CRA Pre-Assessment

Cyber Resilience Act – Schnell-Check Ihrer Betroffenheit

Beantworten Sie die Fragen mit Ja / Nein / Unbekannt. Die vorläufige CRA-Auswertung wird unten automatisch erstellt. Diese Selbsteinschätzung basiert auf der Verordnung (EU) 2024/2847 und ersetzt weder ein Audit noch eine rechtliche Prüfung.

Fragebogen

Nr.	Frage	Antwort
	Abschnitt A | Produkt & Marktzugang	
A1	Bietet Ihr Unternehmen Software, Hardware oder Geräte an, die sich mit anderen Geräten, Systemen oder Netzwerken verbinden können?	
A2	Werden diese Produkte am EU-Markt, außerhalb einer Gruppe, angeboten, verkauft, lizenziert oder zum Download bereitgestellt?	
A3	Werden diese Produkte oder die Produktlizenzen nur eigenen Gruppengesellschaften zur Verfügung gestellt?	
A4	Gibt es Hinweise, dass für diese Produkte Spezialregeln gelten, z. B. Medizinprodukte, Fahrzeuge, Luftfahrt oder Verteidigung?	
A5	Braucht diese Produkte für wesentliche Funktionen eine Cloud, ein Server-Backend, eine API oder einen Fernzugriff Ihres Unternehmens?	
A6	Werden diese Produkte auch nach dem 11.12.2027 noch angeboten, verkauft oder wesentlich verändert durch z.B. neue Funktionen oder sicherheitsrelevante Updates?	
	Abschnitt B | Ihre Rolle im Produktlebenszyklus	
B1	Entwickelt oder vermarktet Ihr Unternehmen diese Produkte unter eigenem Namen und/oder eigener Marke?	
B2	Stellen Sie Produkte anderer Hersteller unverändert und untere deren Namen/Marke bereit?	
B3	Wurden diese Produkte durch Ihre Einheit wesentlich verändert oder in eine eigene Lösung integriert, sodass sich Zweck, Funktionen oder Sicherheit wesentlich ändern?	
	Abschnitt C | Ausgangslage für eine CRA-Readiness	
C1	Gibt es in Ihrem Unternehmen eine schriftliche Richtlinie zur Produktsicherheit sowie eine klar zuständige Person oder Rolle dafür?	
C2	Wird für Ihre Produkte regelmäßig geprüft und dokumentiert, welche Cyber-Risiken bestehen?	
C3	Werden Ihre Produkte mit sicheren Voreinstellungen ausgeliefert?	
C4	Gibt es einen bekannten Kontaktweg, über den Schwachstellen gemeldet werden können?	
C5	Können Sie Sicherheitsupdates für diese Produkte erstellen, testen und an Nutzer:innen bereitgestellen?	
C6	Gibt es eine Übersicht der eingesetzten Software-, Open-Source- und Drittkomponenten (Software Bill of Materials, SBOM)?	
C7	Ist für jedes Produkt festgelegt und gegenüber Nutzer:innen kommuniziert, wie lange es Sicherheitsupdates bekommt?	
C8	Gibt es bereits Dokumentation zum Produkt, z. B. Architektur, Produktbeschreibung, Risikoanalyse oder Betriebsdokumentation?	

Ihr Ergebnis

CRA-Betroffenheit	Rolle(n)-Hinweis	Aufwands- und Risikoindikator
- (Bitte Abschnitt A vollständig ausfüllen)	- (bitte Abschnitt B ausfüllen)	- (bitte Abschnitt C vollständig beantworten)

Bei möglicher CRA-Betroffenheit: Was kommt in der Umsetzung auf Sie zu?

Der CRA verlangt mehr als eine einmalige Konformitätsbewertung – u. a. fortlaufende Vulnerability-Handling-Prozesse, technische Dokumentation, definierte Supportzeiträume, Nutzerinformationen, Sicherheitsupdates sowie ggf. Marktüberwachungskooperation. Die Umsetzung umfasst typischerweise fünf Reifedomänen:

1. Governance & Dokumentation	Produktsicherheits-Policies, Rollen und Verantwortlichkeiten, technische Dokumentation je Produkt, regelmäßige Reviews, Zusammenarbeit mit Marktüberwachungsbehörden.
2. Risikomanagement, Security-by-Design & Security-by-Default	Systematische Cyber-Risikobewertungen mit Zweckbestimmung, Betriebsumgebung und Nutzungsdauer, sichere Entwicklung, sichere Voreinstellungen, Security-Tests.
3. Schwachstellen- & Patch-Management	Empfang und Bearbeitung von Schwachstellenmeldungen, koordinierte Offenlegung, Bereitstellung von Security-Updates, Software Bill of Materials (SBOM), risikobasierte Priorisierung, Meldepflichten (24 h Frühwarnung / 72 h Meldung nach Art 14 CRA).
4. Produktlebenszyklus-Management	Begründete Supportzeiträume (mind. 5 Jahre), End-of-Life-Kommunikation, strukturierte Behebung von Sicherheitsproblemen, Monitoring im Betrieb, Lessons Learned.
5. Awareness, Kompetenz & Skills	Ausreichende Kompetenzen für sichere Produktentwicklung, Trainings, Kultur der offenen Meldung, Nutzung externer Expertise, Anbindung an ISMS/QMS und Kompetenz-Reviews.

Verstöße gegen CRA-Pflichten können mit Bußgeldern von bis zu 15 Mio. € bzw. 2,5 % des weltweiten Jahresumsatzes geahndet werden.

Sie möchten das Thema mit EY vertiefen?

Bitte nehmen Sie mit uns Kontakt auf Roman Tobler Senior Manager - roman.tobler@at.ey.com

Hinweis: Diese Selbsteinschätzung ersetzt keine individuelle rechtliche Prüfung. Eine belastbare CRA-Einordnung erfordert eine vertiefte Analyse der Produkte, der Rolle des Unternehmens, des Marktzugangs, möglicher Ausnahmen sowie der relevanten CRA-Pflichten. Die konkrete Ableitung von Pflichten und Konformitätsanforderungen erfolgt erst im Rahmen einer weiterführenden Produkt- und Rollenanalyse.