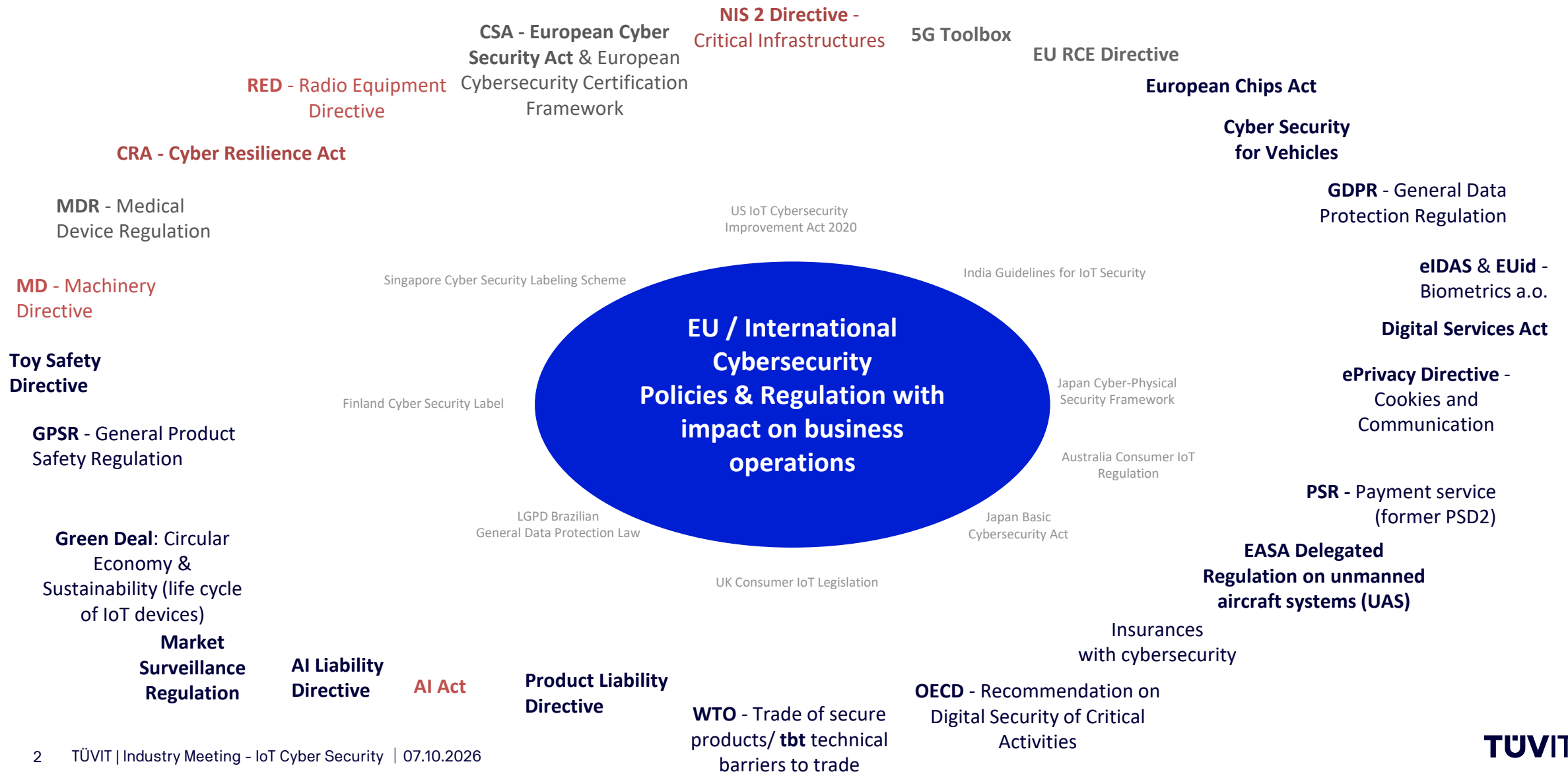


Von der Regulierung zur Umsetzung: CRA mit Hilfe von (EN) IEC 62443

EU regulations and directives on Cyber Security



Der Cyber Resilience Act im Überblick

Regulierung (EU) 2024/2847 schafft einen harmonisierten Cybersecurity-Rahmen für alle Produkte mit **digitalen Elementen (PwDE)**, die in der EU in Verkehr gebracht werden – von IoT-Geräten bis zu industriellen Steuerungssystemen.

10.12.2024

06.12.2025

11.09.2026

20.01.2027

11.12.2027

CRA tritt in Kraft

NIS2 in D tritt in Kraft

Pflicht:
Schwachstellen-
management &
Meldewesen

Neue MVO in EU
tritt in Kraft

Volle Anwendbarkeit des
CRAs für alle
“essentiellen
Produktfunktionen”

Geltungsbereich: Produkte mit digitalen Elementen
(Hard- und Software mit Kommunikationsfähigkeiten), Bsp:

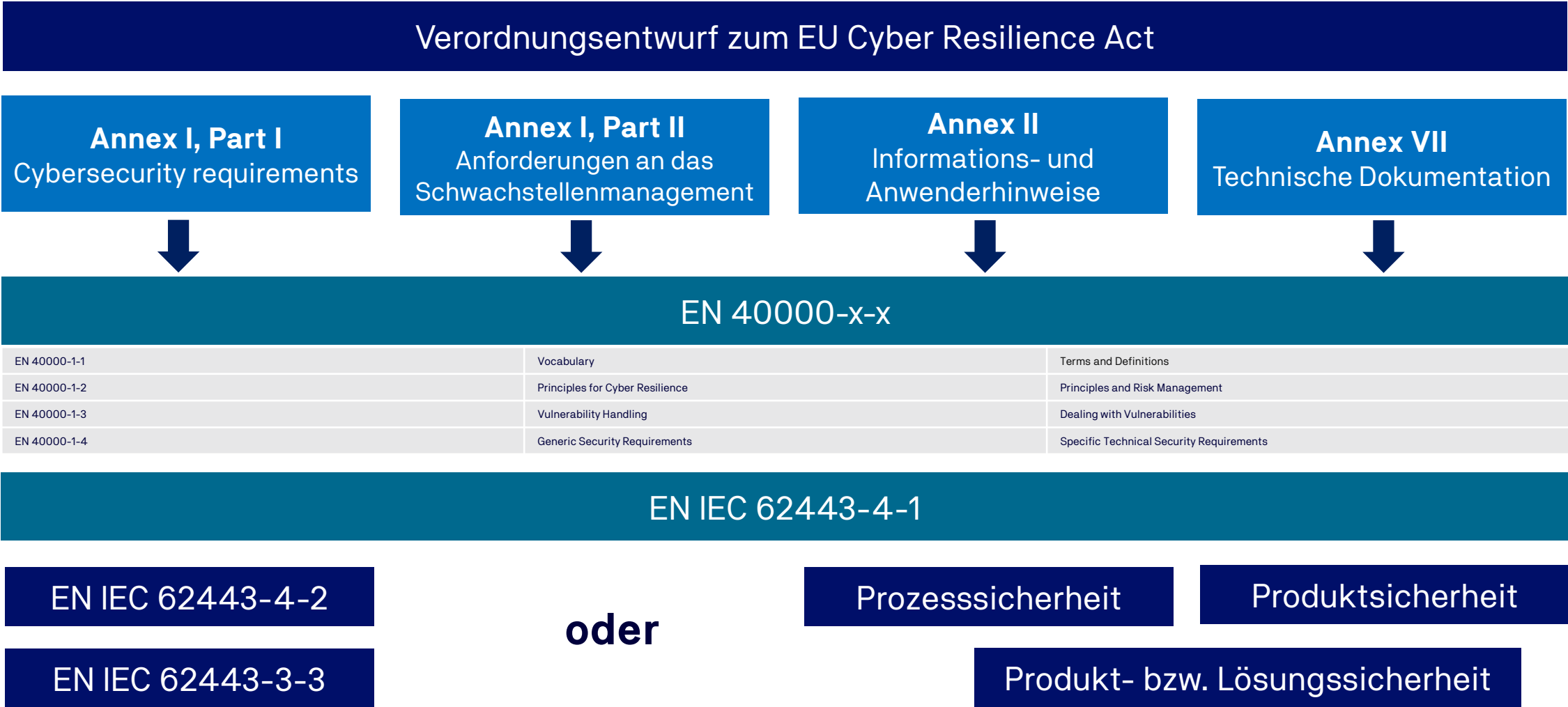
- Consumer-IoT-Geräte
- Professionelle IT-Systeme
- Software-Produkte
- Industrielle Steuerungssysteme (inkl. kritische Infrastruktur)

Sanktionen bei Verstoß

bis zu 2,5 %

des weltweiten Jahresumsatzes (Art. 69 CRA)
zzgl. Verlust der CE-Kennzeichnung

(EN) IEC 62443 als strukturierter Rahmen für den CRA (1/2)



(EN) IEC 62443 als strukturierter Rahmen für den CRA (2/2)

Wer regelt was



Welche Normen für welches Produkt?

Produkttyp	Relevante Normen
Consumer-IoT, Software, IT-Produkte	EN 40000 + produktspezifische CRA-Normen
Industrielle Produkte / OT	EN 40000 + IEC 62443
Maschinen mit digitalen Komponenten	En 40000 + IEC 62443 + Maschinenverordnung

Proposed ETSI EN 3046xx Standards as harmonized standards for CRA Class 1&2 Products

[EN_304-617_V1.0.0_2026-08-12_Browsers_Enquiry-draft.pdf](#)

[EN_304-618_V0.2.2_2026-06-22_Password-managers_Enquiry-draft.pdf](#)

[EN_304-619_V1.0.0_2026-07-15_Antivirus_Enquiry-draft.pdf](#)

[EN_304-620_v1.0.0_2026-08-12_Virtual-Private-Networks_Enquiry-draft.pdf](#)

[EN_304-621_V1.0.5_2026-08-12_Network-Management-Systems_Enquiry-draft.pdf](#)

[EN_304-622_V1.0.0_2026-08-12_Security-Information-Event-Management_Enquiry-draft.pdf](#)

[EN_304-623_V0.1.3_2026-06-17_Boot_Managers_Enquiry-draft.pdf](#)

[EN_304-624_V1.0.0_2026-08-05_PKI_certificate_issuance_software_Enquiry-draft.pdf](#)

[EN_304-625_V1.0.0_2026-08-10_Network-Interfaces_Enquiry-draft.pdf](#)

[EN_304-626_V1.0.1_2026-08-12_Operating-Systems_Enquiry-draft.pdf](#)

[EN_304-627_V1.0.1_2026-07-06_Routers-modems-switches_Enquiry-draft.pdf](#)

[EN_304-631_V1.0.0_2026-07-20_Smart-home-virtual-assistants_Enquiry-draft.pdf](#)

[EN_304-632_V1.0.0_2026-07-20_Smart-home-security-products_Enquiry-draft.pdf](#)

[EN_304-633_V1.0.0_2026-07-20_Internet-connected-toys_Enquiry-Draft.pdf](#)

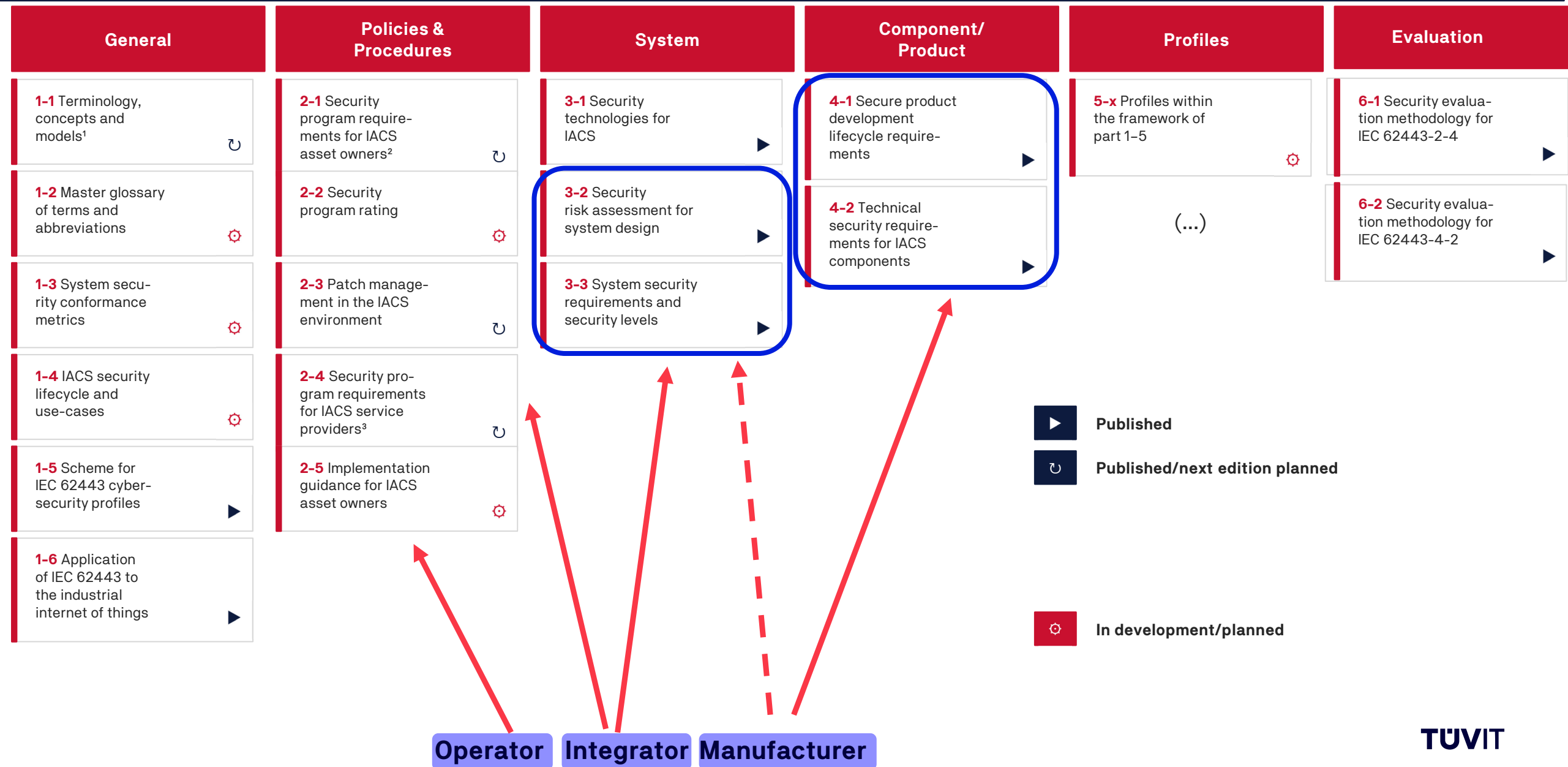
[EN_304-634_V1.0.0_2026-07-24_Personal-wearables_Enquiry-draft.pdf](#)

[EN_304-635_V1.0.1_2026-06-24_Virtualization_Container_Enquiry-draft.pdf](#)

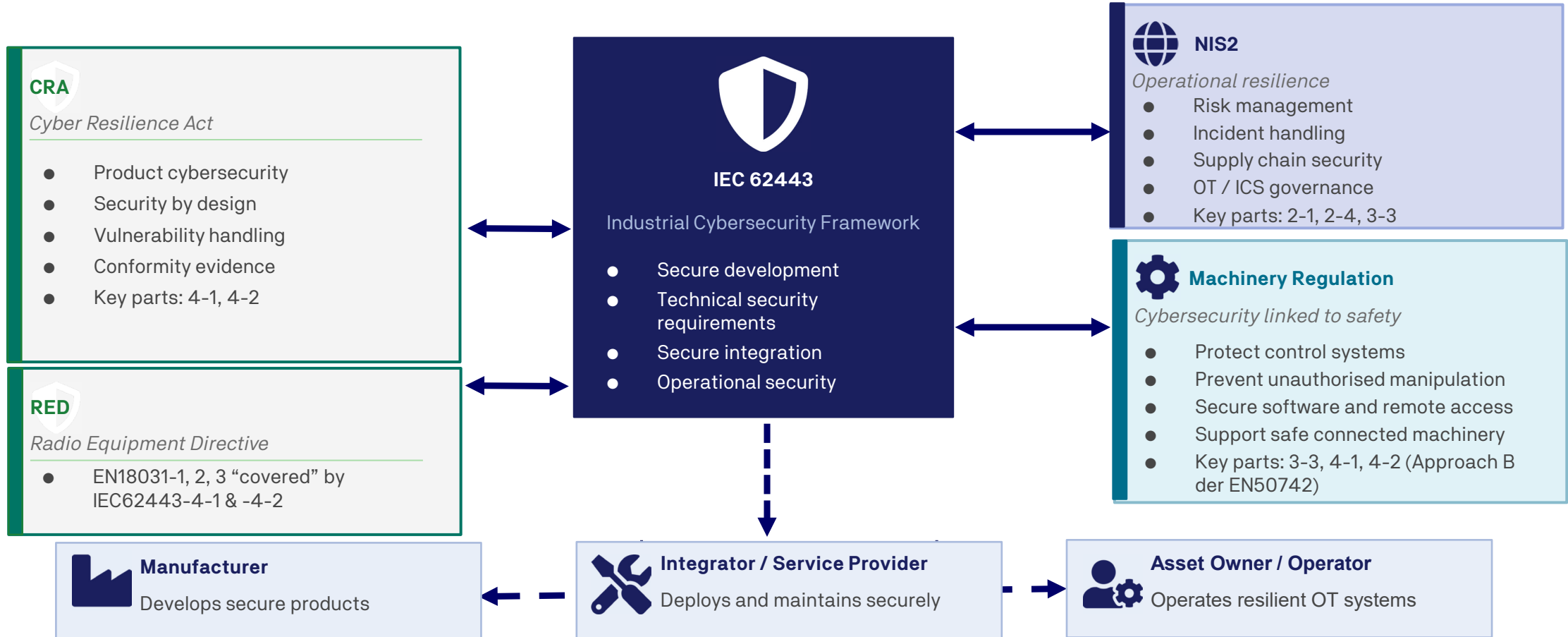
[EN_304-636_V1.0.0_2026-07-09_Firewalls_Enquiry-draft.pdf](#)

IEC 62443

Security for Industrial Automation and Control Systems



Wie (EN) die Norm IEC 62443 CRA, NIS2 und die Maschinenrichtlinie unterstützt



Die Norm IEC 62443 bildet eine Brücke zwischen gesetzlichen Anforderungen und der praktischen Umsetzung der Cybersicherheit in der Industrie.

Pflichten der Hersteller

Bevor ein Produkt mit digitalen Elementen in der EU in Verkehr gebracht werden darf, muss der Hersteller folgenden **Prozess** durchlaufen:



Ohne nachgewiesene Konformität darf kein digitales Produkt ab dem 11.12.27 im EU-Markt verkauft werden.

Klassifizierung nach CRA

Standardprodukte mit digitalen Elementen	Wichtige Produkte – Klasse I	Wichtige Produkte – Klasse II	Kritische Produkte mit digitalen Elementen
<i>Nicht gelistet in Anhang III oder IV</i>	<i>Anhang III, Teil I</i>	<i>Anhang III, Teil II</i>	<i>Anhang IV</i>
Konformitätsbewertung	Konformitätsbewertung	Konformitätsbewertung	Konformitätsbewertung
Interne Kontrolle (Modul A) möglich wesentlichen Cybersicherheitsanforderungen aus Anhang I	Selbstbewertung möglich bei Anwendung harmonisierter Normen – andernfalls notifizierte Stelle erforderlich	Notifizierte Stelle erforderlich (z. B. Modul B+C oder Modul H)	Bewertung durch Dritte oder EU-Cybersicherheits- Zertifizierungsschema
Beispielprodukte	Beispielprodukte	Beispielprodukte	Beispielprodukte
• Videospiele • Bildbearbeitungssoftware • Allgemeine Software & Geräte • Vernetzte Haushaltsgeräte IEC62443	• Passwort-Manager • Betriebssysteme • Browser, VPN-Produkte • Router, Modems, Switches • SIEM, Netzwerkmanagement	• Firewalls • Intrusion-Detection-/ • Prevention-Systeme • Manipulationssichere • Mikroprozessoren & Mikrocontroller	• Smart-Metering-Gateways • Smartcards / Secure Elements • Hardware-Sicherheitsmodule • HW-Geräte mit Sicherheitsboxen EU CC

EN 40000 Normen Familie

Die Normenreihe EN 40000 konzentriert sich in erster Linie auf die Umsetzung des Cyber Resilience Act (CRA).

EN 40000-1-1	Vocabulary	Terms and Definitions
EN 40000-1-2	Principles for Cyber Resilience	Principles and Risk Management
EN 40000-1-3	Vulnerability Handling	Dealing with Vulnerabilities
EN 40000-1-4	Generic Security Requirements	Specific Technical Safety Requirements

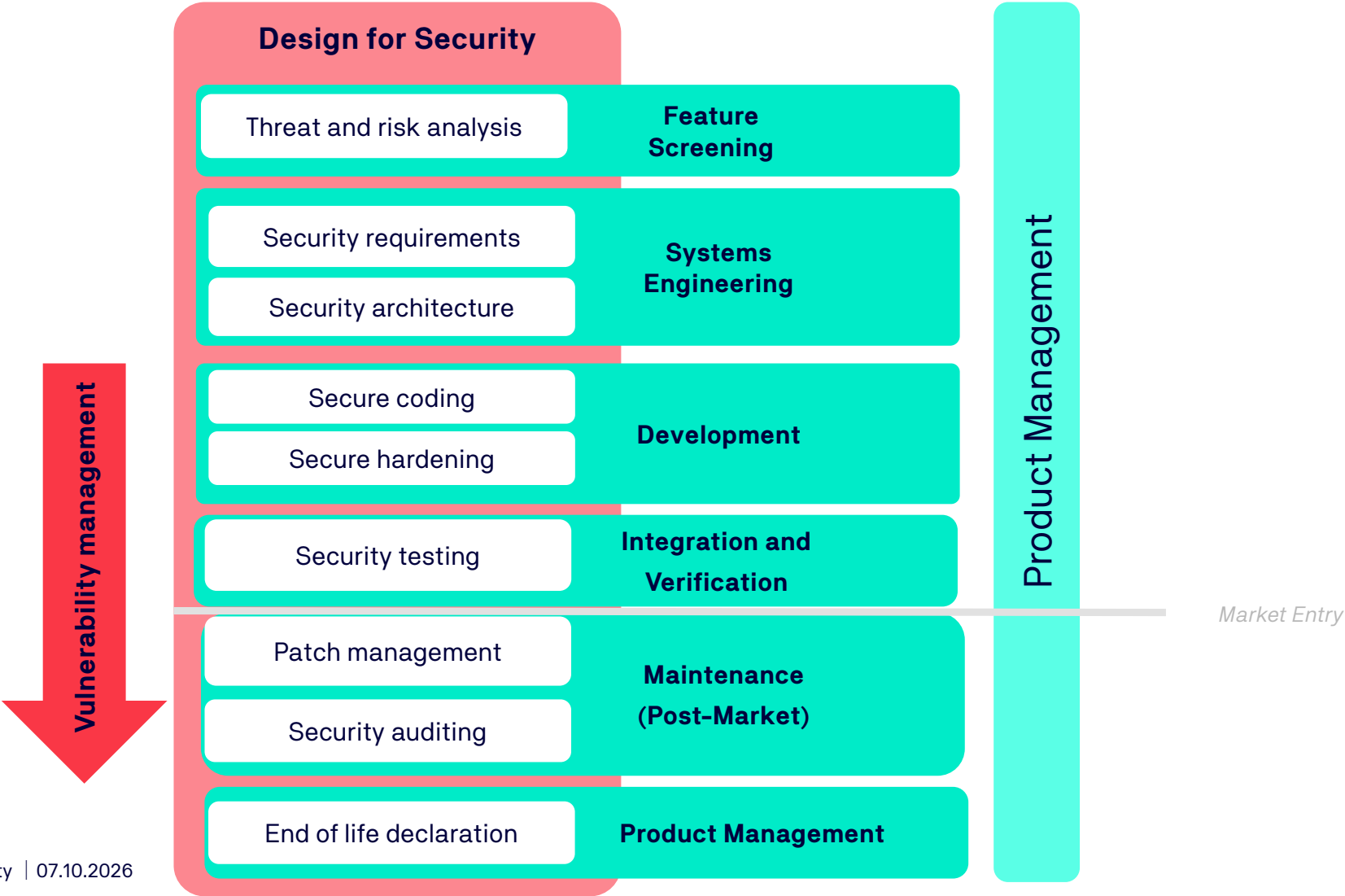
EN 40000-1-2

- Risikobasierter Ansatz
- Sicherheit durch Design
- Sicherheit als Standard
- Bedrohungs- und Risikoanalyse
- Festlegung von Risikoakzeptanzkriterien
- Risikobehandlung und -überwachung
- Sichere Architektur und Implementierung
- Sichere Produktion
- Wartung und Updates
- Sichere Außerbetriebnahme

EN 40000-1-4

- Sichere Standardkonfiguration
- Zugriffskontrolle
- Schutz der Vertraulichkeit und Integrität
- Sicherheitsupdates
- Schwachstellenanalyse
- Verringerung der Angriffsfläche
- Protokollierung und Überwachung
- Datenminimierung
- Verfügbarkeit
- Sichere Datenlöschung

Überblick über den „Sicheren Produkt Lebenszyklus“ nach der IEC62443-4-1 und die relevanten Stakeholder



IEC 62443-4-2 – Technische Sicherheitsanforderungen (Beispiel)

CR 1.1 – Human user identification and authentication	5.3	CR 1.1 – Identifizierung und Authentifikation von menschlichen Nutzern	SL-1	SL-2	SL-3	SL-4
	5.3.1	Die Komponente muss die Fähigkeit haben, alle menschlichen Nutzer an allen Schnittstellen mit der Möglichkeit eines Zugriffs durch den menschliche Nutzer nach SR 1.1 in IEC 62443-3-3 zu identifizieren und zu authentifizieren. Diese Fähigkeit muss an allen Schnittstellen, die menschlichen Nutzern Zugriff auf die Komponente gewähren, eine Identifizierung und Authentifikation in einer Art und Weise durchsetzen, dass die Trennung von Aufgaben und das Prinzip der minimal erforderlichen Rechte entsprechend den geltenden IT-Sicherheitsleitlinien und -vorgehensweisen unterstützt wird. ANMERKUNG Die gelten IT-Sicherheitsrichtlinien unterliegen lokalen Vorgaben.	✓	✓	✓	✓
	5.3.3.1	(1) Eindeutige Identifizierung und Authentifikation Die Komponente muss die Fähigkeit haben, alle menschlichen Nutzer eindeutig zu identifizieren und zu authentifizieren.		✓	✓	✓
	5.3.3.2	(2) Multifaktor-Authentifikation über alle Schnittstellen Die Komponente muss die Fähigkeit haben, eine Multifaktor-Authentifikation für den Zugriff aller menschlichen Nutzer auf die Komponente zu verwenden.			✓	✓

TÜVIT-Leistungen (CRA)

- Scoping Workshop & Gap-Analyse
 - Erweiterte GAP-Analyse zur Unterstützung der Konformitätsbewertung
 - Begleitete Threat & Risk Analyse nach IEC 62443-3-2
 - Unabhängige Penetrationstests
 - Konformitätsbewertung für die CRA-Zertifizierung (sobald Akkreditierung für Modul B und H abgeschlossen ist)
 - Alle zertifizierbaren Normenteile der IEC 62443
-
- **Ab Q1/27 (Plan) : EN IEC 62443 & CRA Zertifizierungen**

Kontakt

Gerald Krebs

TÜV Informationstechnik GmbH

TÜV NORD GROUP

Product and Sales Management for Cybersecurity

Am TÜV 1

45307 Essen

Tel./Mobil: +49 201 8999-411 / +49 160 8885427

E-Mail: g.krebs@tuvit.de

URL: [IEC 62443: Auf Industrial Security setzen | TÜVIT](#)