Cyber Resilience Act(CRA)

Checkliste

1. Produktklassifizierung

- ☐ Alle Produkte mit digitalen Elementen sind erfasst
- ☐ Produkte sind nach CRA-Risikoklassen klassifiziert (Standard / Klasse 1 / Klasse 2 / kritisch)
- ☐ Klassifizierung ist dokumentiert und nachvollziehbar begründet
- ☐ Verantwortlichkeiten für Klassifizierung sind definiert
- ☐ Regelprozess zur Aktualisierung der Klassifizierung ist etabliert

2. Technische Umsetzung im Engineering

- ☐ Security-by-Design ist im Entwicklungsprozess verankert
- ☐ Sicherheitsanforderungen sind Teil der Architekturphase
- ☐ Mechanismen für sichere Updates und Patches sind implementiert
- ☐ Abhängigkeiten (Third-Party Components) sind dokumentiert
- ☐ Vulnerability Management Prozess ist definiert und aktiv
- ☐ Sicherheitsrisiken werden kontinuierlich bewertet
- ☐ Secure Development Guidelines sind etabliert

3. Compliance & Dokumentation

- ☐ Technische Dokumentation ist CRA-konform aufgebaut
- ☐ Produktdokumentation ist vollständig und aktuell
- ☐ Sicherheitsanforderungen sind nachvollziehbar dokumentiert
- ☐ Interne Compliance-Prozesse sind definiert
- ☐ Audit- und Nachweispflichten sind berücksichtigt
- ☐ Schnittstelle zwischen Engineering und Compliance ist definiert
- ☐ Verantwortlichkeiten für regulatorische Updates sind festgelegt

Cyber Resilience Act(CRA)

Checkliste

4. Meldepflicht & Incident Management

- ☐ Prozess zur Erkennung aktiver Schwachstellen ist etabliert
- ☐ Definition „schwerwiegender Sicherheitsvorfall" ist intern geregelt
- ☐ Eskalationsprozess ist definiert (Engineering → Security → Compliance)
- ☐ Meldefristen gemäss CRA sind implementiert
- ☐ Kommunikationswege zu Behörden sind vorbereitet
- ☐ Incident Response Team ist definiert und geschult
- ☐ Meldeprozess wurde getestet

5. Lagerprodukte & Ersatzteile

- ☐ Lagerprodukte sind auf CRA-Konformität geprüft
- ☐ Prozesse für Re-Validierung von Bestandsware sind definiert
- ☐ Ersatzteile sind klassifiziert (identisch / funktional / neu)
- ☐ Regeln für Ersatzteilbewertung sind dokumentiert
- ☐ Lieferantenanforderungen sind CRA-konform angepasst
- ☐ Lebenszyklusstrategie berücksichtigt CRA-Anforderungen

6. Organisation & Governance

- ☐ Interdisziplinäres CRA-Ownership ist definiert
- ☐ Zusammenarbeit zwischen Engineering, Security und Compliance ist etabliert
- ☐ Schulungen zum CRA sind durchgeführt
- ☐ Regelmässige Reviews und Updates sind geplant
- ☐ Management ist über Risiken und Fristen informiert
- ☐ CRA-Roadmap ist erstellt