

Cyber Resilience Act

Der Weg zur Konformität



Agenda

Thematische Abschnitte

1. Vorstellung des CRA
2. Meilensteine des CRA
3. Weg zur Konformität

Vorstellung des Cyber Resilience Act

Wie stehen CRA und die CE-Kennzeichnungspflicht zueinander?



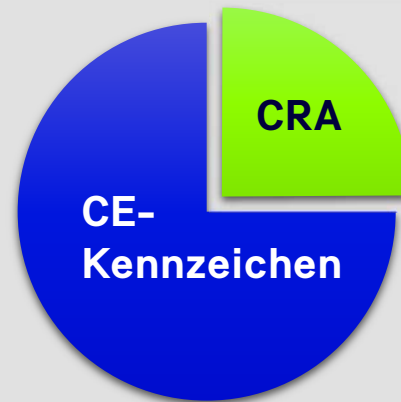
Der CRA ist eine EU-Verordnung (wie auch die DSGVO) mit dem Ziel, die digitale Sicherheit für „**Produkte mit digitalen Elementen**“ in der EU zu stärken.

Dies sind Hard- oder Software-Produkte (ggf. inkl. Backend), deren bestimmungsgemäße oder vorhersehbare Verwendung eine direkte oder indirekte, logische oder physische Datenverbindung zu einem Gerät oder Netz einschließt.

CE Kennzeichen

CE-Kennzeichen allgemein:

- **Markteintrittsvoraussetzung** in den EWR* für die meisten Produkte, sofern keine anderen Regelungen bestehen. Das Ziel sind sichere Produkte.
- Die Kennzeichnungspflicht ergibt sich aus **EU-Richtlinien und -Verordnungen** – u. a. dem **CRA**.
- Kennzeichnungspflicht nicht für alle Produkte.



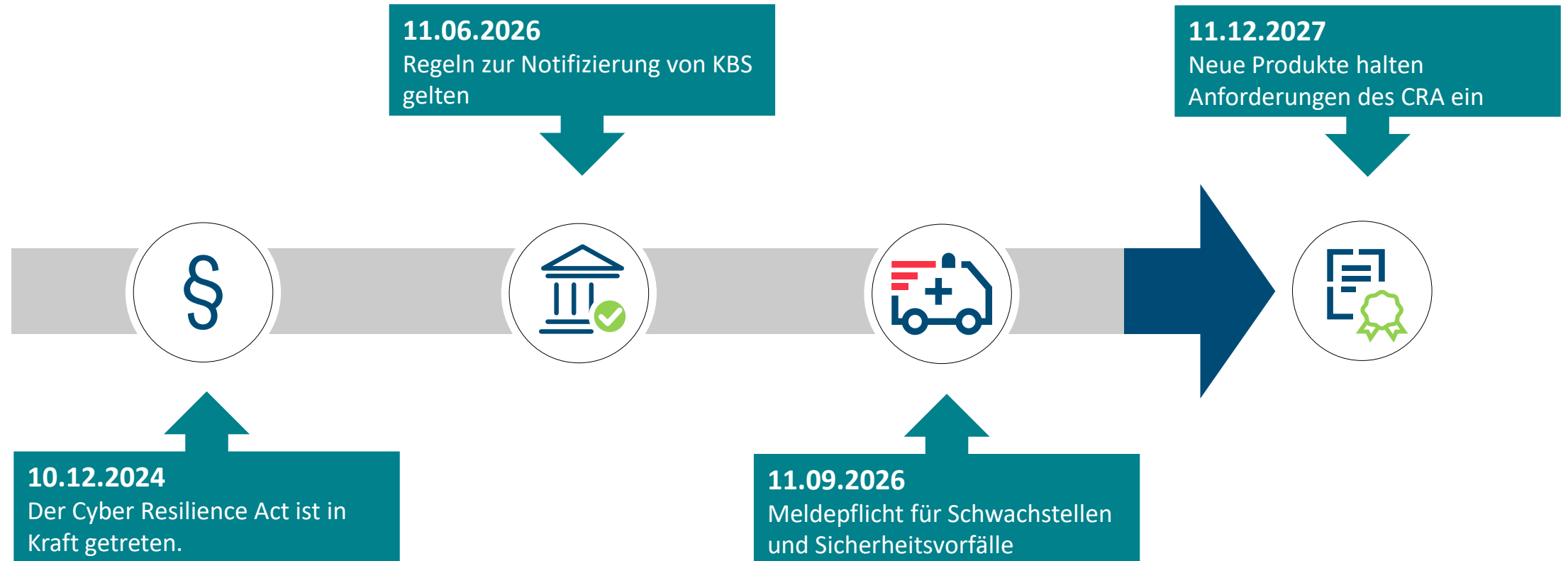
*EWR: Europäischer Wirtschaftsraum

Bezug zum CRA:

- Ohne Konformität zum CRA kann für „**Produkte mit digitalen Elementen**“ keine CE-Kennzeichnung erfolgen (Artikel 27 ff).
- Hersteller müssen nachweisen / bestätigen, dass sie den CRA erfüllen (ab **11.12.2027**)
- **Ohne CE-Kennzeichen** dürfen die Produkte ab dem 11.12.2027 nicht im EWR* in Verkehr gebracht / verkauft werden. Bereits zuvor in Verkehr gebrachte Produkte sind nur bei wesentlicher Änderung betroffen – die Meldepflicht gilt für sie aber schon seit 11.09.2026.

Meilensteine des Cyber Resilience Act

Wichtige Schritte innerhalb des Übergangszeitraums



Weg zur Konformität

Sechs Schritte vom Produktinventar bis zur CE-Kennzeichnung



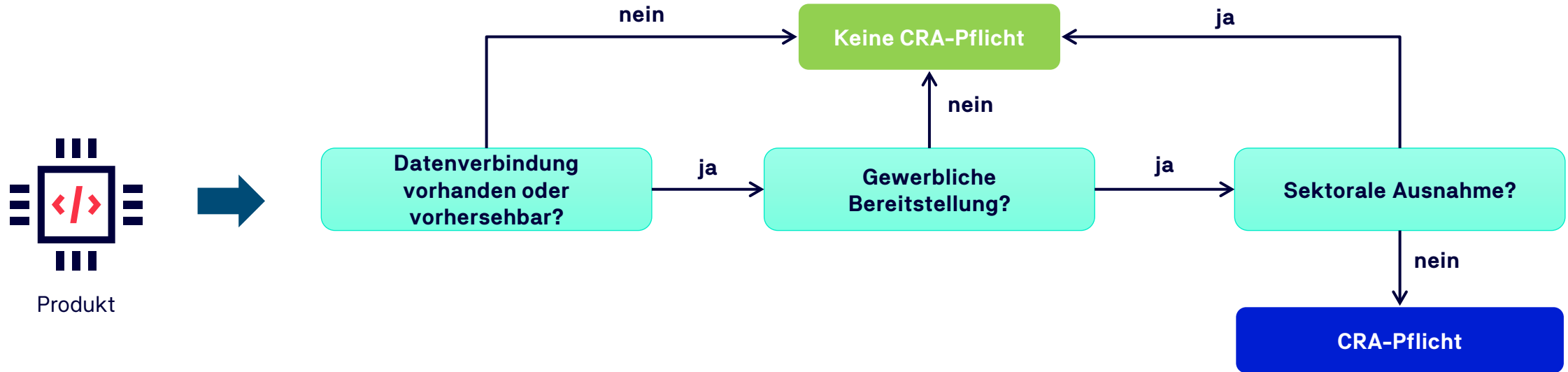
Weg zur Konformität

Sechs Schritte vom Produktinventar bis zur CE-Kennzeichnung



Schritt 1 im Detail: Produktinventarisierung & Klassifizierung

Fällt mein Produkt unter den CRA?



Details

Datenverbindung: Hierzu zählen WLAN, Bluetooth, USB, API etc.

Gewerbliche Bereitstellung: entscheidend ist die geschäftliche Absicht, nicht der Preis – auch kostenlose Bereitstellung zählt, wenn sie monetarisiert wird (z. B. über Werbung, Datennutzung, kostenpflichtigen Support). Nicht-kommerzielle Spenden oder reine Kostendeckung zählen nicht. Maßgeblich ist die Bereitstellungsphase, nicht die Finanzierung der Entwicklung – ein spendenfinanziertes Open-Source-Projekt bleibt außerhalb des CRA, solange die Software selbst nicht monetarisiert wird. Ausnahme: Open-Source-Stewards (Art. 24) haben eingeschränkte Pflichten.

Sektorale Ausnahme: Medizinprodukte, Kfz-Typgenehmigung, Luftfahrt, Seeschifffahrt, Verteidigung

Schritt 1 im Detail: Produktkategorien innerhalb des CRA

Anhänge III und IV des CRA

Produkte mit digitalen Elementen	Wichtige Produkte mit digitalen Elementen Klasse I*	Wichtige Produkte mit digitalen Elementen Klasse II	Kritische Produkte mit digitalen Elementen
„Standardklasse“: Alle Produkte, die in keiner der anderen Gruppen einsortiert sind! - Ca. 90% aller Produkte	- Passwort-Manager - Public-Key-Infrastrukturen und Software für die Ausstellung digitaler Zertifikate - Router, Modems für die Internetanbindung und Switches - Netzmanagementsysteme Artikel 7 bzw. Annex III - Produkte erfüllen Funktionen mit Relevanz für Cybersicherheit anderer Produkte, Netze oder Dienste - Produkte erfüllen Funktionen, die ein erhebliches Risiko nachteiliger Auswirkungen bergen. - Anpassungen durch EU-Kommission	- Hypervisoren etc. - Firewalls, Intrusion-Detection-Systeme - Manipulationssichere Mikroprozessoren und -Mikrocontroller	- Hardware mit Sicherheitsboxen - Smart-Meter-Gateways - Andere Geräte für fortgeschrittene Sicherheitszwecke - Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselementen Artikel 8 bzw. Annex IV - Abhängigkeit wesentlicher Einrichtungen (u.a. nach NIS 2) von Produkten - Potentielle Gefahr für kritische Lieferketten

Bei Mehrfachzuordnung

- Einordnung:** nach der Kernfunktion des Produkts (Art. 7 Abs. 1) – Nebenfunktionen zählen nicht zusätzlich
- Beispiel:** Ein NAS mit VPN bleibt in der Standardklasse
- Technische Beschreibungen** aller 26 Kategorien: Durchführungsverordnung (EU) 2025/2392 vom 28.11.2025

Weg zur Konformität

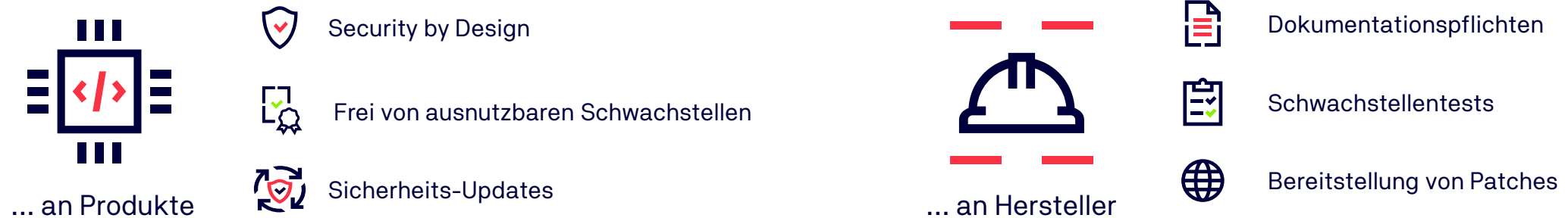
Sechs Schritte vom Produktinventar bis zur CE-Kennzeichnung



Schritt 2: Grundlegende Sicherheitsanforderungen

Anhang I des CRA

Anhang I definiert 22 grundlegende Cybersicherheitsanforderungen, welche für das Produkt (14) und den Hersteller (8) gelten. Im Kontext des CRA werden sie als „Essential Cybersecurity Requirements“ (ECR) bezeichnet und bilden die sogenannten horizontalen Anforderungen. Beispielhafte Anforderungen ...



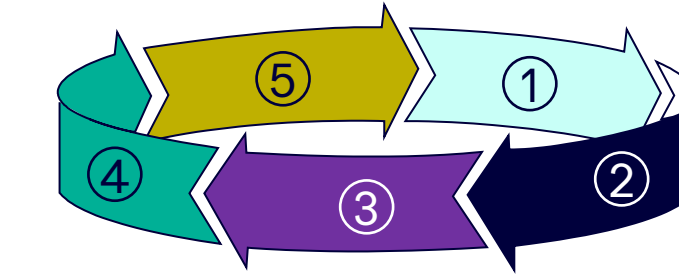
- Die horizontalen Anforderungen werden in europäischen Normen konkretisiert (prEN 40000-Reihe, noch im Entwurf).
- Für wichtige und kritische Produkte (Anhang III/IV) entstehen zusätzlich produktspezifische, sogenannte vertikale Normen.

Schritt 2: Risikobewertung & Gap-Analyse: Wie geht man vor?

Praktischer Ansatz ohne feste Methodenvorgabe

Risikobewertung aktualisieren: Wirksamkeit der Maßnahmen prüfen, verbleibende Restrisiken bewerten und dokumentieren – für die Prozess-Reife z. B. erneut mit dem ENISA SME Maturity Model, um Fortschritt seit der letzten Bewertung objektiv zu messen

Maßnahmen ableiten und umsetzen: Identifizierte Gaps risikobasiert priorisieren und durch technische oder organisatorische Maßnahmen schließen – als Orientierung z. B. der risikobasierte Maßnahmenkatalog der BSI TR-03183-1 (maschinenlesbar via OSCAL)



Produkt analysieren: Architektur, Funktionen, Schnittstellen, Einsatzumgebung und Abhängigkeiten erfassen, um daraus **Verwendungszweck, vorhersehbare (Fehl-)Nutzung, Nutzungsbedingungen** und **erwartete Nutzungsdauer** abzuleiten (Art. 13 Abs. 3)

Gap-Analyse durchführen: Die anwendbaren CRA-Anforderungen mit dem tatsächlichen Zustand des Produkts und der Herstellerprozesse vergleichen und Abweichungen identifizieren – für die Prozess-Reife z. B. mit dem ENISA SME Maturity Model.

Risiken bewerten: Bedrohungen und Schwachstellen identifizieren, mögliche Auswirkungen bewerten und daraus die für das Produkt anwendbaren Sicherheitsanforderungen bestimmen – als Orientierung z. B. die Bedrohungs- und Sicherheitszielbeschreibungen der prEN 40000-1-4

Das Ergebnis jeder Aktualisierung fließt unmittelbar in die technische Dokumentation ein – die vor Markteinführung vorliegen und über den gesamten Support-Zeitraum aktuell gehalten werden muss (Art. 13 Abs. 4).

Weg zur Konformität

Sechs Schritte vom Produktinventar bis zur CE-Kennzeichnung



Schritt 3 im Detail: SBOM

Software Bill of Material

Was gehört die SBOM

- **Inhalt:** mind. alle Top-Level-Komponenten inkl. Version und Herkunft, auch Open Source/Drittanbieter – tiefere Ebenen empfohlen
- **Format:** maschinenlesbares Format
 - **BSI TR-03183-2** (nicht bindend): CycloneDX ≥ 1.6 oder SPDX $\geq 3.0.1$, Pflichtfelder u. a Name/Version, Ersteller, purl, Lizenz, Hash, Abhängigkeiten
 - **Vorteil TR-Nutzung:** Prüfsicherheit ggü. BSI als Marktüberwachungsbehörde, weniger Interpretationsspielraum
- **Aktualisierung:** bei jeder neuen Version bzw. jedem sicherheitsrelevanten Update
- **Aus CM ableitbar:** Lock-Files/Build-Tools liefern die Basis (Syft/cdxgen), Lücken bei Formatnormierung, Vendor-Code und Hardware-BOM bleiben

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "metadata": {
    "timestamp": "2026-10-01T08:00:00Z",
    "manufacturer": { "name": "Beispiel GmbH" },
    "component": { "bom-ref": "gateway", "name": "IoT-Gateway" }
  },
  "components": [
    {
      "bom-ref": "libcurl",
      "name": "libcurl",
      "version": "8.9.1",
      "manufacturer": { "name": "curl project" },
      "purl": "pkg:generic/curl@8.9.1",
      "licenses": [ { "license": { "id": "curl" } } ],
      "hashes": [ { "alg": "SHA-512", "content": "3f5c...a91e" } ],
      "properties": [
        { "name": "bsi:component:filename", "value": "libcurl.so.4" },
        { "name": "bsi:component:executable", "value": "executable" },
        { "name": "bsi:component:archive", "value": "no archive" },
        { "name": "bsi:component:structured", "value": "structured" }
      ]
    },
    { "bom-ref": "openssl", "name": "openssl", "version": "3.3.2", ... }
  ],
  "dependencies": [
    { "ref": "gateway", "dependsOn": [ "libcurl" ] },
    { "ref": "libcurl", "dependsOn": [ "openssl" ] }
  ]
}
```

Schritt 3 im Detail: Schwachstellenmanagement

Was der CRA vor und nach der Markteinführung verlangt

Vor Markteinführung: Schwachstellenmanagement aufbauen



Schwachstellen identifizieren

Alle Komponenten per SBOM erfassen und laufend auf bekannte Schwachstellen prüfen



Offenlegung regeln (CVD-Policy)

Festlegen, wie Hinweise von außen bearbeitet und erst nach Behebung veröffentlicht werden



Kontaktstelle für Hinweise einrichten

Erreichbare Anlaufstelle, über die Externe Schwachstellen mitteilen können



Sichere Update-Verteilung

Updates so ausliefern, dass sie nicht manipuliert oder untergeschoben werden können

MARKTEINFÜHRUNG



Voraussetzung für den Marktzugang:

Keine bekannten ausnutzbaren Schwachstellen

d. h. im konkreten Einsatz des Produkts nicht angreifbar

Nach Markteinführung: Schwachstellenmanagement betreiben



Regelmäßig testen

Sicherheitstests vor dem Release und danach laufend wiederholen; Methode frei wählbar



Unverzüglich beheben

Die gefährlichsten zuerst; Sicherheitsupdates möglichst getrennt von neuen Funktionen



Updates ausliefern

Unverzüglich und kostenlos¹ – mit Hinweisen, was Nutzer tun müssen



Sicherheitshinweis veröffentlichen

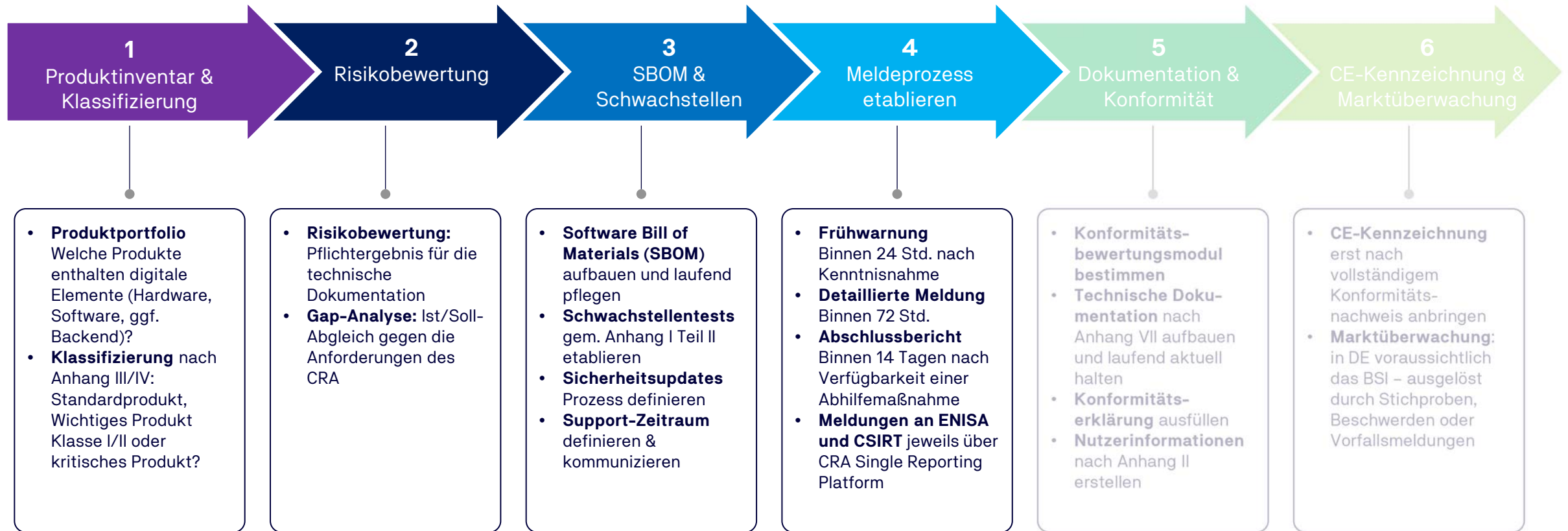
Nach Behebung (Advisory): was betroffen ist, wie schwer, wie man sich schützt

Support-Zeitraum: Zeitraum, in dem der Hersteller Sicherheitsupdates liefern muss, i. d. R. mind. 5 Jahre (Art. 13 Abs. 8) · Grundlage: Anhang I Teil I Nr. 2a und Teil II

¹ sofern bei maßgeschneiderten Produkten für Geschäftskunden nicht anders vereinbart

Weg zur Konformität

Sechs Schritte vom Produktinventar bis zur CE-Kennzeichnung



Schritt 4 im Detail: Meldeprozess für Schwachstellen und Vorfälle

Was gemeldet wird, mit welcher Frist – und an wen



Aktiv ausgenutzte Schwachstelle

Art. 3 Nr. 42

Zuverlässiger Nachweis, dass ein Angreifer sie ohne Erlaubnis ausgenutzt hat – die bloße Existenz reicht nicht



Schwerer Sicherheitsvorfall

Art. 14 Abs. 5

Gefährdet Verfügbarkeit, Echtheit, Integrität oder Vertraulichkeit – oder schleust Schadcode ein (bzw. kann das)



Nicht meldepflichtig

Bekannte Lücke ohne Angriff, Proof of Concept, Pentest-Fund, autorisierte Forschung

Seit 11.09.2026

Meldefristen ab Kenntnisnahme – gilt auch für Produkte, die bereits im Markt sind



Wer muss informiert werden?



Behörden seit 11.09.2026

Über die Single Reporting Platform gleichzeitig an ENISA und BSI (nationales CSIRT)



Betroffene Nutzer seit 11.09.2026

Über den Vorfall bzw. die Schwachstelle und mögliche Schutzmaßnahmen (Art. 14 Abs. 8)



Zulieferer ab 11.12.2027

Schwachstellen in Fremdkomponenten an deren Hersteller melden (Art. 13 Abs. 6)

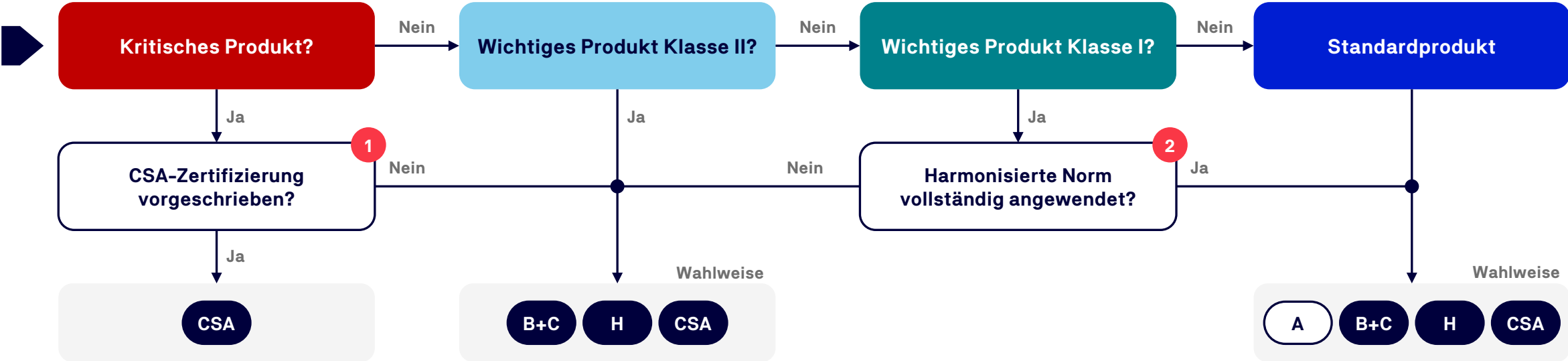
Weg zur Konformität

Sechs Schritte vom Produktinventar bis zur CE-Kennzeichnung



Schritt 5 im Detail: Welches Bewertungsverfahren gilt?

Konformitätsbewertungsverfahren nach Art. 32 CRA



- 1 Nur wenn per delegiertem Rechtsakt ein EU-Zertifikat vorgeschrieben ist (Art. 8 Abs. 1) – sonst gilt der Weg für Klasse II (Art. 32 Abs. 4).
- 2 Selbsterklärung nur bei vollständiger Anwendung einer hEN, gemeinsamer Spezifikation oder eines EU-Zertifikats ≥ „mittel“ (Art. 32 Abs. 2) – bis dahin braucht Klasse I faktisch eine notifizierte Stelle.

Legende gefüllt = mit notifizierter Stelle bzw. Zertifizierungsstelle

A Interne Kontrolle Selbsterklärung des Herstellers	B+C Baumusterprüfung + Bauart-konformität Stelle prüft ein Baumuster	H Umfassende Qualitätssicherung Stelle bewertet das QS-System	CSA EU-Cybersicherheitszertifikat nach VO (EU) 2019/881
--	---	--	--

Schritt 5 im Detail: Technische Dokumentation

Anhang VII: die acht Pflichtinhalte



1

Produktbeschreibung

Zweck, Softwareversionen, Hardware-Fotos, Nutzerinformationen



2

Design & Prozesse

Architektur, SBOM, CVD-Policy, Kontaktadresse, Update-Verteilung



3

Risikobewertung

Welche der 14 Produktanforderungen gelten – und wie sie umgesetzt sind



4

Support-Zeitraum

Grundlage für die festgelegte Dauer (Art. 13 Abs. 8)



5

Normen & Spezifikationen

Angewandte Normen, Spezifikationen, Zertifikate – oder eigene Lösung



6

Testberichte

Nachweis der Konformität mit Anhang I Teil I und II



7

Konformitätserklärung

Kopie der EU-Konformitätserklärung



8

SBOM auf Anfrage

Herausgabe an die Marktüberwachung auf begründete Anfrage



5 Normen & Spezifikationen im Detail

Norm angewandt? Liste mit Fundstelle – bei Teilanwendung die Teile benennen

Keine Norm? Eigene Lösung beschreiben: wie Anhang I stattdessen erfüllt wird

Immer: Liste sonstiger technischer Spezifikationen – der Ankerpunkt für Auditoren

Typische Einträge

BSI TR-03183 Teil 1-3 · EN 18031-Reihe (aus der Funkanlagenrichtlinie) · ETSI EN 303 645 · IEC 62443-4-1/-4-2 · ISO/IEC 29147, 30111

Vor dem Inverkehrbringen erstellt, laufend aktuell gehalten (Art. 31) · **Aufbewahrung: mind. 10 Jahre oder Support-Zeitraum – der längere zählt (Art. 13 Abs. 13)**

Schritt 5 im Detail: EU-Konformitätserklärung

Voraussetzungen, Verantwortung und Pflichtinhalt (Art. 28, Anhang V)

Wann ist sie gültig? Art. 28

- ✓ **Bewertung abgeschlossen** – das gewählte Verfahren ist tatsächlich durchlaufen
- ✓ **Vor dem Inverkehrbringen erstellt** – Voraussetzung für das CE-Zeichen
- ✓ **Vollständig** – alle 8 Pflichtelemente aus Anhang V
- ✓ **In der geforderten Sprache** – des jeweiligen Mitgliedstaats
- ✓ **Aktuell gehalten** – bei Änderungen am Produkt nachgeführt



Unterschrift immer vom Hersteller

in alleiniger Verantwortung – auch bei Modul B+C, H oder CSA. Die notifizierte Stelle stellt ihr eigenes Zertifikat aus und wird in der Erklärung nur referenziert.

Gelten mehrere EU-Rechtsakte (z. B. RED, EMV, CRA): eine gemeinsame Erklärung (Art. 28 Abs. 3).

EU-KONFORMITÄTSERLÄRUNG

Pflichtinhalt nach Anhang V

- 1 Produkt: Name, Typ, eindeutige Kennung
- 2 Hersteller bzw. Bevollmächtigter mit Anschrift
- 3 Erklärung der alleinigen Verantwortung
- 4 Gegenstand der Erklärung, rückverfolgbar
- 5 Konformität mit der Harmonisierungsvorschrift
- 6 Angewandte Normen / Spezifikationen
- 7 ggf. notifizierte Stelle: Name, Nr., Verfahren, Zertifikat
- 8 Ort, Datum, Name, Funktion, Unterschrift

Weg zur Konformität

Sechs Schritte vom Produktinventar bis zur CE-Kennzeichnung



Schritt 6 im Detail: CE-Kennzeichnung & Marktüberwachung

Kennzeichnen, im Markt halten, überwacht werden



Was bei Verstößen droht

1

Korrektur verlangen

2

Bereitstellung einschränken

3

Rücknahme oder Rückruf

15 Mio. €
oder 2,5 % vom Jahresumsatz
Kernanforderungen verletzt
Anhang I, Art. 13, 14

10 Mio. €
oder 2 % vom Jahresumsatz
Sonstige Pflichten verletzt
z. B. CE, Doku, Erklärung

5 Mio. €
oder 1 % vom Jahresumsatz
Falsche Angaben
gegenüber Behörden oder Stellen

Bußgelder (Art. 64) – jeweils der höhere Betrag

Vielen Dank

Christian Noetzel

Tel.: +49 201 8999-651

E-Mail: c.noetzel@tuvit.de

