Deloitte.

# Cyber Resilience Act

WKW – Digitale Arbeitswelten

# Vorstellung

Ich freue mich auf den heutigen Vortrag

## Deloitte

# 1

Weltweit führend im Bereich Security Consulting: Im Jahr 2025 zum **13. Mal in 14 Jahren** mit dem größten Marktanteil Platz 1.

Quelle: Gartner, Market Share: Security Services, Worldwide

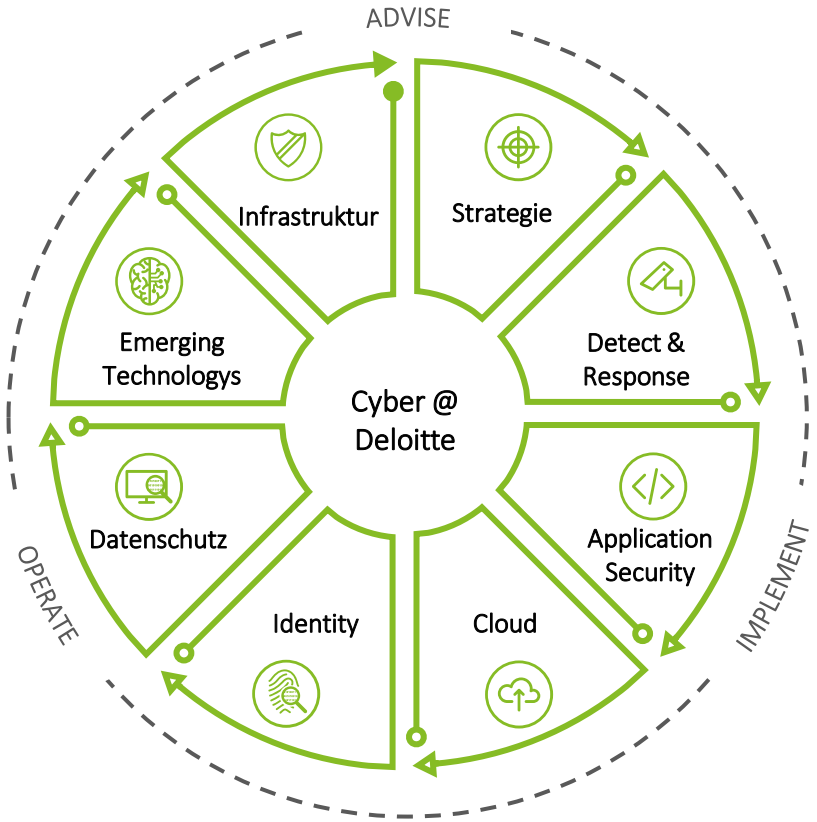

**Georg Schwondra**

Partner – Cyber

+43 664 80537 3760

gschwondra@deloitte.at


## Portfolio



# CRA | Allgemeines

## Allgemeine Informationen zum Cyber Resilience Act

### Was ist der CRA?

- CRA (Cyber Resilience Act) ist eine EU-Verordnung.
- Der CRA soll die Cybersicherheit von Produkten mit digitalen Elementen innerhalb der EU zu stärken.

### Adressaten

- Der CRA richtet sich an Hersteller, Importeure und Händler von Produkten mit digitalen Elementen, die auf dem EU-Markt bereitgestellt werden.

### Inhalt

- Vorgaben zur Cybersicherheit, z. B. Sicherheitsdesign, Schwachstellenmanagement und sichere Datenverarbeitung.
- Anforderungen an die Meldung von Schwachstellen und Sicherheitsvorfällen
- Sanktionen bei Verstößen, wie hohe Geldbußen oder Maßnahmen gegen nicht konforme Produkte.

### Ziel

- Cybersicherheit von Produkten in der EU stärken, um Angriffsflächen, -möglichkeiten und deren Auswirkungen zu minimieren.
- Vertrauen in den digitalen Binnenmarkt fördern, indem sichere Produkte gewährleistet werden.
- Einheitliche Anforderungen an die digitale Produktsicherheit in der gesamten EU schaffen.

### Umsetzung

- CRA ist am 11. Dezember 2024 in Kraft getreten.
- Die Verordnung gilt direkt in allen EU-Mitgliedstaaten und muss nicht in nationales Recht umgesetzt werden.
- Ab 11. September 2026 ist bereits die Meldepflicht für Sicherheitsvorfälle und Schwachstellen einzuhalten.
- Ab 11. Dezember 2027, sprich nach 3 Jahren Umsetzungsfrist ist der CRA vollständig in Geltung, d. h. alle Produkte müssen vollständig konform sein.

# CRA | Betroffenheit

## Wie erkenne ich, ob mein Produkt davon betroffen ist?

Der CRA betrifft Produkte mit digitalen Elementen, welche innerhalb der EU bereitgestellt werden und deren bestimmungsgemäßer Zweck oder vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz miteinschließt

- Handelt es sich um ein Soft- oder Hardwareprodukt?
- Hat das Produkt eine direkte oder indirekte Datenverbindung zu einem anderen Gerät oder Netz?
- Wird das Produkt auf dem EU-Markt bereitgestellt und sie agieren als Hersteller, Importeur oder Händler?
- Fällt das Produkt unter eine der Ausnahmen zum CRA?

**Der CRA ist relevant für das Produkt**

# CRA | Ausnahmen

Gewisse Produkte unterliegen strengeren Verordnungen oder erfordern bereits Cybersicherheitsmaßnahmen und sind daher von der Verordnung ausgenommen, um Doppelregulierung zu vermeiden.

**Medizinprodukte bzw. in-Vitro-Diagnostika**

Produkte, die unter die Verordnungen (EU) 2017/745 und 2017/746 fallen (Artikel 2 (2) a und b)

**Fahrzeuge und -teile**

Fahrzeuge und ihre Bauteile, die durch die Verordnung (EU) 2019/2144 geregelt werden (Artikel 2 (2) c)

**Luftfahrtkomponenten**

Produkte, die nach der Verordnung (EU) 2018/1139 zertifiziert wurden (Artikel 2 (3))

**Nat. Sicherheitsprodukte**

Produkte für ausschließliche Zwecke der nationalen Sicherheit, Verteidigungszwecke oder Verschlusssachen. (Artikel 2 (7))

**Schiffsausrüstung**

Schiffsausrüstung, die der Richtlinie 2014/90/EU unterliegt (Artikel 2 (4))

**Ersatzteile**

Ersatzteile, die ausschließlich identische Komponenten in bestehenden Produkten ersetzen. (Artikel 2 (6))

# CRA | Klassifikation der Produkte

Produkte werden basierend auf ihren Funktionen klassifiziert und unterliegen je nach Klassifikation unterschiedlichen Überprüfungsanforderungen.

| „Unwichtige“ Produkte mit digitalen Elementen | Wichtige Produkte mit digitalen Elementen | | Kritische Produkte |
|---|---|---|---|
| | Klasse I | Klasse II | |
| **Beschreibung** | | | |
| Produkte mit digitalen Elementen, die keiner höheren Kategorie zugeordnet sind. Ein Großteil der betroffenen Produkte wird in diese Kategorie fallen. | Produkte mit digitalen Elementen, die in erster Linie Funktionen, die für die Cybersicherheit anderer Produkte, Netze oder Dienste von entscheidender Bedeutung sind. Weiters bergen diese Produkte ein erhebliches Risiko nachteiliger Auswirkungen, wie bspw. fehlende Verfügbarkeit, Gesundheitsverfall, Datenschutz usw. | | Anhang IV listet kritische Produkte mit digitalen Elementen auf, wie bspw. Hardwaregeräte mit Sicherheitsboxen (TPM), Smart-Meter-Gateways etc. |
| **Konformitäts-bewertung** | | | |
| Internes Kontrollverfahren (Modul A) | | | |
| | EU-Baumusterprüfung + interne Fertigungskontrolle (Modul B + C) | | Modul B + C |
| | Umfassende Qualitätssicherung (Modul H) | | Modul H |
| | Europäisches Schema für die Cybersicherheitszertifizierung | | |

Primär Sekundär

# CRA | Empfohlene Vorgehensweise

Mithilfe unserer erpropten Vorgehensweise basierend auf dem Deloitte Cyber Strategy Framework lassen sich die Anforderungen strukturiert bearbeiten.


## Analyse der Betroffenheit

- Klärung einer mögl. Betroffenheit als Hersteller, Importeur oder Händler im Sinne des CRA

## Definition des SOLL-Zustands

- Welche Anforderungen muss ein Hersteller, Importeur oder Händler erfüllen?
- Ableitung des Soll-Zustands von den CRA-Anforderungen unter Beachtung von Best Practices und des Stands der Technik

## Erfassung des IST-Zustands

- Erfassung und Dokumentation der aktuellen Maßnahmen bzw. des Status Quos basierend auf den CRA-Anforderungen

## Gap-Analyse & Definition von Maßnahmen

- Identifizierung von Gaps zwischen dem Soll- und Ist-Zustand inkl. Ableitung von entsprechenden Maßnahmen zur Umsetzung

Umsetzung der Maßnahmen!

# CRA | Diskussion und Fragen