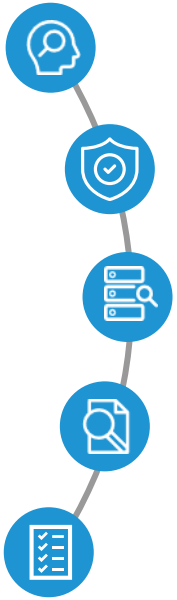
Cyber Resilience Act (CRA) / Security Step by Step

Ihr Weg zum Sicheren Produkt

… where ideas turn into success!

CRA & Security Step by Step

Anforderungen des EU Cyber Resilience Act (CRA) für Sensorhersteller



1. **Analyse & Vorbereitung**
2. **Entwicklung & Design**
3. **Update- & Schwachstellenmanagement**
4. **Dokumentation & CE-Kennzeichnung**
5. **Organisation & Schulung**

5 Schritte als Grundlage für Ihre CRA-Roadmap mit Entwicklungs-Unterstützung durch MESCO

Cyber Resilience Act (CRA)

Schritt für Schritt

Schritt 1: Analyse & Vorbereitung

- Alle Produkte mit digitalen Elementen identifizieren (Sensoren mit Firmware, Kommunikationsschnittstellen, IoT-Anbindung).
- Software-Stückliste (SBOM) erstellen: jede verwendete Softwarekomponente dokumentieren
- Risikoanalyse starten: Welche Angriffsflächen haben die Produkte (z. B. Funkmodule, Netzwerk-Ports, APIs)?
- Verantwortliche Person/Team für Cybersecurity & Compliance benennen.

Cyber Resilience Act (CRA)

Schritt für Schritt

Schritt 2: Entwicklung & Design

- Secure Development Lifecycle (SDLC) einführen / Sicherheitsanforderungen bei Design & Architektur
- Bedrohungsmodellierung (Threat Modeling) für das neue Produkt
- Code-Reviews & Automatisierte Sicherheitsscans einführen
- Sicherheitsfunktionen „by default“ aktivieren (z. B. verschlüsselte Kommunikation, sichere Authentifizierung)

Cyber Resilience Act (CRA)

Schritt für Schritt

Schritt 3: Update- & Schwachstellenmanagement

- Mechanismen für Sichere Updates (Firmware oder OTA) implementieren.
- Definieren: Wie lange werden Updates garantiert? (Erwartbare Nutzungsdauer)
- Meldeprozess für Schwachstellen einrichten (interne + externe Meldung an ENISA/Behörden).
- Prozesse dokumentieren (wer, wann, wie wird reagiert)

Cyber Resilience Act (CRA)

Schritt für Schritt

Schritt 4: Dokumentation & CE-Kennzeichnung

- Technische Unterlagen erstellen (Risikoanalyse, Sicherheitsarchitektur, Update-Strategie, Schwachstellenmanagement, Benutzerhinweise).
- Konformitätserklärung vorbereiten.
- CE-Kennzeichnung erweitern: künftig ist CRA ein Teil der Konformitätsprüfung

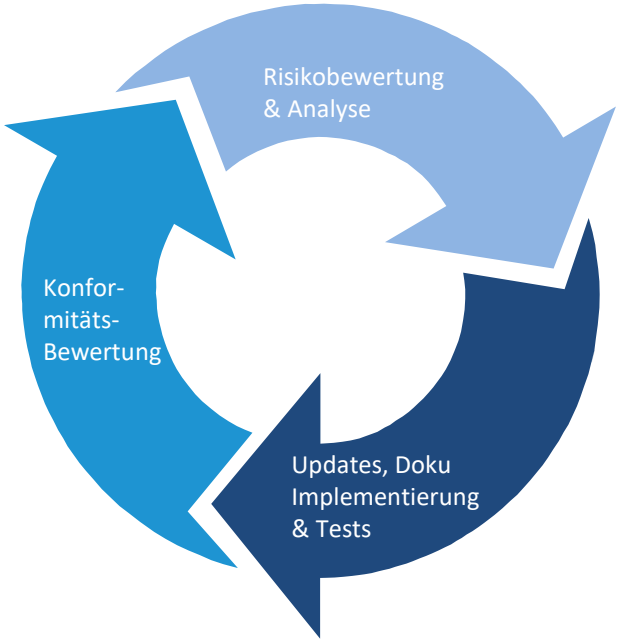
Cyber Resilience Act (CRA)

Schritt für Schritt

Schritt 5: Organisation & Schulung

- Mitarbeitende (Entwicklung, Service, Support) zu CRA-Anforderungen schulen
- Lieferkette sicherstellen: Zulieferer liefern CRA-konforme Komponenten
- Internes Audit-System aufbauen (regelmäßige Überprüfung der Sicherheitsprozesse)
- Notfallpläne für Cybersecurity-Incidents erarbeiten (Incident Response Plan)

MESCO Dienstleistungen



- Auswahl des geeigneten Konformitäts-bewertungsverfahrens
- Durchführung von Risikobewertungen und Minimierung der Angriffsflächen
- Integration von Schutzmechanismen
- Entwicklung von (cyber-)sicherer Feldbus-Kommunikation
- Identifikation und Behandlung von Schwachstellen
- **HW/SW Entwicklung von Sicheren Automatisierungskomponenten**
- Erstellung einer Software Bill of Materials (SBOM)
- Support CRA Certification

Cyber Resilience Act (CRA)

Zeitplan

Aktueller Stand und Fristen

- 2024 CRA veröffentlicht in EU-Amtsblatt
- 06/2026 Konformitätsbewertung durch Externe wie z.B. TÜV Süd möglich
- 09/2026: Schwachstellenmeldungen und Sicherheitsvorfallmeldungen sind verpflichtend
- **11.12.2027: Alle neu in Verkehr gebrachten Produkte müssen CRA-konform sein** (Übergangsfrist endet).

Quellen:
BSI - Technische Richtlinie BSI TR-03183 - BSI TR-03183 Cyber-Resilienz-Anforderungen

Kontaktieren Sie Uns

MESCO Engineering GmbH

Berner Weg 7
79539 Lörrach
Germany
+49 7621 1575 440

Sales@mesco-engineering.com

https://mesco-engineering.com/

MESCO Engineering, Inc.

2125 Center Avenue, Suite 507
Fort Lee, New Jersey 07024
USA
Tel. +1 201 302 6002

info@mesco.us

MESCO Engineering GmbH

Wentzingerstraße 23
79106 Freiburg
Germany
Tel. +49 7621 1575 0
Fax +49 7621 1575 175

info@mesco.de

MESCO Engineering AG

Klosterzelgstrasse 1a
5210 Windisch
Switzerland
Tel. +41 56 560 37 00
Fax +41 61 641 67 28

info@mesco.ch