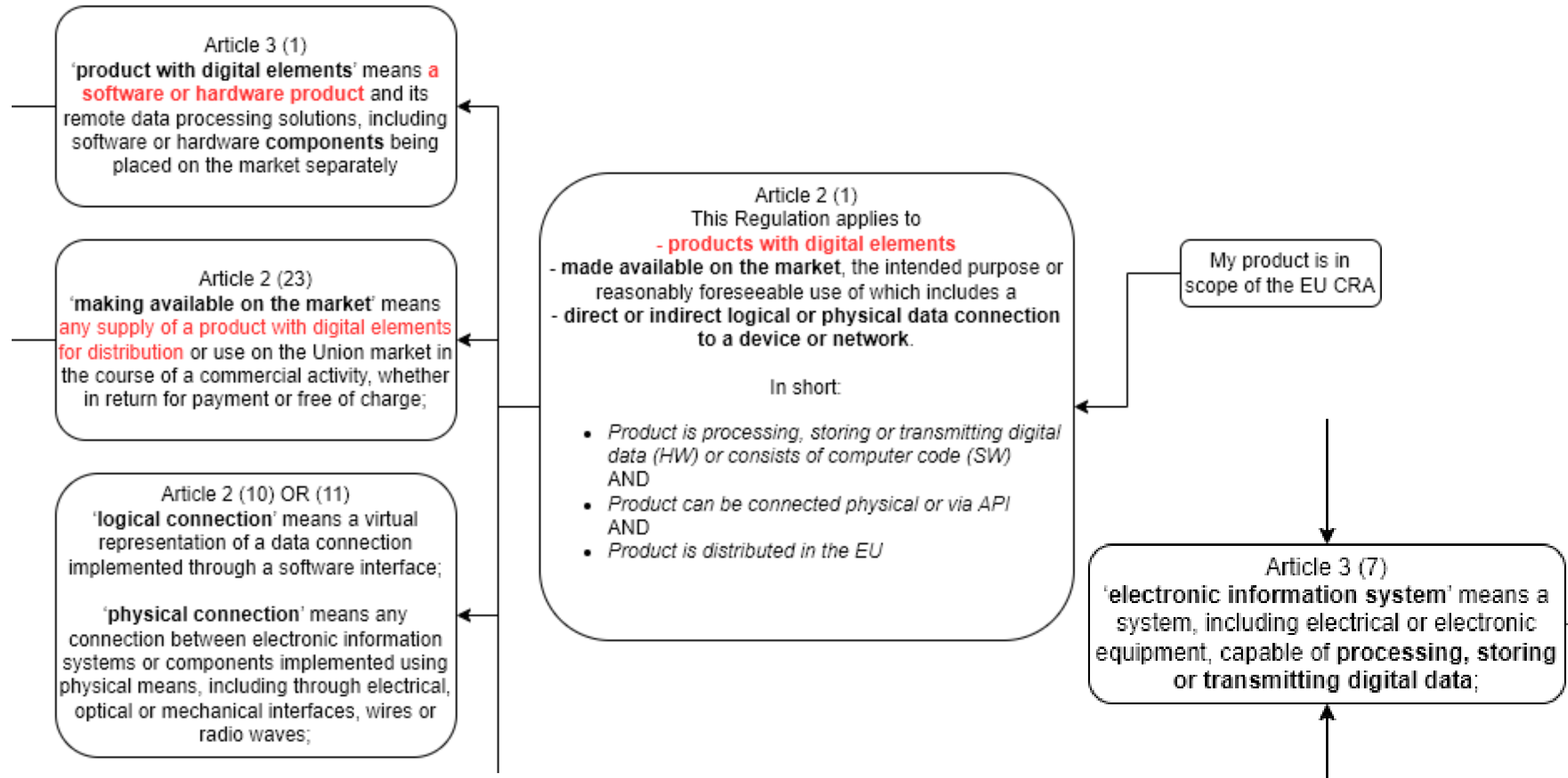
Cyber Resilience Act



CRA – Product with digital elements



CRA – Product with digital elements



CRA Annex III



List of products with increased conformity assessment requirements

Important:

- Same essential requirements
- Machinery is not on the list

Annex III / IIIa - Important and Critical Products and their conformity assessment procedures	
Important annotation to the list of important/critical products: The Annex III list is focusing on the "core functionality" of the product.	
<p style="text-align: center;">Important Products - Class II (Third-party conformity assessment)</p> <p>Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments</p> <p>Firewalls, intrusion detection and/or prevention systems</p> <p>Tamper-resistant microprocessors</p> <p>Tamper-resistant microcontrollers</p>	<p style="text-align: center;">Important Products Class I (Self-declaration with hEN fully applied)</p> <p>Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers</p> <p>Standalone and embedded browsers</p> <p>Password managers</p> <p>Software that searches for, removes, or quarantines malicious software</p> <p>Products with digital elements with the function of virtual private network (VPN)</p> <p>Network management systems</p> <p>Security information and event management (SIEM) systems</p> <p>Boot managers</p> <p>Public key infrastructure and digital certificate issuance software</p> <p>Physical and virtual network interfaces</p> <p>Operating systems</p> <p>Routers, modems intended for the connection to the internet, and switches</p> <p>Microprocessors with security-related functionalities</p> <p>Microcontrollers with security-related functionalities</p> <p>Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities</p> <p>Smart home general purpose virtual assistants</p> <p>Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems</p> <p>Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features</p> <p>Personal wearables products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/746 or Regulation (EU) 2017/746 do not apply or personal wearable products that are intended for the use by and for children</p>
<p style="text-align: center;">Critical Products (EU certification scheme)</p> <p>Hardware Devices with Security Boxes</p> <p>Smart meter gateways within smart metering systems as defined in Article 2 (23) of Directive (EU) 2019/944 and other devices for advanced security purposes, including for secure cryptoprocessing</p> <p>Smartcards or similar devices, including secure elements</p>	
<p style="text-align: center;">"Core Functionality"</p> <p>The categories of important and critical products with digital elements referred to in Annex III of the CRA should be understood as the products which have the core functionality of the type that is listed in Annex III. For example, Annex III lists products which are defined by their core functionality as firewalls, intrusion detection or prevention systems as important products in class II. As a result, firewalls, intrusion detection or prevention systems are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate firewalls, intrusion detection or prevention systems. The Commission should adopt an implementing act to specify the definitions of the product categories covered under class I and class II as set out in Annex III.</p> <p style="text-align: center;"><i>Source: Recital 27, EU Cyber Resilience Act</i></p>	
<p style="text-align: center;">"No Inheritance"</p> <p>Products with digital elements which have the core functionality of a category that is listed in Annex III to this Regulation shall be [...] subject to the conformity assessment procedures referred to in Article 24 (2) and (3). The integration of a product with digital elements which has the core functionality listed in Annex III does not in itself render the product in which is integrated subject to the conformity assessment procedures referred to in Article 24 (2) and (3).</p> <p style="text-align: center;"><i>Source: Article 6, EU Cyber Resilience Act</i></p>	

CRA Annex III – Core Functionality

List of products with increased conformity assessment requirements

Important:

- Core functionality of the product
- No inheritance of criticality in combined products

"Core Functionality"

The categories of important and critical products with digital elements referred to in Annex III of the CRA should be understood as the products which have the **core functionality** of the type that is listed in Annex III. For example, Annex III lists products which are defined by their core functionality as firewalls, intrusion detection or prevention systems as important products in class II. As a result, firewalls, intrusion detection or prevention systems are subject to mandatory third-party conformity assessment. This is not the case for other products not explicitly referred to in Annex III to this Regulation which may integrate firewalls, intrusion detection or prevention systems. The Commission should adopt an implementing act to specify the definitions of the product categories covered under class I and class II as set out in Annex III.

Source: Recital 27, EU Cyber Resilience Act

"No Inheritance"

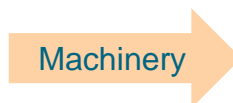
Products with digital elements which have the **core functionality** of a category that is listed in Annex III to this Regulation shall be [...] subject to the conformity assessment procedures referred to in Article 24 (2) and (3). The integration of a product with digital elements which has the core functionality listed in Annex III **does not in itself render the product in which is integrated subject to the conformity assessment procedures** referred to in Article 24 (2) and (3).

Source: Article 6, EU Cyber Resilience Act

Note: source numbering changed to Recital 45 and Art. 7 (1)

CRA Annex III

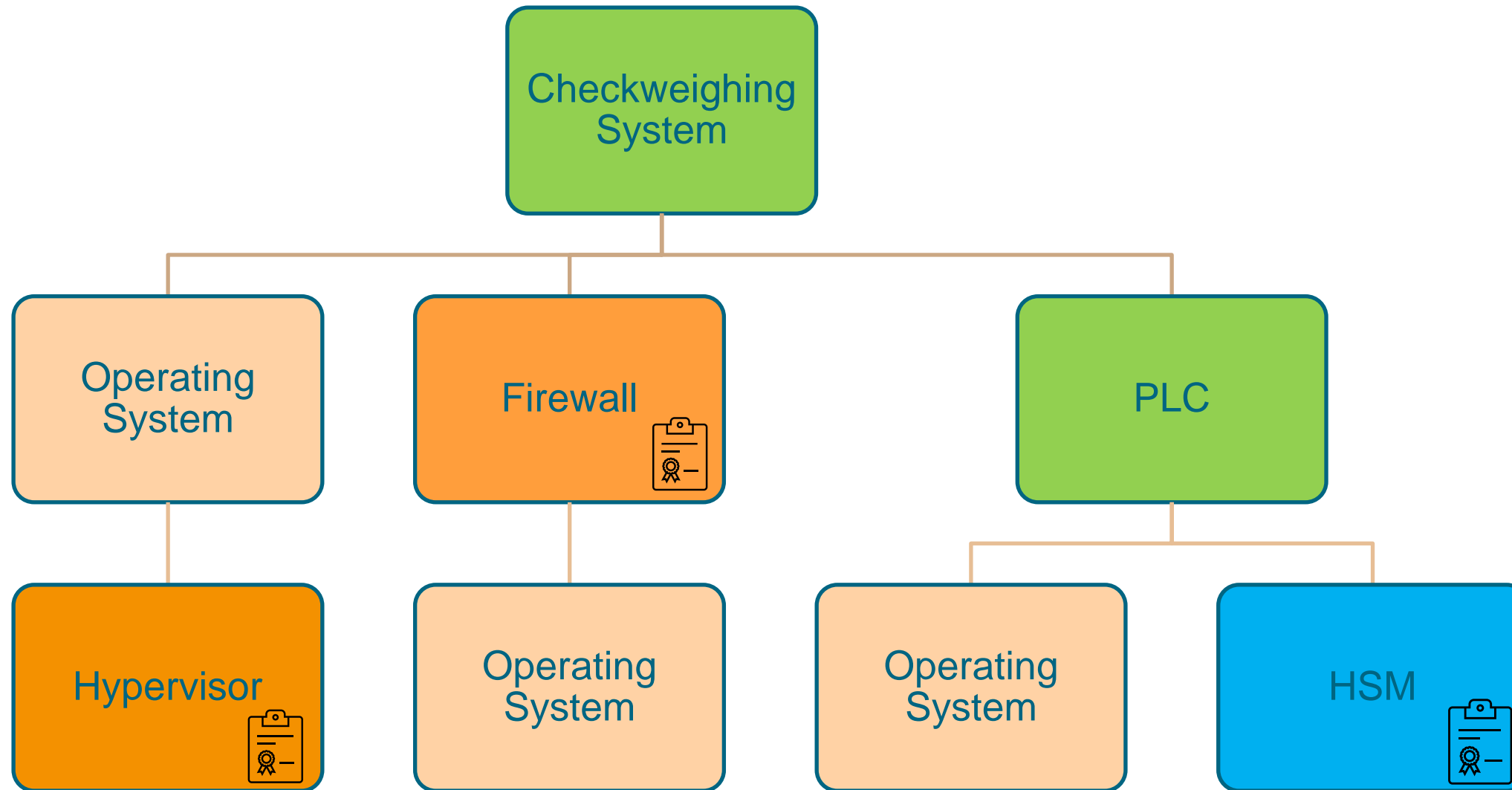
Available conformity assessment procedures depending on the product category



Conformity assessment procedure to demonstrate conformity with the essential requirements (or parts thereof) set out in Annex I				
Type	Module A (Self-Declaration) Annex VIII Part I	Module B+C (EU-based type examination) Annex VIII Part II + III	Module H (Full Qualified Assurance) Annex VIII Part IV	EU Certification Scheme "substantial" or "high" (EU) 2019/881
Product with digital elements Art 32 (1)	X	X	X	X
Important Product Class I Art. 32 (2)	if hEN is fully applied	X	X	at least "substantial"
Important Product Class II Art. 32 (3)		X	X	at least "substantial"
Critical Product Art. 32 (4), Art. 8 (1)		(X)	(X)	X
Open Source Product Class I/II Art. 32 (5), Art. 32 (1)	X*	X	X	X*

*provided that the technical documentation is made available to the public at the time of placing on the market

CRA: Combined Products / Machinery



✓ „Common“
Module A:
Self Declaration

✓ Important (I)
Module A (hEN):
Self Declaration*

✓ Important (II)
Module B+C:
Type Examination

✓ Critical
EU Cybersecurity
Certification Scheme

* when hEN is published, listed in the Official Journal of the European Union and fully applied

NIS2 Directive



NIS 2 – Scope: machinery is in, how to find out?

1. Scope: NACE-Code C26-C30
2. Size Cap Rule: Medium (50+)

Germany only: Rule of „Independent IT“

Croatia only: Notification by Authority until Feb. 15, 2025

Hungary only: Supervision Fee of 0.015% of sales (max. 25k EUR)

GERMANY (2022)	Total companies	NIS2 affected (>50 EE)	of which NIS2 50-250 EE
WZ08-20 Manufacture of chemicals and chemical products	1,717	1,097 (64%)	820 (75%)
WZ08-21 Manufacture of basic pharmaceutical products and pharmaceutical preparations	364	259 (71%)	144 (56%)
WZ08-26 Manufacture of computer, electronic and optical products	2,010	1,165 (58%)	886 (76%)
WZ08-27 Manufacture of electrical equipment	2,261	1,358 (60%)	991 (73%)
WZ08-28 Manufacturer of machinery and equipment	6,254	3,646 (58%)	2,724 (75%)



Mettler-Toledo GmbH

MAIN INDUSTRY: Electrical engineering

UPDATED 2024-05-14

Key Facts

INDUSTRIES

- > Electrical engineering (C26)
- > Repair and installation (C33)

PRODUCTS AND SERVICES

- > Handel
- > Anwendungen
- > Software

SIZE (REVENUE & EMPLOYEES)

Large company

Source: implisense.com

NIS 2 – Minimum Requirements (Art. 21)

- a. policies on risk analysis and information system security;
- b. incident handling;
- c. business continuity, such as **backup management** and disaster recovery, and crisis management;
- d. **supply chain security** including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- e. security in network and information systems **acquisition**, development and **maintenance**, including **vulnerability handling and disclosure**;
- f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- g. basic cyber hygiene practices and cybersecurity training;
- h. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- i. human resources security, access control policies and **asset management**;
- j. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate.

Cross points to Cyber Resilience Act

Conclusions



- **Machinery is undisputable in scope of all new regulations**
- **Focus on IT/OT infrastructure, digital services and products with digital elements**
- **NIS2 needs national transposition – it will be different**
- **Prepare to support your products after placing on the market**
- **Check your suppliers on their preparedness**
- **Speak with a Notified Body to prepare for RED Conformity**
- **Leverage standards ISO 27001 (NIS2) and EN IEC 62443 (CRA)**
- **No security - no business**



Competence Center Industrial Security
VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main - Germany



Steffen Zimmermann
+49 69 6603 - 1978
Steffen.Zimmermann@vdma.org



Biljana Gabric
+49 69 6603 - 1360
Biljana.Gabric@vdma.org



Maximilian Moser
+49 30 3069 - 1909
Maximilian.Moser@vdma.org

<https://vdma.org/cybersecurity>

BACKUP



6 9 3 2 0

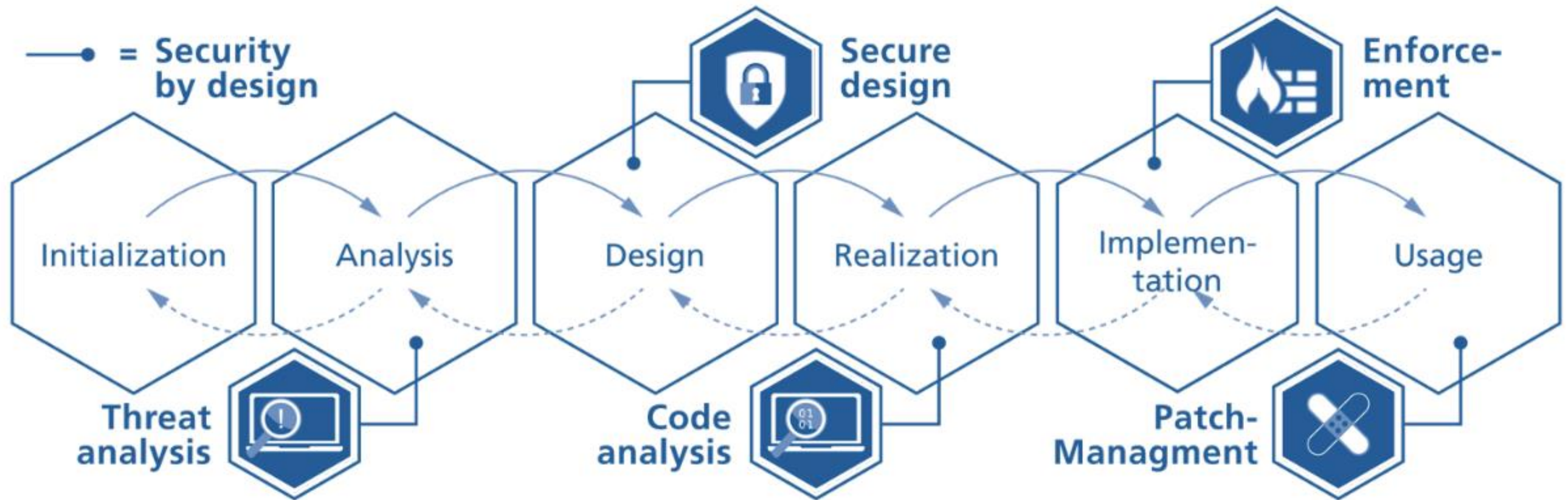


6 9 3 1 9



6 9 3 1 8

CRA – integration in product lifecycle is crucial

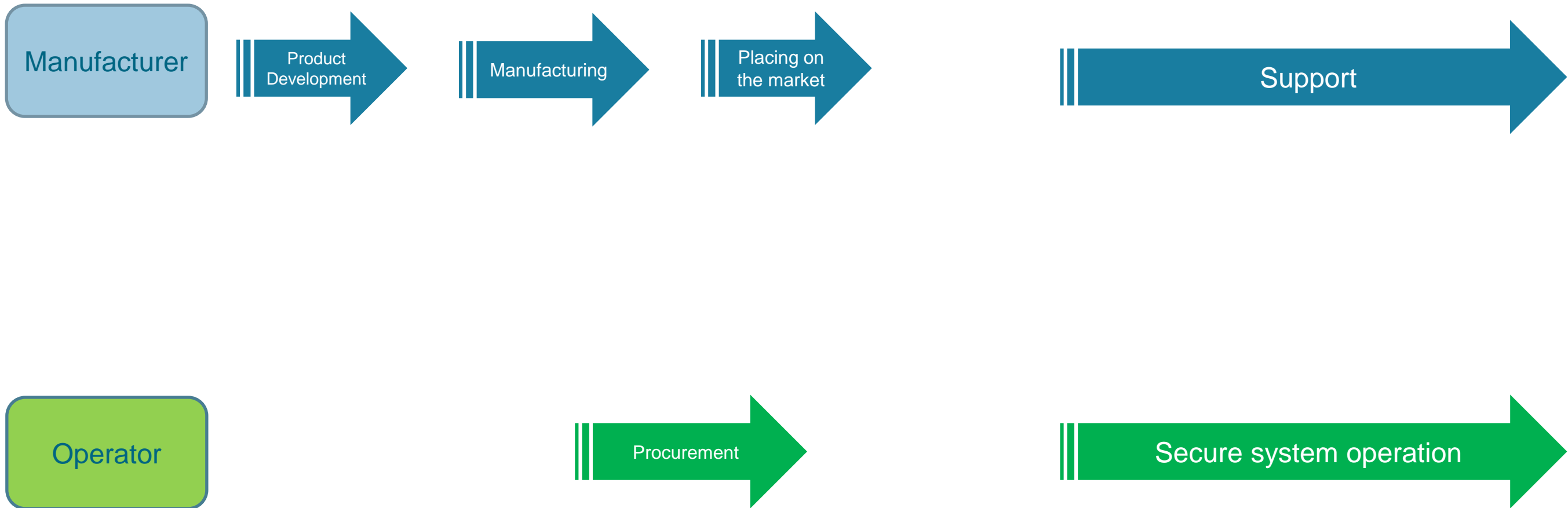


Source: Fraunhofer IEM, Dr. Focke

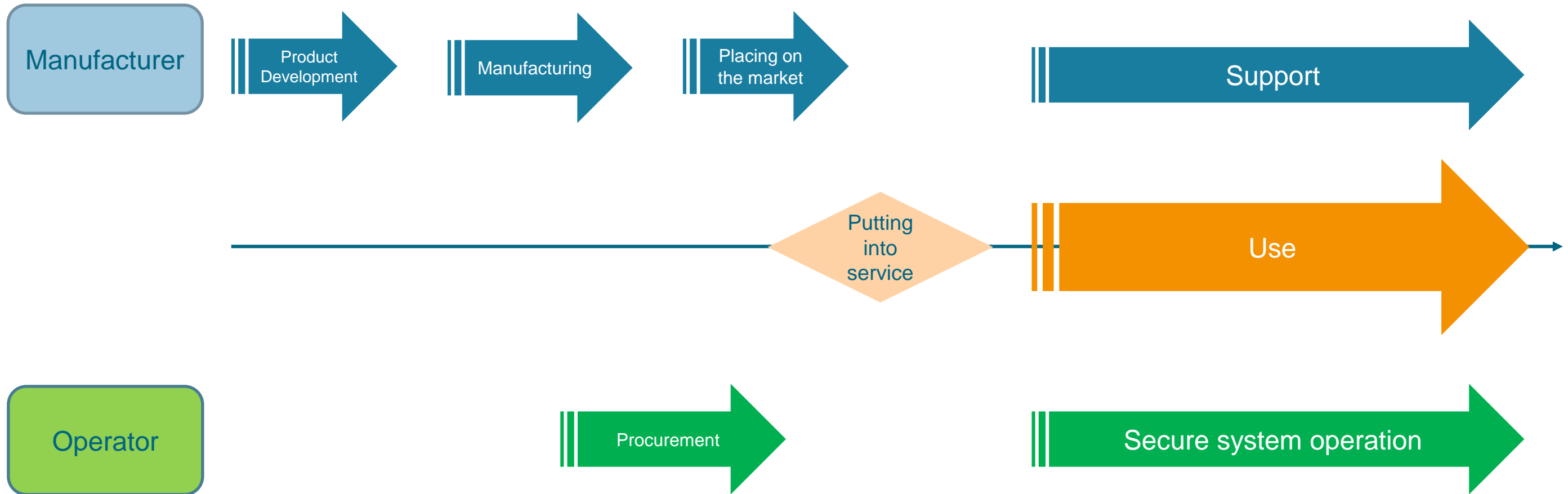
Cyber resilience in the product life cycle



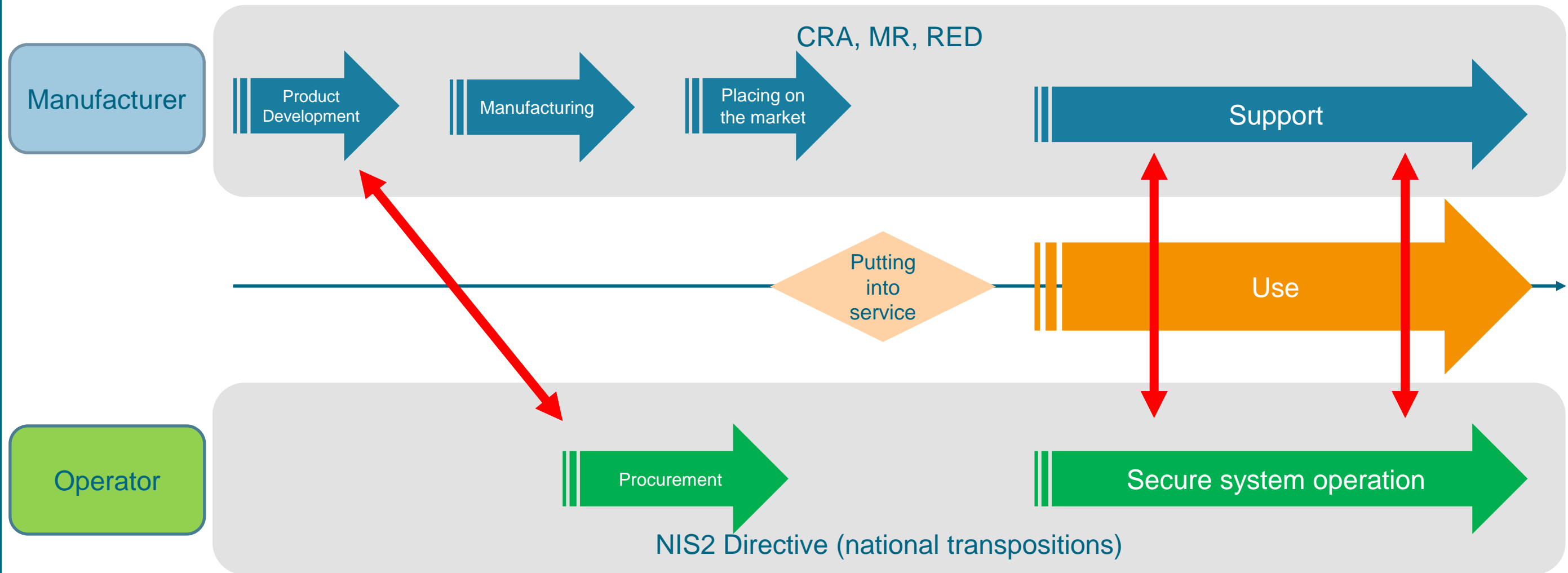
Cyber resilience in the product life cycle



Cyber resilience in the product life cycle



Cyber resilience in the product life cycle



CRA: Cyber Resilience Act
 MR: Machinery Regulation
 RED: Delegated Act Radio Equipment Directive
 NIS2: Network and Information Systems Directive 2

NIS 2 – Management Obligations

- **management bodies** of essential and important entities:
 - **approve** the **cybersecurity risk management measures** taken by those entities in order to comply with requirements on “cybersecurity risk management measures (Article 18)
 - **oversee the implementation** of “cybersecurity risk management measures”
 - **can be held liable** for the non-compliance by the entities with NIS 2 obligations → **natural person (member of the board) is personally liable**
- **members of management bodies:**
 - required to follow **specific trainings** on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the services provided by the entity
 - **encourage** essential and important entities to offer **similar training to all employees**

NIS2 – VDMA ISO 2001:2022 Mapping

NIS2Um suCG requirement (GERMANY) wichtige Einrichtungen	Keywords	ISO 27k Reference (Controls numbering based on 27001:2022)	Coverage
<p>§30 Risikomanagementmaßnahmen 1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme</p>	<p>Policies Risk management</p>	<p>Chapter 5 "Policy" Chapter 6.1 "Actions to address risks and opportunities" A.5.1 "Policies for Information Security"</p>	<p>27k covers NIS2 requirement</p>
<p>§30 Risikomanagementmaßnahmen 2. Bewältigung von Sicherheitsvorfällen</p>	<p>Incident Management</p>	<p>A.5.24 "Information security incident management planning and preparation" A.5.26 "Response to information security incident" A.5.27 "Learning from information security incidents"</p>	<p>27k covers NIS2 requirement</p>
<p>§30 Risikomanagementmaßnahmen 3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement</p>	<p>Business Continuity Management</p>	<p>5.29 Information security during disruption 5.30 ICT readiness for business continuity 8.13 Information backup 8.14 Redundancy of information processing facilities</p>	<p>27k covers NIS2 requirement except for overall "crisis management" requirement</p>
<p>§30 Risikomanagementmaßnahmen 4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern [...] (8) Bei der Erwägung geeigneter Maßnahmen nach Absatz 4 Nummer 4 berücksichtigt die Einrichtung [...] die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse.</p>	<p>Supply Chain Security</p>	<p>#Supplier_relationships_security A.5.19 Information security in supplier relationships A.5.20 Addressing information security within supplier agreements A.5.21 Managing information security in the ICT supply chain A.5.22 Monitoring, review and change management of supplier services A.5.23 Information security for use of cloud services</p>	<p>27k covers NIS 2 requirement</p>

CRA/NIS2: VDMA Supplier Self Disclosure



- » Based on EN IEC 62443, free to use, in German and English
- » Linked to CRA and MR (TISAX, NIS2 in preparation)
- » <https://www.vdma.org/viewer/-/v2article/render/82349740>

Thema & Referenz zu Mindestanforderungen	Frage	Antwort	Ergänzende Kommentare	MVO-Pflicht	CRA-Pflicht	CSRS	CSRS
1	Version: 2023, Stand 12.05.2023						
2	Governance						
3	GOV	Haben Sie in Ihrem Unternehmen Security-Richtlinie formuliert, dokumentiert und etabliert?	nein			x	x
4	GOV	- Wenn JA: Besteht eine anerkannte Security-Zertifizierung?	0%	Freitext		x	x
5	GOV	- Wenn JA: Umfasst der Scope der Security-Richtlinien die interne Office-IT? Bitte geben sie die abgedeckten Bereiche (Scope) mit an.	0%	Freitext		x	x
6	GOV	- Wenn JA: Umfasst der Scope der Security-Richtlinien die Produktion? Bitte geben sie die abgedeckten Bereiche (Scope) mit an.	0%	Freitext		x	x
7	GOV	- Wenn JA: Umfasst der Scope der Security-Richtlinien die Produktentwicklung? Bitte geben sie die abgedeckten Bereiche (Scope) mit an.	0%	Freitext		x	x
8	GOV	- Wenn JA: Umfasst der Scope der Security-Richtlinien die Service-Abteilung? Bitte geben sie die abgedeckten Bereiche (Scope) mit an.	0%	Freitext		x	x
9	GOV	- Wenn JA: Wird eine Security Leistungsbeschreibung mit Ihren Dienstleistern in Übereinstimmung mit den Security-Richtlinien vereinbart?	0%	Freitext		x	x
10	GOV						
11	Asset-Management						
12	AMS	Erstellen Sie für die zu verkaufenden Produkte einen Nachweis über die verbauten/verwendeten Komponenten und deren technischen Eigenschaften?	0%	Freitext		x	x
13	AMS	Dokumentieren Sie die implementierten Security-Fähigkeiten der Komponenten/Maschine/Anlage und zu deren Nutzung?	nein	Freitext	x	x	x
14	Risikomanagement						
15	SRM	Führen Sie eine Risikobewertung Ihrer Komponenten/Maschine/Anlage durch, die die im Betrieb zu erwartenden IT-Sicherheitsrisiken abdeckt?	0%	Freitext	x	x	x
16	SRM	- Wenn ja, gehen Sie nach einem allgemein anerkannten Verfahren vor (z.B. nach IEC 62443, VDE 2182)?	nein	Freitext		x	x
17	SRM	Werden Gefährdungen der Safety durch Cyberrisiken gem. MVO beurteilt?	nein	Freitext	x	x?	x
18	Sicherheitskonzept						
19	SIK	Wird die Risikobewertung regelmäßig oder im Rahmen von Auftragsabwicklungen aktualisiert?	ja/nein	Freitext		x	x
20	SIK	Gibt es einen Prozess der erforderliche Maßnahmen zur Härtung vor der Auslieferung einer Komponente/Maschine/Anlage fordert?	ja/nein	Freitext		x?	x
21	SIK	Gibt es einen Schwachstellenmanagement-Prozess, der sicherstellt, dass die Komponente/Maschine/Anlage ohne bekannt gemachte und aktiv ausgenutzte Schwachstellen in Betrieb genommen wird?	0%	Freitext	x (safety)	x	x
22	Lieferanten-Management / Engineering-Prozess						
23	SCS	Beachten Sie Security -Vorgaben & Hinweise der Hersteller bei der Systemintegration?	ja/nein	Freitext			x

CRA: Essential Requirements

Requirements that products to be placed on the internal market have to fulfil

Essential security requirements

- products with digital elements shall be designed, developed and produced in such a way that they ensure a risk-adequate level of cybersecurity
- products with digital elements shall be delivered without any known exploitable vulnerabilities
- concrete security requirements:
 - secure-by-default configuration;
 - protection from unauthorised access;
 - protect confidentiality & integrity of stored, transmitted or processed data (encryption), commands, programs and configuration;
 - minimisation of data processed;
 - protect availability of essential functions;
 - minimise negative impact on availability of services provided by other devices / networks;
 - designed, developed and produced to limit attack surfaces;
 - designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
 - provide security related information by recording and/or monitoring relevant internal activity;
 - ensure that vulnerabilities can be addressed through security updates.

Vulnerability handling requirements

- manufacturers shall:
 - identify and document vulnerabilities and components contained in the product (SBOM)
 - address and remediate vulnerabilities without delay
 - effective & regular tests & reviews
 - security update: disclose info about fixed vulnerabilities
 - policy on coordinated vulnerability disclosure
 - facilitate information sharing about potential vulnerabilities
 - mechanisms in place to securely distribute updates
 - dissemination without delay and free of charge of security patches or updates

NIS 2 – Annex I and II



Essential Entities

all LARGE entities operating in the following sectors:

- Energy
 - electricity (supply, DSO, TSO, producers, nominated electricity market operators, electricity market participants providing aggregation, demand, response or storage, as well as operators of recharging points)
 - district heating and cooling
 - oil
 - gas
 - hydrogen
- Transport
 - air
 - rail
 - water
 - road
- Banking
- Financial Market Infrastructures
- Health
- Drinking Water
- Waste Water
- Digital Infrastructure
- ICT-service management (B2B)
- Public Administration entities excl. judiciary, parliaments and central banks
- Space

regardless of size:

- providers of public electronic communications networks or publicly available electronic communications services;
- trust service providers;
- top-level domain name registries and DNS service providers;
- public administration entities (central government and regional level)
- other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities
- entities defined by Member States before 16 January 2023 as operators of essential services
- critical entities pursuant to Resilience of Critical Entities Directive

Important Entities

all MEDIUM entities operating in the following sectors:

- Energy
 - electricity
 - district heating and cooling
 - oil
 - gas
 - hydrogen
- Transport
 - air
 - rail
 - water
 - road
- Banking
- Financial Market Infrastructures
- Health
- Drinking Water
- Waste Water
- Digital Infrastructure
- ICT-service management (B2B)
- Public Administration entities excl. judiciary, parliaments and central banks
- Space

all medium and large entities operating in the following sectors:

- postal and courier services
- waste management
- manufacture, production and distribution of chemicals
- food production, processing and distribution
- **manufacturing of:**
 - **medical devices and in vitro diagnostic medical devices**
 - **computer, electronic and optical products**
 - **electrical equipment**
 - **machinery and equipment**
 - **motor vehicles, trailers and semi-trailers**
 - **transport equipment**
- digital providers
 - online marketplaces
 - online search engines
 - social networking services platforms
- **research**

Micro and Small Entities

in general:

- **excluded** from the scope of the Directive

exceptions:

- providers of electronic communications networks
- providers of publicly available electronic communications services
- trust service providers
- Top-level domain name (TLD) name registries
- public administration
- certain other entities

size-cap rule: all medium & large enterprises that operate within these sectors / offer these services affected