Kurzstudie

Cyber Resilience Act (CRA)

ALLIANZ Industrie 4.0 BADEN-WÜRTTEMBERG

Praxisorientierte Einordnung, typische Umsetzungsherausforderungen und priorisierte Handlungsempfehlungen für den industriellen Mittelstand in Baden-Württemberg

Kompletter Name der Verordnung:

VERORDNUNG (EU) 2024/2847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), abrufbar unter:
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402847

Hinweis:

Die Unterlage ist bewusst managementtauglich formuliert und ersetzt keine Rechtsberatung. Maßgeblich bleiben der Verordnungstext, spätere Guidance sowie einschlägige Standards und Konformitätsverfahren.

Inhalt

Abkürzungsverzeichnis 4
Management Summary 6
1. Zielsetzung und Einordnung 7
2. Was unter den CRA fällt – und was nicht 8
3. Rollen entlang der Wertschöpfungskette 9
4. Produktkategorien und Konformitätsbewertung 10
5. Zentrale Herstellerpflichten über den Produktlebenszyklus 11
6. Übergangsregeln, Bestandsprodukte und Zeitplanung 12
7. Sorgfaltspflichten bei Drittkomponenten 14
8. SBOM, Dokumentation und Vulnerability Handling in der Praxis 15
9. Typische Herausforderungen im industriellen Mittelstand 16
10. Priorisierte Handlungsempfehlungen 18
10.1 Must-haves 18
10.2 Nice-to-haves 21
11. Beispielhafte Unternehmenssituationen 22
12. Vertiefende Materialien und aktuelle Entwicklungen 24
13. Fazit 24
14. Quellenverzeichnis 26
15. Verfasser der Studie 29
16. Impressum 30
Anlagen 31
A. Umsetzungsleitfaden für Produktverantwortliche und Umsetzungsteams 31
B. CRA-Leitfaden für die Leitungsebene 43

Abkürzungsverzeichnis

Die folgenden Abkürzungen werden im Dokument verwendet. Die Erläuterungen sind bewusst knapp und managementtauglich formuliert.

Abkürzung	Langform	Kurzerläuterung
BSI	Bundesamt für Sicherheit in der Informationstechnik	Cybersicherheitsbehörde des Bundes; im CRA-Kontext in Deutschland zudem zuständig als nationale Marktaufsichtsbehörde; veröffentlicht unter anderem Managementhinweise und technische Richtlinien zum CRA.
BSI-TR	Technische Richtlinie des BSI	Vom BSI veröffentlichte technische Richtlinie; im CRA-Kontext insbesondere relevant für allgemeine Anforderungen, SBOM und Schwachstellenmeldungen.
CE	Conformité Européenne	Kennzeichnung, mit der Hersteller die Konformität ihres Produkts mit den einschlägigen EU-Anforderungen erklären.
CRA	Cyber Resilience Act	EU-Verordnung zu horizontalen Cybersicherheitsanforderungen für Produkte mit digitalen Elementen.
CSAF	Common Security Advisory Framework	Standardisiertes Format zur strukturierten Veröffentlichung von Security Advisories.
CVD	Coordinated Vulnerability Disclosure	Koordinierter Prozess für die Annahme, Bewertung und Offenlegung von Schwachstellenmeldungen.
ENISA	European Network and Information Security Agency	Als zentrales europäisches IT-Sicherheitsinstitut fungiert die ENISA als offizielle Meldestelle für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle digitaler Produkte.
EU	Europäische Union	Politisch-rechtlicher Rahmen, in dem der CRA gilt.
EU-FAQ	Frequently Asked Questions der Europäischen Kommission	Vorläufige Auslegungshilfe der Kommissionsdienststellen zum CRA; wichtig für Scope-, Übergangs- und Praxisfragen. Das Dokument hat jedoch keinen Rechtscharakter.
FAQ	Frequently Asked Questions	Sammlung häufig gestellter Fragen mit kompakten Antworten.
FOSS	Free and Open Source Software	Freie und quelloffene Software; bestimmte nicht-kommerzielle FOSS-Konstellationen sind vom CRA ausgenommen.

Abkürzung	Langform	Kurzerläuterung
IAO	Institut für Arbeitswirtschaft und Organisation	Hier bezogen auf das Fraunhofer IAO als Mitautor der OT-Security-Studie.
IT	Informationstechnologie	Klassische Informations- und Unternehmens-IT, etwa Systeme für Datenverarbeitung, Kommunikation und Administration.
KMU	Kleine und mittlere Unternehmen	Zentrale Zielgruppe der Unterlagen im industriellen Mittelstand.
OEM	Original Equipment Manufacturer	Hersteller bzw. Zulieferer von Komponenten oder Produkten, die in Lösungen anderer Anbieter integriert oder unter anderer Marke vermarktet werden.
OT	Operational Technology	Betriebsnahe Steuerungs-, Produktions- und Automatisierungstechnik in industriellen Umgebungen.
SBOM	Software Bill of Materials	Maschinenlesbare Software-Stückliste mit Informationen zu enthaltenen Komponenten und Abhängigkeiten.
SME	Small and Medium-sized Enterprises	Englischer Begriff für kleine und mittlere Unternehmen; entspricht inhaltlich KMU.
TR	Technische Richtlinie	Technisches Richtliniendokument mit Konkretisierungen, Prüflogiken und Umsetzungshinweisen.
VEX	Vulnerability Exploitability Exchange	Format zur Aussage, ob und in welchem Umfang eine bekannte Schwachstelle ein konkretes Produkt tatsächlich betrifft.

Management Summary

Worum es für das Management jetzt geht

Der CRA ist kein isoliertes Compliance-Thema, sondern betrifft ein Produkt-, Entwicklungs-, Support- und Lieferkettenthema. Für viele Industrieunternehmen ist nicht die Detailfrage einzelner Normen die erste Hürde, sondern Transparenz: Welche Produkte fallen überhaupt in den Anwendungsbereich, welche Marktrolle nimmt das Unternehmen je Produkt ein, welche Drittkomponenten sind sicherheitsrelevant und welche Prozesse müssen bis zu den gestaffelten Fristen, wie September 2026 beziehungsweise Dezember 2027, belastbar stehen.

Die wichtigsten Erkenntnisse für Geschäftsführung und Bereichsleitungen sind:

- Seit 10. Dezember 2024 ist der CRA in Kraft. Ab 11. September 2026 gelten Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle. Praktisch heißt das: Frühwarnung grundsätzlich „unverzüglich", spätestens binnen 24 Stunden, Folgemeldung spätestens binnen 72 Stunden; Abschlussbericht bei aktiv ausgenutzten Schwachstellen spätestens binnen 14 Tagen nach Verfügbarkeit einer Korrektur- oder Minderungsmaßnahme, bei schwerwiegenden Sicherheitsvorfällen binnen eines Monats.
- Die übrigen Hauptpflichten gelten ab 11. Dezember 2027 für Produkte mit digitalen Elementen, die ab diesem Datum neu auf dem EU-Markt bereitgestellt werden. Produkte, die bereits vor diesem Datum in Verkehr gebracht wurden, fallen grundsätzlich erst dann in die allgemeine CRA-Konformitätslogik, wenn sie nach dem 11. Dezember 2027 wesentlich geändert werden. [Q01, Q04, Q05, Q19, Q21]
- Im Zentrum des CRA stehen vor allem Hersteller von Produkten mit digitalen Elementen; je nach Marktrolle betreffen einzelne Pflichten aber auch Importeure und Händler. Für den industriellen Mittelstand relevant sind damit insbesondere Anbieter vernetzter Maschinen, Embedded-Software, industrieller Komponenten und Stand-alone-Software. [Q19, Q21]
- Betroffen sein können nicht nur klassische vernetzte Geräte, sondern auch Stand-alone-Software, Firmware, separat vermarktete Komponenten und unter Umständen Remote Data Processing Solutions, wenn deren Wegfall Produktfunktionen verhindern würde. [Q02, Q03, Q04, Q19]
- Für den industriellen Mittelstand ist die größte operative Herausforderung meist nicht ein einzelner Nachweis, sondern das Zusammenspiel aus Scope-Klärung, Rollenklärung, risikobasierter Entwicklung, SBOM, Due Diligence für Drittkomponenten, Vulnerability Handling und technischer Dokumentation. [Q06, Q09, Q11, Q16]

Empfohlene Management-Agenda für die nächsten Monate:

Zeithorizont	Priorität	Management-Fokus
sofort	Hoch	Produktinventur, Rollenklärung und Verantwortlichkeiten je Produktfamilie aufsetzen
bis Sommer 2026	Hoch	Meldewege, Security-Kontakte, CVD-Policy und internes Eskalationsmodell definieren
bis 11.09.2026	Hoch	Organisatorische Fähigkeit zur CRA-Meldung aktiv ausgenutzter Schwachstellen und schwerer Vorfälle sicherstellen
bis Ende 2026	Mittel-Hoch	SBOM-, Drittkomponenten- und Dokumentationslogik für priorisierte Produkte aufbauen
bis 11.12.2027	Hoch	Konformitäts- und Supportfähigkeit für neue beziehungsweise wesentlich geänderte Produkte belastbar nachweisen

Ein zentrales Gestaltungsprinzip dieser Kurzstudie lautet daher: erst Orientierung und Priorisierung, dann vertiefende Umsetzung.

1. Zielsetzung und Einordnung

Die Kurzstudie soll Unternehmen nicht mit regulatorischen Details überladen, sondern als Wegweiser dienen. Sie holt Unternehmen auf ihrem aktuellen Stand ab, erleichtert den Einstieg in das Thema und verweist an geeigneter Stelle auf vertiefende Materialien.

2. Was unter den CRA fällt – und was nicht

Nach der vorläufigen FAQ der Europäischen Kommission ist ein Produkt mit digitalen Elementen dann im Anwendungsbereich, wenn drei Kriterien kumulativ erfüllt sind: Es muss sich um ein Produkt mit digitalen Elementen handeln, es muss auf dem Markt bereitgestellt werden und sein bestimmungsgemäßer oder vernünftigerweise vorhersehbarer Gebrauch muss eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netzwerk umfassen. [Q02, Q03, Q19]

- Typisch im Scope sind Hardware mit Embedded Software, Stand-alone-Software, Firmware, industrielle IoT-Komponenten, Gateways, Steuerungen, Router, Sensorik mit Netzbezug und separat vermarktete digitale Komponenten.
- Mit zu prüfen sind Remote Data Processing Solutions, wenn deren Fehlen eine Produktfunktion verhindern würde.
- Nicht im Scope sind insbesondere bestimmte bereits anderweitig regulierte Produktgruppen, reine Eigenentwicklungen für den Eigengebrauch ohne Inverkehrbringen sowie FOSS-Konstellationen ohne kommerzielle Bereitstellung.
- Für KMU wichtig: Die Ausnahme für nicht-kommerzielle FOSS-Konstellationen bedeutet nicht, dass Open-Source-Komponenten in kommerziell bereitgestellten Produkten CRA-neutral wären. Wer FOSS-Bausteine in ein vermarktetes Produkt integriert, muss deren Risiken im Rahmen der eigenen Sorgfaltspflichten, SBOM und Schwachstellenbearbeitung berücksichtigen. [Q19]
- In industriellen Umgebungen liegt ein häufiger Fehler darin, nur die sichtbare Hauptmaschine zu betrachten. Es sollen jedoch verschiedene Elemente wie Treiber, Firmware, Engineering-Tools, Edge-Komponenten, Service-Software oder Fernwartungsanteile nicht systematisch betrachtet werden.

Praxisrückschluss für KMU
Der erste relevante Arbeitsschritt ist eine saubere Produktinventur. Ohne belastbare Liste der Produktfamilien, Versionen, Remote-Anteile und Drittkomponenten ist weder ein sinnvoller Self-Check noch eine priorisierte Umsetzungsplanung möglich. Ergänzend ist es entscheidend, die zugehörigen Entwicklungs-, Änderungs- und Betriebsprozesse zu kennen und nachvollziehbar zu dokumentieren, da diese die Grundlage für eine CRA-konforme Umsetzung bilden.

Gerade für den Maschinen- und Anlagenbau ist außerdem wichtig, zwischen Produkt, integrierten Komponenten und Betriebsumgebung zu unterscheiden.

3. Rollen entlang der Wertschöpfungskette

Für die Praxis entscheidend ist die Marktrolle je Produkt. In industriellen Lieferketten fällt technische Verantwortung nicht immer mit regulatorischer Verantwortung zusammen. Wer ein Produkt unter eigenem Namen oder eigener Marke auf dem EU-Markt bereitstellt, kann Herstellerpflichten tragen – auch dann, wenn wesentliche Bestandteile von Dritten stammen.

Rolle	**Typische Konstellation**	**Praktische Kernfrage**
Hersteller	Entwickelt oder lässt entwickeln und bringt unter eigenem Namen in Verkehr	Sind Risikoanalyse, technische Dokumentation, Supportperiode und Konformitätsverfahren belastbar organisiert?
„Quasi-Hersteller"/Hersteller in OEM-/White-Label-Konstellationen	Integriert Fremdkomponenten oder vertreibt Lösungen unter eigener Marke	Welche Risiken aus Fremdkomponenten, Verträgen und Nachweispflichten müssen für das Gesamtprodukt beherrscht werden?
Importeur/ Einführer	Bringt außerhalb der EU hergestelltes Produkt auf den Unionsmarkt	Sind zentrale Herstellernachweise, Kennzeichnungen und Ansprechpartner plausibel vorhanden?
Händler	Stellt Produkt ohne wesentliche Änderung bereit	Wie wird mit erkennbarer Nichtkonformität, fehlenden Angaben oder Rückrufen umgegangen?

Aus Sicht des höheren Managements ist die Rollenklärung ein Steuerungsthema: Ohne eindeutige Verantwortlichkeit je Produktfamilie bleiben Prioritäten, Budgets und Eskalationen diffus. Daher wären folgende Management-Fragen relevant: Wer verantwortet Scope, wer Dokumentation, wer Security-Entscheidungen, wer Lieferantenkommunikation und wer meldet kritische Schwachstellen oder Vorfälle?

4. Produktkategorien und Konformitäts-bewertung

Nicht jedes Produkt folgt derselben Konformitätslogik. Der CRA unterscheidet Standardprodukte sowie wichtige und kritische Produkte. Ende 2025 hat die Kommission die technischen Beschreibungen der Kategorien durch die Durchführungsverordnung (EU) 2025/2392 konkretisiert. Für Unternehmen ist das relevant, weil sich daraus unterschiedliche Wege der Konformitätsbewertung ergeben. [Q01, Q06, Q07, Q19]

Kategorie	Einordnung	Typische Konsequenz
Standard-produkt	Alle betroffenen Produkte, die nicht als wichtiges oder kritisches Produkt eingestuft sind	Interne Kontrolle/Selbstbewertung grundsätzlich möglich
Wichtiges Produkt Klasse I	Produkte mit in Anhang III beschriebenen Kernfunktionen, z. B. bestimmte Sicherheits- und Netzkomponenten	Je nach Normenlage Selbstbewertung mit Konformitätsvermutung oder notifizierte Stelle
Wichtiges Produkt Klasse II	Risikoreichere Kategorien wie bestimmte Firewalls, IDS/IPS, Hypervisoren	Keine reine Selbstbewertung; stärkere Rolle externer Konformitätsbewertung
Kritisches Produkt	Produkte mit besonders sensibler Kernfunktion, z. B. Secure Elements oder Smart-Meter-Gateways	Zertifizierungs- beziehungsweise strengere Bewertungslogik

Wichtig ist die Kerngedanken-Logik der FAQ: Die Integration einer wichtigen oder kritischen Komponente macht das Gesamtprodukt nicht automatisch selbst wichtig oder kritisch. Maßgeblich ist die Kernfunktion der vermarkteten Gesamtlösung.
Für typische Mittelstandsprodukte lässt sich daraus grob ableiten: Viele vernetzte Maschinenkomponenten, HMI- oder Engineering-Software fallen zunächst in die Standardkategorie, sofern ihre Kernfunktion nicht ausdrücklich gelistet ist. Wichtige Produkte können etwa Router, Betriebssysteme, Netzmanagementsysteme oder Passwortmanager sein; wichtige Produkte Klasse II insbesondere Firewalls, IDS/IPS oder Hypervisoren. Kritische Produkte sind deutlich enger gefasst, etwa Secure Elements, Smartcards oder Smart-Meter-Gateways. Maßgeblich bleibt jeweils die Kernfunktion des vermarkteten Produkts. [Q19]

Aktueller Entwicklungsstand

Die Kommission skizziert auf ihrer CRA-Implementierungsseite weitere Umsetzungsschritte, darunter erste Standardisierungsdeliverables ab Q3 2026, die Anwendung der Meldepflichten ab 11. September 2026 sowie die volle Anwendung des CRA ab 11. Dezember 2027. Für Unternehmen heißt das: Die Vorbereitungsphase läuft bereits, auch wenn nicht alle Details final ausstandardisiert sind.

5. Zentrale Herstellerpflichten über den Produktlebenszyklus

Die Pflichten des CRA greifen über den gesamten Produktlebenszyklus. Für industrielle Unternehmen empfiehlt sich eine Gliederung in sechs operative Pflichtbereiche, die auch für die Management Summary gut verdichtet werden können.

Pflichtbereich	Worum es geht	Warum es in der Praxis schwierig wird
Risikobasierter Ansatz	Cybersecurity-Risiken systematisch ermitteln, bewerten und behandeln	Methodik, Verantwortlichkeiten und Aktualisierung fehlen oft produktbezogen
Sichere Entwicklung und sichere Voreinstellungen	Sicherheitsanforderungen früh in Entwicklung und Voreinstellungen verankern	Legacy-Produkte, Variantenvielfalt und Zeitdruck im Engineering
Technische Dokumentation	Nachweise zu Produkt, Architektur, Risiko, Tests, Nutzerinformationen und Updates vorhalten	Unterlagen liegen verstreut; Dokumentation ist nicht auf Nachweisfähigkeit ausgelegt
SBOM und Drittkomponenten	Komponenten transparent machen und Due Diligence für Zulieferer umsetzen	Tooling, Datenqualität und Lieferantentransparenz sind oft unzureichend
Schwachstellenmanagement	Schwachstellen empfangen, bewerten, beheben, kommunizieren und melden	Es fehlen CVD-Policy, PSIRT-/CSIRT-Kontakte, Security Advisories und Eskalationswege
Support und Updates	Sicherheitsupdates über die Supportperiode bereitstellen	Lange Produktlebenszyklen, eingebettete Drittkomponenten und knappe Ressourcen

Die BSI-TR Teil 1 bis 3 liefern hierfür eine wichtige fachliche Orientierung, auch wenn sie den Verordnungstext nicht ersetzen.

- Teil 1 erklärt, wie Unternehmen Risiken systematisch bewerten.
- Teil 2 beschreibt, welche Informationen zu Software-Komponenten (SBOM) vorliegen sollten.
- Teil 3 zeigt, welche Prozesse für den Umgang mit Schwachstellen und Meldungen nötig sind.

Für KMU ist das vor allem als praktische Prüflogik relevant: Welche Informationen müssen vorliegen, welche Prozesse müssen etabliert sein und welche Nachweise sollten strukturiert verfügbar sein? Gerade bei Industrieprodukten mit zehn bis zwanzig Jahren Nutzungsdauer entsteht dabei ein Zielkonflikt zwischen Kundenerwartung, Supportzusagen von Zulieferern und interner Patchfähigkeit. Zugleich bleibt maßgeblich, dass Supportperiode, Risikobewertung und konkrete Umsetzung am CRA selbst sowie an künftiger Guidance und Normung gemessen werden. [Q20, Q21, Q22, Q23]
Art. 13 Abs. 8 und 9 CRA verlangen, dass die Supportperiode unter Berücksichtigung der Art des Produkts sowie der erwarteten Nutzungsdauer festgelegt wird. Sie beträgt grundsätzlich mindestens zehn Jahre, sofern die erwartete Nutzungsdauer nicht kürzer ist. Unternehmen müssen frühzeitig planen, wie sie Sicherheit über viele Jahre hinweg gewährleisten.

6. Übergangsregeln, Bestandsprodukte und Zeitplanung

Für viele Industrieunternehmen ist die Übergangslogik geschäftskritisch. Daher gelten folgende Fristen:

- **Der CRA gilt nicht pauschal rückwirkend für alle Bestandsprodukte:**
  - Produkte, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden, müssen nicht automatisch in die volle allgemeine CRA-Konformitätslogik überführt werden.
  - Allerdings gelten die Meldepflichten nach Art. 14 ab dem 11. September 2026 auch für Produkte, die bereits vor dem 11. Dezember 2027 auf dem Markt bereitgestellt wurden.
  - Vor dem 11. Dezember 2027 in Verkehr gebrachte Produkte bleiben grundsätzlich außerhalb der allgemeinen Hauptpflichten, solange sie nach diesem Datum nicht substantiell geändert werden.
  - Zugleich ist wichtig: Ab dem 11. Dezember 2027 neu auf den Markt gebrachte Einheiten müssen die CRA-Anforderungen erfüllen, auch wenn der Produkttyp bereits vor diesem Datum existierte. [Q01, Q03, Q04, Q19]

- Reine Sicherheitsupdates und Bugfixes gelten nicht automatisch als substantielle Änderung. Maßgeblich ist vielmehr, ob eine Änderung die ursprünglich vorgesehene Funktion oder das Risikoprofil des Produkts wesentlich verändert. Ein Update, das nur Fehler behebt, ist daher anders zu bewerten als ein Update, das neue Funktionen freischaltet oder den Einsatzzweck erweitert. [Q19, Q21]

- Ab 11. September 2026 müssen Unternehmen bei aktiv ausgenutzten Schwachstellen und schwerwiegende Sicherheitsvorfällen reagieren. Typisch sind:
  - **Erste Meldung bzw. Frühwarnung binnen 24 Stunden**
  - **Genauere Infos bzw. Folgemeldung binnen 72 Stunden**
  - **Abschlussbericht bei Schwachstellen binnen 14 Tagen** nach Verfügbarkeit einer Maßnahme, bei Sicherheitsvorfällen binnen eines Monats. [Q19, Q21]

- Neue Stückzahlen eines Produkttyps, die ab dem 11. Dezember 2027 erstmals auf dem EU-Markt bereitgestellt werden, dürfen nicht allein deshalb als unproblematisch betrachtet werden, weil der Produkttyp schon früher existierte. Maßgeblich ist das einzelne Inverkehrbringen bzw. Bereitstellen auf dem Markt, nicht nur das historische Entwicklungsdatum des Produkttyps.

- Für KMU ist deshalb eine Doppelstrategie sinnvoll: kurzfristig Meldefähigkeit und Krisenkommunikation herstellen, mittelfristig die produktbezogene Konformitätslogik für priorisierte neue oder wesentlich veränderte Produkte aufbauen.

Stichtag	Was relevant wird
11.06.2026	Anwendung der Vorschriften zur Benennung von Konformitätsbewertungsstellen
11.09.2026	Meldepflichten für aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle
Q3 2026	erste Standardisierungsdeliverables laut Kommission
11.12.2027	volle Anwendung des CRA auf Produkte mit digitalen Elementen, die ab diesem Datum neu auf dem EU-Markt bereitgestellt werden; Bestandsprodukte nur bei wesentlicher Änderung

Was bedeutet das für KMU konkret?

Unternehmen sollten zweigleisig vorgehen:

- Kurzfristig: In der Lage sein, Sicherheitsvorfälle zu erkennen und fristgerecht zu melden
- Mittelfristig: Produkte so entwickeln und dokumentieren, dass sie die CRA-Anforderungen erfüllen

Gerade gegenüber dem Management sollte diese Zeitlogik nicht als Entwarnung kommuniziert werden. Die Fristen verschieben nicht den Handlungsbedarf, sondern definieren, bis wann Mindestfähigkeiten belastbar vorhanden sein müssen.

7. Sorgfaltspflichten bei Drittkomponenten

Die Integration eingekaufter oder frei verfügbarer Komponenten gehört zu den größten praktischen Hebeln und Risiken. Die EU-FAQ macht deutlich, dass sich Hersteller nicht allein auf das Vorliegen einer CE-Kennzeichnung einzelner Komponenten verlassen können. Erforderlich ist eine angemessene Sorgfalt, damit integrierte Komponenten die Cybersicherheit des Gesamtprodukts nicht kompromittieren. Das gilt ausdrücklich auch für Open-Source-Komponenten, die selbst nicht im Anwendungsbereich des CRA liegen. [Q06, Q11, Q19]

Prüffeld	**Leitfrage für Einkauf, Entwicklung und Freigabe**
Updatehistorie	Erhält die Komponente regelmäßig Sicherheitsupdates und sind Release- oder Patchhinweise nachvollziehbar dokumentiert?
Schwachstellenlage	Sind relevante Schwachstellen, Hinweise zum Supportende (End of Life, EOL) oder bekannte Exploits bekannt?
SBOM/Transparenz	Liegen verlässliche Komponenteninformationen, Versionsdaten oder SBOMs vor?
Supportperiode	Passt der Supportzeitraum der Komponente zur erwarteten Nutzungsdauer des Gesamtprodukts?
Einsatzzweck	Entspricht die Nutzung im eigenen Produkt dem intendierten Nutzungskontext der Komponente?
Zusatztests	Sind zusätzliche technische Prüfungen wie Penetration Tests, Fuzzing oder Firmware-Analysen erforderlich?

Gerade im industriellen Mittelstand entsteht der Aufwand häufig nicht durch die einzelne Komponente, sondern durch die Beschaffung belastbarer Informationen: Versionsstände, Supportzusagen, bekannte Schwachstellen, SBOMs und Ansprechpartner müssen über eigene Teams, Zulieferer und gegebenenfalls OEM-Ketten hinweg zusammengeführt werden.

8. SBOM, Dokumentation und Vulnerability Handling in der Praxis

Das Thema SBOM sollte in den Unterlagen weder über- noch unterschätzt werden. Eine SBOM ist keine bloße Bestandteilliste, sondern sie hilft, den Überblick über eingesetzte Software zu behalten, Schwachstellen schneller zu erkennen und Updates gezielt zu steuern.
Gleichzeitig muss der Aufwand realistisch betrachtet werden: Eine SBOM allein macht ein Unternehmen noch nicht bereit für CRA und ihre Aussagekraft hängt stark davon ab, ob Komponenten-, Versions- und Lieferanteninformationen überhaupt verlässlich verfügbar sind. [Q09, Q11, Q22]

- Nach der BSI-TR muss eine SBOM maschinenverarbeitbar sein und bestimmte Mindestinformationen enthalten, etwa Angaben zu Ersteller, Komponentenname, Version, Dateiname, Abhängigkeiten, Lizenzinformationen und Hash-Werten. [Q22]
- Informationen zu Schwachstellen gehören nicht in die SBOM selbst, sondern in getrennte Advisories beziehungsweise VEX- oder CSAF-nahe Formate. [Q22]
- Für die Praxis ist das Schlagwort SBOM weniger entscheidend als die Prozessfrage:
  - Wer erzeugt sie,
  - wann wird sie aktualisiert,
  - wie werden Varianten behandelt und
  - wie werden Lieferanteninformationen integriert.

Die Kernherausforderung ist dabei oft, die erforderlichen Informationen überhaupt belastbar und aktuell zu erhalten. [Q22]

Ähnlich verhält es sich beim Schwachstellenmanagement. Teil 3 der BSI-TR macht deutlich, dass eine Sicherheitskontaktseite, eine Security.txt, funktionale Kontaktwege, eine CVD-Policy und veröffentlichbare Sicherheitshinweise zentrale Bausteine eines belastbaren Melde- und Reaktionsprozesses sind. Sie machen Ansprechpartner, Meldewege, Reaktionszeiten und den vorgesehenen Ablauf für externe Meldende und Marktakteure transparent. [Q09, Q20, Q23]

Mindestbaustein	Nutzen im CRA-Kontext
Security-Kontaktseite	macht Ansprechpartner und Meldewege auffindbar
Security.txt	ermöglicht standardisierte maschinelle Auffindbarkeit von Security-Kontakten
CVD-Policy	beschreibt Ablauf, Verantwortlichkeiten und Reaktionszeiten für Schwachstellenmeldungen
PSIRT-/CSIRT-Verantwortung	schafft interne Zuständigkeit für Annahme, Bewertung und Eskalation
Sicherheitshinweise	unterstützen Nutzerkommunikation und Nachweis der Behebung

Dieser operative Blick ist gerade für das Management wichtig: Die Frage lautet nicht nur, ob ein Unternehmen technisch patchen kann, sondern ob es organisatorisch in der Lage ist:

- Schwachstellen entgegenzunehmen,
- zu priorisieren,
- zu beheben,
- zu dokumentieren,
- zu kommunizieren und
- gegebenenfalls fristgerecht zu melden.

Dazu gehören in der Praxis vor allem auch eine zentrale Kontaktmöglichkeit für Sicherheitsmeldungen.

9. Typische Herausforderungen im industriellen Mittelstand

Die Besonderheiten des industriellen Mittelstands ähneln in Teilen den Mustern, die auch in der OT-Security-Studie der Allianz Industrie 4.0 hervorgehoben werden. Entscheidend ist die Kombination aus hoher Wertschöpfungstiefe, langlebigen Produkten, knappen Spezialressourcen und oft historisch gewachsenen Architekturen. [Q12, Q13, Q14, Q16, Q24, Q25]

- Legacy und Langlebigkeit: Produkte und Komponenten verbleiben oft viele Jahre im Feld; Support- und Updatefragen sind dadurch besonders anspruchsvoll.
- Lieferkettenabhängigkeiten: Eingekaufte Bibliotheken, OEM-Bausteine, Betriebssystemanteile oder Chipsätze bestimmen mit, ob Support- und Sicherheitszusagen realistisch sind.
- OT-/IT-Nähe: In industriellen Produkten wirken Cybersecurity-Risiken oft direkt auf Verfügbarkeit, Servicefähigkeit, Betriebssicherheit und Kundenvertrauen.
- Varianz der Ausgangslagen: Manche Unternehmen verfügen bereits über Entwicklungs- und Security-Prozesse; andere stehen noch vor der grundlegenden Produktinventur.
- Begrenzte personelle Ressourcen: Gerade kleinere Unternehmen brauchen handhabbare Einstiegspunkte statt sofortiger Vollständigkeitsansprüche.

Diese Realität erfordert keine Vollständigkeit von Beginn an, sondern eine realistische Staffelung: zunächst Mindestvoraussetzungen schaffen, danach systematisch vertiefen.

10. Priorisierte Handlungsempfehlungen

Aus den offiziellen EU- und BSI-Unterlagen sowie den verfügbaren Materialien und Arbeitsentwürfen ergibt sich für die Kurzstudie eine Priorisierungslogik in zwei Ebenen ([Q01, Q04, Q05, Q06, Q08, Q09, Q11, Q16]):

- Must-haves, also Themen, die man auf jeden Fall angehen muss, und
- Nice-to-haves, also Themen, die empfehlenswert sind.

10.1 Must-haves

Volle CRA-Konformität ist das Ziel bis Dezember 2027, aber nicht der erste Schritt. Der erste Schritt ist einfacher: wissen, welche Produkte betroffen sind, und die wichtigsten Grundlagen rechtzeitig legen. Besonders wichtig: **Ab dem 11. September 2026** müssen Hersteller Sicherheitslücken aktiv melden – auch für Produkte, die schon länger auf dem Markt sind. Wer bis dahin keinen funktionierenden Meldeprozess hat, verstößt gegen die Verordnung. Das ist der härteste Zwischenstichtag und bestimmt, was zuerst zu tun ist.
Die sieben Punkte folgen dieser Logik: erst Orientierung und Handlungsfähigkeit, dann schrittweise Vertiefung. Im Folgenden sind die Schritte ausführlicher beschrieben.

1. Bestandsaufnahme: Welche Produkte sind überhaupt betroffen?
Bevor irgendetwas anderes angegangen wird, braucht es Klarheit darüber, was das Unternehmen eigentlich auf den EU-Markt bringt und was davon unter den CRA fällt. Gemeint sind nicht nur die Hauptprodukte, sondern auch Softwareversionen, Firmware, Engineering-Tools und Fernwartungsfunktionen. In der Praxis werden beim ersten Durchgang regelmäßig Dinge übersehen: Serviceschnittstellen, separat verkaufte Softwaremodule, Remote-Zugänge. Wichtig ist auch, für Produkte, die eindeutig nicht betroffen sind, kurz zu notieren warum – eine unbegründete Nichtberücksichtigung ist im Zweifel schwerer zu erklären als eine dokumentierte Entscheidung.
Ergebnis: Eine strukturierte Liste aller relevanten Produkte mit erstem Hinweis, ob CRA-Pflichten greifen.

2. Rolle klären: Hersteller, „Quasi-Hersteller", Importeur/Einführer oder Händler?
Der CRA unterscheidet verschiedene Marktrollen und knüpft daran sehr unterschiedliche Pflichten. Wer ein Produkt unter eigenem Namen verkauft, trägt in der Regel die volle Herstellerverantwortung (Hersteller und Quasi-Hersteller), auch wenn Teile des Produkts von Dritten stammen. Das betrifft OEM-Konstellationen, White-Label-Produkte und Integrationsgeschäfte. Intern geht es darum, für jede Produktfamilie zu klären: Wer ist zuständig für die Dokumentation? Wer entscheidet über den Support-Zeitraum? Wer handelt, wenn eine Sicherheitslücke gemeldet wird? Ohne diese Klärung bleibt alles Weitere unverbindlich.
Ergebnis: Dokumentierte Marktrolle je Produktfamilie, benannte Ansprechpersonen für Produktmanagement, Entwicklung und Sicherheit.

3. Sicherheitsrisiken bewerten – für die wichtigsten Produkte zuerst

Der CRA verlangt, dass Sicherheitsrisiken systematisch bewertet und dokumentiert werden. Für viele Unternehmen ist das Neuland – nicht weil Risikobewertung unbekannt wäre, sondern weil sie produktbezogen und nachvollziehbar sein muss. Der richtige Einstieg ist kein vollständiges Framework für alle Produkte auf einmal. Es reicht ein belastbarer Mindestansatz für die wichtigsten Produktlinien: Wo kann jemand angreifen? Was wäre der Schaden? Was ist schon geschützt, was fehlt noch? Diese Bewertung ist nicht nur Pflichterfüllung, sie ist die Grundlage für alle weiteren technischen Entscheidungen.
Ergebnis: Dokumentierte Risikobewertung für priorisierte Produktlinien, Grundlage für technische Maßnahmen und Dokumentation.

4. Meldeprozess einrichten – bis spätestens September 2026

Ab dem 11. September 2026 gilt: Wer eine aktiv ausgenutzte Sicherheitslücke entdeckt oder einen schwerwiegenden Vorfall feststellt, muss das binnen 24 Stunden an die europäische Behörde ENISA melden. Binnen 72 Stunden folgt eine detailliertere Meldung, nach spätestens einem Monat ein Abschlussbericht. Diese Pflicht gilt auch für Produkte, die schon heute auf dem Markt sind. Das bedeutet: Lange vor der vollen Konformität braucht es eine funktionierende Grundstruktur. Konkret: eine öffentlich erreichbare Kontaktseite für Sicherheitsmeldungen, eine kurze schriftliche Beschreibung, wie das Unternehmen mit gemeldeten Lücken umgeht, und klare interne Zuständigkeiten, damit im Ernstfall niemand erst fragen muss, wer zuständig ist.
Ergebnis: Öffentlicher Security-Kontakt, schriftlicher Umgang mit Sicherheitsmeldungen, getesteter Meldeweg zu ENISA.

5. Komponentenliste (SBOM) für ein Produkt anlegen

Eine SBOM (kurz für „Software Bill of Materials“) ist eine strukturierte Liste aller Software-Bausteine, die in einem Produkt stecken: Bibliotheken, Abhängigkeiten, Versionen. Sie ist Pflicht nach CRA und gleichzeitig das Fundament für das spätere Schwachstellenmanagement. Der richtige Einstieg ist kein vollständiger Rollout über alle Produkte, sondern ein Pilot mit einem repräsentativen Produkt. Dieser Pilot zeigt, welches Werkzeug passt, wer die Liste aktuell hält und wo noch Informationen von Lieferanten fehlen. Diese Erkenntnisse sind die Grundlage für alles Weitere.
Ergebnis: SBOM für ein Referenzprodukt, dokumentierter Prozess zur Erstellung, identifizierte Lücken.

6. Festlegen, wie lange Sicherheitsupdates bereitgestellt werden

Der CRA verlangt, dass Hersteller Sicherheitsupdates über einen angemessenen Zeitraum bereitstellen, der sich an der erwarteten Nutzungsdauer des Produkts orientiert. Für Industrieprodukte, die zehn Jahre oder länger im Einsatz bleiben, ist das eine der schwierigsten Anforderungen. Die Antwort hängt auch davon ab, wie lange Drittthersteller ihre Komponenten unterstützen. Der erste Schritt ist keine perfekte Lösung dieser Langzeitfragen, sondern eine schriftlich fixierte, intern freigegebene Entscheidung: Wie lange gibt es Updates für welches Produkt? Was passiert, wenn eine verbaute Komponente vom Hersteller nicht mehr gepflegt wird?

Ergebnis: Schriftlich dokumentierter Support-Zeitraum und Update-Logik je Produktfamilie, abgestimmt mit Vertrieb und Produktmanagement.

7. Einheitliche Ablage für alle sicherheitsrelevanten Unterlagen

Der CRA schreibt vor, was zur technischen Dokumentation eines Produkts gehört: Produktbeschreibung, Risikoanalyse, Testergebnisse, Komponentenliste, Nutzerhinweise, Angaben zu Updates und Schwachstellenbehandlung. In vielen Unternehmen liegen diese Informationen verteilt in Entwicklungstools, Ticketsystemen, Wiki-Seiten und E-Mails und sind nicht darauf ausgelegt, im Ernstfall schnell vorgelegt zu werden. Der erste Schritt ist kein aufwendiges Dokumentenmanagementsystem, sondern ein einfaches Template und eine klare Ablagestruktur: Was gehört wohin? Wer hält es aktuell? Was passiert bei einer neuen Produktversion?

Ergebnis: Dokumentationstemplate, definierte Ablagestruktur, benannte Verantwortlichkeit für Pflege.

10.2 Nice-to-haves

Wer die sieben Grundschritte abgeschlossen hat, ist tendenziell gut vorbereitet. Die folgenden fünf Punkte machen CRA-Compliance dauerhaft effizienter und belastbarer. Sie sind nicht dringend, aber strategisch sinnvoll.

1. Komponentenlisten automatisch erzeugen und auf Sicherheitslücken prüfen
Der manuelle Pilot zeigt schnell: Das eigentliche Problem ist nicht das Format, sondern die Aktualität. Wer die SBOM-Erstellung in den normalen Entwicklungsprozess integriert, bekommt bei jedem Release automatisch eine aktuelle Liste, ohne Zusatzaufwand. Noch wertvoller wird das, wenn diese Liste automatisch mit bekannten Sicherheitslücken abgeglichen wird. Ergebnis: kein manuelles Nachschauen mehr, sondern ein Frühwarnsystem, das meldet, wenn eine verbaute Komponente ein bekanntes Problem hat.

2. Lieferanten systematisch prüfen mit einheitlichen Unterlagen
Den ersten Überblick über Drittkomponenten zu haben ist gut. Der nächste Schritt ist Systematik: einheitliche Fragebögen für Zulieferer, klare Vertragsklauseln zu Updates und Sicherheitspflichten, feste Kriterien für die Freigabe neuer Komponenten. Gerade wer in OEM-Ketten oder als Integrator tätig ist, profitiert davon doppelt durch weniger Überraschungen bei Sicherheitslücken in Fremdprodukten und bessere Verhandlungsposition gegenüber Lieferanten.

3. Sicherheitsinformationen strukturiert nach außen kommunizieren
Ein erreichbarer Security-Kontakt ist Pflicht. Der nächste Schritt ist die Qualität der Kommunikation: strukturierte Sicherheitshinweise, die Kunden und Partner maschinell verarbeiten können (Formate: CSAF, VEX). Das klingt technisch hat aber einen direkten Geschäftswert: Industriekunden, die selbst CRA-pflichtig sind, werden zunehmend erwarten, dass ihre Zulieferer klar und schnell kommunizieren, ob eine bekannte Schwachstelle ihre Produkte betrifft.

4. CRA in bestehende Abläufe einbauen statt parallel dazu
Wer CRA als Parallelprozess betreibt, hat dauerhaft Doppelarbeit. Der nachhaltige Weg: Sicherheitsanforderungen fließen ins normale Anforderungsmanagement ein, Risikobewertungen werden Teil regulärer Produktentscheidungen, SBOM-Pflege ist Teil des Releases. Je mehr CRA im Arbeitsalltag unsichtbar wird, desto günstiger und belastbarer ist die Compliance, weil Nachweise nicht nachträglich zusammengesucht werden müssen, sondern automatisch entstehen.

5. Fortschritt regelmäßig messen und der Geschäftsführung sichtbar machen

Ohne Zahlen bleibt CRA ein Projektthema ohne Steuerung. Ein einfaches Dashboard mit wenigen Kennzahlen reicht: Wie viele Produkte haben eine aktuelle Risikobewertung? Wie schnell wurden Schwachstellenmeldungen bearbeitet? Wie vollständig ist die Dokumentation? Diese Übersicht gibt der Geschäftsführung die Grundlage, Ressourcen gezielt einzusetzen, und schafft Nachweise, die gegenüber Kunden, Partnern oder der Marktaufsicht zählen.

11. Beispielhafte Unternehmenssituationen

Nachfolgend sind typische Unternehmenssituationen knapp gespiegelt.

Konstellation 1: KMU-Maschinenbauer

Ein mittelständischer Sondermaschinenbauer liefert Anlagen mit integrierter SPS-Steuerung, HMI-Panel und optionaler Fernwartungsanbindung via VPN. Die Maschinen laufen beim Kunden 10 – 15 Jahre. Der Hersteller hat bislang keine formalisierte Softwareentwicklung, Updates laufen über den Außendienst oder werden vom Kunden selbst eingespielt. Typische Fragen im CRA-Kontext:

- Scope: Ist die Maschine als Ganzes ein „Produkt mit digitalen Elementen“ oder sind Steuerung und Fernwartungszugang getrennt zu bewerten?
- Rolle: Wer ist Hersteller der Embedded Software, der Maschinenbauer selbst, der SPS-Lieferant oder beide?
- Supportperiode: Welche Update-Verpflichtung entsteht für eine Maschine mit 12 Jahren Laufzeit und was bedeutet das für den After-Sales-Prozess?
- Fernwartung: Erhöht die VPN-Anbindung die Produktkategorie (Klasse I)? Welche Anforderungen gelten dann zusätzlich?
- Dokumentation: Was muss in die technische Dokumentation und wer im Unternehmen kann das aktuell erstellen?

Konstellation 2: Embedded-/Komponentenhersteller

Ein Elektronikunternehmen entwickelt Steuerungsmodule mit Firmware, die in Maschinen verschiedener OEMs verbaut werden. Die Module haben keine eigene Benutzeroberfläche; Firmware-Updates werden vom OEM verwaltet. Das Unternehmen hat keine direkte Kundenbeziehung zum Endnutzer. Typische Fragen im CRA-Kontext:

- Produktkategorie: Gilt das Modul als eigenständiges Produkt mit digitalen Elementen oder greift die Komponenten-Ausnahme?
- SBOM: Muss das Unternehmen eine Software Bill of Materials liefern und in welchem Format erwartet das der OEM-Kunde?
- Verantwortungsteilung: Wer ist für Sicherheitsupdates zuständig, wenn der OEM die Firmware-Distribution kontrolliert? Wie muss das vertraglich geregelt sein?
- Due Diligence: Welche Nachweise verlangen OEMs künftig beim Einkauf und wie ist das Unternehmen vorbereitet?
- Vulnerability Handling: Wie muss der Prozess aussehen, wenn eine Schwachstelle in der Firmware bekannt wird und das Modul bereits in hundert verschiedenen Maschinen verbaut ist?

Konstellation 3: Industrieller Softwareanbieter

Ein Softwarehaus vertreibt eine SCADA-Anwendung zur Anlagenvisualisierung sowie Zusatzmodule für Reporting und Alarmmanagement. Kunden betreiben die Software teils on-premise, teils als gehostete Installation. Ältere Versionen sind noch bei vielen Bestandskunden im Einsatz; der Hersteller unterstützt formal die letzten zwei Major Releases. Typische Fragen im CRA-Kontext:

- Produktgrenzen: Gilt jedes Modul als eigenständiges Produkt oder bildet die Gesamtanwendung eine einzige CRA-Einheit? Was ist bei Drittkomponenten im Software-Stack?
- Versionierung: Ab welchem Änderungsumfang gilt ein Update als neues Produkt mit neuem Konformitätspfad?
- Alte Versionen: Besteht eine Sicherheitspflicht für Versionen, die formal aus dem Support gefallen sind, aber noch im Einsatz bei Kunden sind?
- Vulnerability Handling: Wie muss der Meldeprozess zu ENISA aussehen und wer im Unternehmen übernimmt diese Funktion operativ?
- Release- und Archivlogik: Was muss für jede Version dokumentiert und archiviert werden und wie lange?

12. Vertiefende Materialien und aktuelle Entwicklungen

Für die weitere Vertiefung und laufende Aktualisierung sind insbesondere folgende Materialien relevant:

- FAQs on the Cyber Resilience Act, Version 1.2, Europäische Kommission, Januar 2026 [Q19]
- Cyber Resilience Act – Implementation, Europäische Kommission, Fortschrittsübersicht mit Zeitleiste, Stand März 2026 [Q01]
- Commission Implementing Regulation (EU) 2025/2392 zu den technischen Beschreibungen wichtiger und kritischer Produkte
- BSI TR-03183 Teil 1 bis 3 zu allgemeinen Anforderungen, SBOM sowie Vulnerability Reports and Notifications [Q21, Q22, Q23]
- BSI Management-Blitzlicht CRA [Q20]
- OT-Security im industriellen Mittelstand, Allianz Industrie 4.0 Baden-Württemberg/Fraunhofer IAO, Juni 2025 [Q24]
- Leitfaden zur Etablierung eines Cyber-Bündnisses, Allianz Industrie 4.0 Baden-Württemberg, 2023 [Q25]

Darüber hinaus ist die Unterstützungslandschaft für KMU in Bewegung. Die Kommission verweist inzwischen explizit auf eigene Informations- und Förderangebote für kleine und mittlere Unternehmen. Anfang 2026 wurde beispielsweise eine erste Kofinanzierungsrunde des SECURE-Projekts für MSMEs angekündigt. Solche Angebote sind nicht Kern des CRA, können aber in der Kommunikation als hilfreicher Einstieg genannt werden. [Q04, Q05, Q08, Q12, Q13, Q15]

13. Fazit

Der Cyber Resilience Act ist keine Regulierungsaufgabe, die sich mit juristischer Lektüre erledigt. Er ist eine Umsetzungsaufgabe mit konkreten Konsequenzen für Produkte, Prozesse und Verantwortlichkeiten. Wer vernetzte Produkte entwickelt, integriert oder unter eigenem Namen in Verkehr bringt, ist betroffen: mit Anforderungen an die Produktsicherheit, an die Transparenz über Komponenten und Risiken, an Schwachstellenkommunikation und an verlässliche Update- und Supportzusagen über den gesamten Produktlebenszyklus.

Das lässt sich nicht in einer Abteilung abarbeiten. Es braucht das Zusammenspiel von Produktverantwortung, Entwicklung, IT-/OT-Security, Qualitätsmanagement und Compliance. Und wo Auslegungsfragen offen sind oder Konformitätswege gewählt werden müssen, auch juristische Einschätzung. Das Management muss keine Regulierungsdetails selbst beantworten, wohl aber die Voraussetzungen schaffen: klare Verantwortlichkeiten, realistische Priorisierung und eine Governance-Struktur, die CRA nicht als Einmalprojekt behandelt, sondern als dauerhaften Bestandteil der Produktverantwortung.

Für die Praxis gilt eine klare Staffelung, zuerst Grundlagenarbeit, nicht Vollständigkeit: Transparenz über betroffene Produkte und die eigene Marktrolle, Meldefähigkeit bis zum Stichtag im September 2026, ein Mindestprozess für Risikobewertung und Schwachstellenhandling. Auf dieser Basis lässt sich alles Weitere realistisch planen mit einem 90-Tage-Paket für die nächsten Schritte und einer Roadmap, die Must-haves und Nice-to-haves bewusst trennt. Diese Logik – erst Orientierung und Handlungsfähigkeit, dann schrittweise Vertiefung – entspricht dem, was EU-Guidance und BSI-Unterlagen empfehlen, und dem, was gut aufgestellte Unternehmen in vergleichbaren Regulierungsprozessen tatsächlich gemacht haben. [Q01, Q04, Q05, Q20]

Am Ende dieser Kurzstudie sollten vier Fragen beantwortet sein:

1. Sind wir vom CRA betroffen und wenn ja, mit welchen Produkten und in welcher Rolle?
2. Was müssen wir bis wann sicher im Griff haben und was kann auf einer zweiten Reifestufe folgen?
3. Wo liegen unsere größten Lücken und welche davon sind vor dem September-Stichtag 2026 wirklich kritisch?
4. Welche nächsten Schritte sind fachlich sinnvoll und im eigenen Unternehmen realistisch umsetzbar?

Wenn diese vier Fragen beantwortet sind, hat die Kurzstudie ihr Ziel erreicht. Sie ist keine fertige Compliance-Roadmap, diese muss jedes Unternehmen auf Basis seiner konkreten Produkte, Rollen und Ausgangslage selbst entwickeln. Aber sie ist die Grundlage für ein realistisches Bild der eigenen Betroffenheit, ein klares Verständnis der zeitlichen Prioritäten und einen ersten priorisierten Handlungsrahmen, der aus einem abstrakten Regulierungsthema einen steuerbaren Umsetzungsprozess macht. [Q01, Q04, Q05, Q08, Q16]

14. Quellenverzeichnis

Quellenmarker im Text werden in eckigen Klammern ausgewiesen (z. B. [Q01]).

[Q01] Europäische Kommission: Cyber Resilience Act – Implementation. 04.03.2026. https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation

[Q02] Europäische Kommission: Cyber Resilience Act | Shaping Europe's digital future. 03.12.2025. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[Q03] Europäische Kommission: Draft Commission guidance on the Cyber Resilience Act – Have your say. Abruf 13.04.2026. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en

[Q04] Europäische Kommission: Commission publishes for feedback draft guidance to assist companies in applying the Cyber Resilience Act. 03.03.2026. https://digital-strategy.ec.europa.eu/en/news/commission-publishes-feedback-draft-guidance-assist-companies-applying-cyber-resilience-act

[Q05] Europäische Kommission: Cyber Resilience Act – Manufacturers. 04.03.2026. https://digital-strategy.ec.europa.eu/en/policies/cra-manufacturers

[Q06] ENISA / Joint Research Centre: Cyber Resilience Act Requirements Standards Mapping. 04.04.2024. https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

[Q07] ENISA: Cyber Resilience Act implementation via EUCC and its applicable technical elements. 26.02.2025. https://certification.enisa.europa.eu/publications/cyber-resilience-act-implementation-eucc-and-its-applicable-technical-elements_en

[Q08] ENISA: SME Cyber Resilience Act Survey. Abruf 13.04.2026. https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/sme-cyber-resilience-act-survey

[Q09] ATHENE: White paper CRA: Empfehlungen zur Umsetzung technischer Anforderungen. Abruf 13.04.2026. https://www.athene-center.de/en/research/think-tank/cyber-resilience-act-cra

[Q10] Fraunhofer SIT: Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht. Stand 12.03.2024. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/CRA_EU-Cyber-Resilience-Act_Whitepaper.pdf

[Q11] Fraunhofer SIT: Cyber Resilience Act – Risk Management. 06.2025. https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/CRA-RiskManagement-202506.pdf

[Q12] BITMi: Cyber Resilience Act – Einordnung und Leitfaden für mittelständische Unternehmen. 01.03.2026. https://bitmi.de/it-sicherheitsblog-cyber-resilience-act-einordnung-und-leitfaden-fuer-mittelstaendische-unternehmen/

[Q13] IHK Köln: Cyber Resilience Act (CRA): Digitale Dienste und Produkte müssen gesichert werden. Abruf 13.04.2026. https://www.ihk.de/koeln/hauptnavigation/digitalisierung-und-innovation/digitalisierung/cyber-resilience-act-6192072

[Q14] Heuking: Cyber Resilience Act: Wer ist betroffen und was Unternehmen jetzt wissen müssen. 09.04.2026. https://www.heuking.de/de/news-events/newsletter-fachbeitraege/artikel/cyber-resilience-act-wer-ist-betroffen-und-was-unternehmen-jetzt-wissen-muessen.html

[Q15] DATEV: EU-Kommission veröffentlicht Draft Guidance zur Anwendung des CRA. 11.03.2026. https://www.datev-magazin.de/nachrichten-steuern-recht/recht/eu-kommission-veroeffentlicht-draft-guidance-zur-anwendung-des-cra-145254

[Q16] ONEKEY: IoT & OT Cybersecurity Report 2025. 03.09.2025. https://www.onekey.com/resource/iot-ot-cybersecurity-report-2025

[Q17] Linux Foundation: Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source. 2025. https://www.linuxfoundation.org/research/cra-readiness

[Q18] it-sicherheit.de / Bitkom: Cyber Resilience Act (CRA) – Bitkom-Studie 2022. Abruf 13.04.2026. https://it-sicherheit.de/it-sicherheitsstudien/cyber-resilience-act-cra/

[Q19] Europäische Kommission: FAQs on the Cyber Resilience Act, Version 1.2. 16.01.2026. Bereitgestellte Unterlage (PDF)

[Q20] BSI: Cyber Resilience Act – Management-Blitzlicht. 11.2024. Bereitgestellte Unterlage (PDF)

[Q21] BSI: TR-03183 Teil 1: General requirements, Version 0.10.0. 12.09.2025. Bereitgestellte Unterlage (PDF)

[Q22] BSI: TR-03183 Teil 2: Software Bill of Materials (SBOM), Version 2.1.0. 20.08.2025. Bereitgestellte Unterlage (PDF)

[Q23] BSI: TR-03183 Teil 3: Vulnerability Reports and Notifications, Version 1.0.0. 20.08.2025. Bereitgestellte Unterlage (PDF)

[Q24] Allianz Industrie 4.0 BW / Fraunhofer IAO: OT-Security im industriellen Mittelstand. 06.2025. https://www.i40-bw.de/wp-content/uploads/2025/06/Studie-OT-Security-im-industriellen-Mittelstand.pdf

[Q25] Allianz Industrie 4.0 BW: Leitfaden Cyber-Bündnis, Anhang 1. 08.2023. https://www.i40-bw.de/wp-content/uploads/2023/08/Leitfaden-Cyber-Buendnis_Anhang-1.pdf

15. Verfasser der Studie

Die DIZ | Digitales Innovationszentrum GmbH versteht sich als verlässlicher Brückenbauer zwischen Wirtschaft, Wissenschaft und Politik. Als neutrale Innovationsagentur für Digitale Transformation, IT-Sicherheit und Künstliche Intelligenz gibt das DIZ Unternehmen, Forschung, Kommunen und öffentlicher Hand Orientierung in der digitalen Transformation und überführt technologische Entwicklungen in die Anwendung. Ein besonderer Schwerpunkt liegt auf den Innovations-, Förder- und Projektservices: von der Ideengenerierung, Förderberatung und Antragstellung über die Konsortialbildung bis zur Koordination von Innovationsprojekten.

Die Hauptbearbeitung der vorliegenden CRA-Studie erfolgte durch das DIZ. Es bringt seine Erfahrung in Projektkoordination, Stakeholdermanagement sowie Förder- und Innovationsberatung ein, um regulatorische Anforderungen praxisnah zu vermitteln. Ziel ist es, Unternehmen Orientierung zu den Anforderungen des Cyber Resilience Act zu geben und den Transfer in konkrete Umsetzungs- und Innovationsprozesse zu unterstützen. Unternehmen, die den CRA als Innovationschance nutzen möchten, finden im DIZ einen erfahrenen Partner.

Das FZI Forschungszentrum Informatik mit Hauptsitz in Karlsruhe ist eine unabhängige und gemeinnützige Forschungseinrichtung, die seit über 40 Jahren neueste wissenschaftliche Erkenntnisse der Informationstechnologie in praxistaugliche Lösungen überführt. Für die vorliegende Studie wurde insbesondere die Expertise des Forschungsbereichs ***Cybersecurity and Law*** einbezogen, der anwendungsorientierte Methoden und Grundlagen für sichere Digitalisierung sowie die Ausgestaltung informationstechnologischer Rechtsrahmen erforscht. Die fachliche Einbindung des FZI erfolgte durch Maria Rill und Aline Vugrincic aus dem Bereich ***Cybersecurity and Law***. Maria Rill leitet die Abteilung und arbeitet unter anderem zu Rechtsinformatik sowie Datenschutz- und IT-Sicherheitsrecht. Aline Vugrincic ist stellvertretende Abteilungsleiterin und seit 2021 als wissenschaftliche Mitarbeiterin im Forschungsbereich tätig.

Bearbeitung: Gennadi Schermann, Jennifer Dinges
DIZ | Digitales Innovationszentrum GmbH, Haid-und-Neu-Straße 18, 76131 Karlsruhe
projekte@diz-bw.de
www.diz-bw.de

Fachliche Mitwirkung: Maria Rill, Aline Vugrincic
FZI Forschungszentrum Informatik, Haid-und-Neu-Straße 10 – 14, 76131 Karlsruhe
www.fzi.de

16. Impressum

Auftraggeber und Herausgeber
Allianz Industrie 4.0 Baden-Württemberg
beim VDMA e. V. Baden-Württemberg
Kronenstr. 3
70173 Stuttgart
Tel.: +49 711 22801-20
E-Mail: info@i40-bw.de
Internet: www.i40-bw.de

Kontakt
Dr. Isabella R. Jesemann
Operations Manager Allianz Industrie 4.0 Baden-Württemberg
Tel.: +49 171 9620357
E-Mail: isabella.jesemann@vdma.eu

Grafiken
DIZ | Digitales Innovationszentrum GmbH
FZI Forschungszentrum Informatik

Layout, Satz und Druck
burger Print & Medien GmbH
Furtstraße 2/1
75242 Neuhausen
E-Mail: info@burgerprint.de
Internet: www.burgerprint.de

Erscheinungsjahr
2026

Anlage A

Umsetzungsleitfaden für Produktverantwortliche und Umsetzungsteams

Reifegradanalyse · Gap-Analyse · Priorisierte 10 Schritte · Rollen · Materialien · Quellenverzeichnis

Zielgruppe	Produktmanagement, Entwicklung, IT-/OT-Security, Qualität/Compliance, Einkauf
Zweck	Operatives Werkzeug für Standortbestimmung, Lückenanalyse und erste Umsetzungsplanung.
Hauptdokument	Bitte zuerst das Hauptdokument (Leitungsebene) lesen, es liefert den Entscheidungsrahmen für diese Anlage.

CRA-Selbsteinschätzung (Reifegradanalyse / Self-Check)

Bewertungsskala: 0 = nicht vorhanden | 1 = teilweise vorhanden | 2 = belastbar umgesetzt.
Bitte je Produktfamilie ausfüllen. Die Ergebnisse bilden die Grundlage für die Gap-Analyse und die Priorisierung der ersten 10 Schritte.

Quellenhinweis: Die Reifegradlogik verdichtet CRA-Pflichten mit BSI-Umsetzungshinweisen und praxisnahen Whitepapern zu Risiko, SBOM und Vulnerability Handling. [Q06, Q09, Q11, Q20, Q21, Q22, Q23]

Handlungsfeld	Leitfrage	0	1	2
Produktinventur	Haben wir eine aktuelle Liste relevanter Produkte, Versionen, Remote-Anteile und Kernkomponenten?	❑	❑	❑
Rollenklärung	Sind Marktrolle, Freigabelogik und Verantwortlichkeiten je Produkt dokumentiert?	❑	❑	❑
Risikobewertung	Gibt es einen wiederholbaren Ansatz für Cybersecurity Risk Assessments?	❑	❑	❑
Security by Design	Werden Sicherheitsanforderungen früh im Entwicklungsprozess berücksichtigt?	❑	❑	❑
Secure Defaults	Werden Produkte mit sicheren Voreinstellungen ausgeliefert?	❑	❑	❑
SBOM	Kann für Kernprodukte eine aktuelle, maschinenverarbeitbare SBOM erzeugt werden?	❑	❑	❑
Drittkomponenten	Gibt es definierte Prüf- und Freigabekriterien für Zulieferer und Komponenten?	❑	❑	❑
Vulnerability Handling	Existieren definierte Wege für Meldung, Analyse, Priorisierung, Behebung und Kommunikation?	❑	❑	❑
Meldefähigkeit	Können Meldungen nach Art. 14 CRA innerhalb der Fristen angestoßen werden (24h-Frühwarnung, 72h-Folgemeldung)?	❑	❑	❑
Support & Updates	Sind Supportperiode und Patchstrategie je Produktfamilie schriftlich festgelegt und kommunizierbar?	❑	❑	❑
Techn. Dokumentation	Sind Risikoanalyse, Tests, Nutzerinformationen und Nachweise strukturiert verfügbar?	❑	❑	❑
Governance	Sind Zuständigkeiten für Management, Produktmanagement, Entwicklung, Security und Compliance benannt?	❑	❑	❑

Skala: 0 = nicht vorhanden | 1 = teilweise vorhanden | 2 = belastbar umgesetzt

Auswertung: 0–8 Pkt. = hoher Strukturierungsbedarf | 9–16 = Grundlagen vorhanden, Lücken schließen | 17–24 = gute Ausgangslage, gezielte Vertiefung

Must-haves und Nice-to-haves nach Zeithorizont

Quellenhinweis: Die Struktur orientiert sich an den Umsetzungsfristen des CRA, der BSI-Logik sowie aktuellen Praxisstudien und KMU-Leitfäden. [Q01, Q04, Q05, Q08, Q12, Q13, Q16, Q24, Q25]

Zeitraum	Must-haves	Nice-to-haves
sofort	CRA-Kernteam benennen; Produktinventur starten; Rollen je Produktfamilie klären; Betroffenheitsprüfung und Negativdokumentation anlegen.	Erste CRA-Kennzahlen definieren; internes Reportingformat aufbauen.
bis Sommer 2026	Security-Kontaktseite, CVD-Policy, Eskalationswege, Security.txt vorbereiten; Konformitätsbewertungsweg je Produktkategorie festlegen.	Strukturierte Security-Advisories und CSAF/VEX-Logik vorplanen.
bis 11.09.2026	Meldefähigkeit für aktiv ausgenutzte Schwachstellen und schwere Vorfälle sicherstellen.	Erste Notfallübungen und Tabletop-Tests durchführen.
bis Ende 2026	SBOM-Pilot, Lieferantenabfragen, Dokumentationstemplates und priorisierte Risikoanalysen aufbauen; technische Dokumentation nach Anhang VII CRA strukturieren.	Stärkere Automatisierung der SBOM- und Schwachstellenprozesse.
bis 11.12.2027	Konformitäts- und Supportfähigkeit für neue/wesentlich geänderte Produkte; CE-Kennzeichnung und EU-Konformitätserklärung.	Weiterführende Prozessintegration und kontinuierliches Reifegradmonitoring.

Gap-Analyse: Wo fehlen noch Bausteine?

Quellenhinweis: Typische Lücken in Produktinventur, Rollenklärung, SBOM, Lieferkette, Security-Kontakten und Dokumentation. [Q06, Q09, Q11, Q16, Q19, Q22, Q23]

Baustein	Leitfrage	Priorität	Nächster sinnvoller Schritt
Produkt/ Scope	Welche Produkte, Versionen und Remote-Funktionen sind betroffen?	Hoch	Produktinventur vervollständigen und Scope-Kriterien dokumentieren.
Kategorien	Ist die Kernfunktion sauber gegen important/critical abgegrenzt?	Mittel-Hoch	Produktkategorien und Konformitätswege je Produktfamilie prüfen.
Drittkomponenten	Fehlen Supportzusagen oder Sicherheitsinformationen von Zulieferern?	Hoch	Due-Diligence-Checkliste und Lieferantenabfrage einführen.
SBOM	Kann für Kernprodukte eine aktuelle SBOM erzeugt werden?	Hoch	Pilot mit 1 – 2 Referenzprodukten starten.
Vulnerability Handling	Gibt es CVD-Policy, Security-Kontakte und PSIRT-/CSIRT-Logik?	Hoch	Mindestprozess und öffentliche Kontaktpunkte aufbauen.
Support/ Updates	Ist die Supportperiode pro Produkt nachvollziehbar festgelegt?	Hoch	Support- und Patchlogik je Produktfamilie entscheiden.
Dokumentation	Sind Risikoanalyse, Tests und Nutzerinformationen strukturiert abrufbar?	Mittel-Hoch	Einheitliche Templates und Ablagestruktur einführen.

Priorisierte erste 10 Schritte

Die folgenden Schritte bauen aufeinander auf und sind auf die CRA-Stichtage abgestimmt. Sie richten sich an Produktverantwortliche und Umsetzungsteams.

Schritt 1: CRA-Verantwortung auf Leitungsebene verankern und Kernteam benennen

CRA-Readiness braucht einen benannten Owner auf Leitungsebene, der Prioritäten setzt, Ressourcen freigibt und im Ernstfall eskalationsfähig ist. Das Kernteam sollte funktionsübergreifend besetzt sein: Produktmanagement, Entwicklung, IT-/OT-Security, Qualität/Compliance und je nach Unternehmensgröße Einkauf.

Ein gemeinsamer Kick-off-Termin auf Basis des Hauptdokuments ist erfahrungsgemäß der effektivste erste Schritt. Er klärt Scope, Rollen und die drei bis fünf größten Lücken in einem einzigen Arbeitsschritt.

Konkretes Ergebnis: *Benannter CRA-Verantwortlicher auf Leitungsebene; dokumentiertes Kernteam mit Funktionszuordnung; erster Review-Termin vereinbart.*

Schritt 2: Produktinventur und Negativdokumentation anlegen

Eine belastbare Produktinventur ist die Voraussetzung für jeden weiteren Schritt. Die Inventur muss bewusst breiter angesetzt werden als das offensichtliche Produktportfolio: Firmware-Stände, Engineering-Tools, Serviceschnittstellen, Fernwartungsanteile und separat vermarktete Softwaremodule werden häufig übersehen.

Mindestens genauso wichtig ist die Negativdokumentation für Produkte, die nach Prüfung eindeutig außerhalb des CRA-Anwendungsbereichs liegen. Eine kurze, datierte Begründung je Produktfamilie genügt, ist aber im Kontext einer Marktaufsichtsprüfung unerlässlich.

Konkretes Ergebnis: *Strukturierte Produktliste mit Versionsständen, Remote-Anteilen und erster CRA-Einordnung; kurze Negativdokumentation für nicht betroffene Produkte.*

Schritt 3: Marktrolle je Produktfamilie dokumentieren; OEM- und White-Label-Konstellationen prüfen

Die Marktrolle bestimmt, welche Pflichten ein Unternehmen trägt. Wer unter eigenem Namen oder eigener Marke in Verkehr bringt, trägt die vollständigen Herstellerpflichten, auch wenn wesentliche Teile zugekauft sind. OEM- und White-Label-Konstellationen müssen deshalb explizit geprüft werden.

Die zentrale Frage lautet: Unter wessen Namen wird das Produkt dem Endkunden bereitgestellt? Die Antwort bestimmt, wer Risikoanalyse, Dokumentation, Konformitätsbewertung, CE-Kennzeichnung und Meldepflichten verantwortet.

Konkretes Ergebnis: *Dokumentierte Marktrolle je Produktfamilie; identifizierte OEM- und White-Label-Konstellationen mit Klärungsbedarf.*

Schritt 4: Produktkategorien bestimmen und Konformitätsbewertungsweg je Kategorie festlegen

Standardprodukte können grundsätzlich im Wege der internen Kontrolle/Selbstbewertung bewertet werden. Für wichtige Produkte Klasse I hängt der Konformitätsbewertungsweg insbesondere davon ab, ob harmonisierte Normen, gemeinsame Spezifikationen oder geeignete Zertifizierungsschemata angewendet werden. Für wichtige Produkte Klasse II sowie kritische Produkte gelten strengere Verfahren; regelmäßig ist eine notifizierte Stelle bzw. ein einschlägiges Zertifizierungsverfahren einzubeziehen.

Maßgeblich ist die Kernfunktion des vermarkteten Produkts, nicht die Kernfunktion integrierter Komponenten. Die Einordnung muss dokumentiert und begründet sein (Durchführungsverordnung (EU) 2025/2392).

Konkretes Ergebnis: *Vorläufige Kategorisierung je Produktfamilie (Standard/wichtig Klasse I/wichtig Klasse II/kritisch); festgelegter Konformitätsbewertungsweg mit Begründung.*

Schritt 5: Mindestansatz für Cybersecurity Risk Assessments definieren

Der CRA fordert einen risikobasierten Ansatz: Cybersicherheitsrisiken müssen produktbezogen, systematisch und nachvollziehbar ermittelt, bewertet und behandelt werden. Das Ergebnis ist nicht nur Grundlage für Schutzmaßnahmen, sondern zentraler Bestandteil der technischen Dokumentation nach Anhang VII CRA.

Pragmatischer Einstieg: Welche Angriffsvektoren sind realistisch? Welche Schadenspotenziale bestehen (Verfügbarkeit, Integrität, Vertraulichkeit)? Welche Maßnahmen fehlen? Die BSI-TR Teil 1 liefert hierfür eine praktische Prüflogik.

Konkretes Ergebnis: *Dokumentierter Mindestansatz für Risikobewertungen; erste Durchführung für priorisierte Produktlinien mit Ergebnissen und identifizierten Maßnahmen.*

Schritt 7: Due-Diligence-Check für Drittkomponenten und Zulieferer etablieren

Hersteller können sich nicht allein auf eine CE-Kennzeichnung einzelner Komponenten verlassen. Wer Drittkomponenten integriert, muss angemessene Sorgfalt walten lassen. Das gilt ausdrücklich auch für Open-Source-Komponenten, die selbst nicht im CRA liegen.

Mindestprozess: Erhält die Komponente regelmäßige Sicherheitsupdates? Sind kritische Schwachstellen oder ein nahes End-of-Life bekannt? Passt der Supportzeitraum zur geplanten Nutzungsdauer? Liegen verlässliche Versionsdaten vor?

Konkretes Ergebnis: *Prüfcheckliste für Drittkomponenten und Zulieferer; Prozess für Erstprüfung und regelmäßigen Review bestehender Abhängigkeiten.*

Schritt 8: Security-Kontaktseite, Security.txt und CVD-Policy vorbereiten; ENISA-Meldeprozess und 24h-/72h-Meldekette testen

Dieser Schritt ist termingebunden: Ab 11. September 2026 müssen Hersteller aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle fristgerecht melden. Abschlussbericht bei aktiv ausgenutzten Schwachstellen spätestens 14 Tage nach Verfügbarkeit einer Korrektur- oder Minderungsmaßnahme; bei schwerwiegenden Sicherheitsvorfällen innerhalb eines Monats nach der 72h-Meldung. Unternehmen müssen Meldungen nach CRA über eine zentrale, von der ENISA betriebene Plattform (Single Reporting Platform) abgeben. Diese Meldungen werden von dort automatisch an das jeweils zuständige nationale Marktaufsichtsbehörde weitergeleitet. In Deutschland ist dies das BSI.

Zu umsetzende Bausteine: erreichbare Security-Kontaktseite, Security.txt-Datei nach RFC 9116, dokumentierte CVD-Policy und – intern – eine getestete Meldekette mit simuliertem Szenario, das die 24-Stunden-Frist unter realistischen Bedingungen durchspielt.

Konkretes Ergebnis: *Öffentlich erreichbarer Security-Kontakt und Security.txt; dokumentierte CVD-Policy; intern getestete Meldekette mit klaren Zuständigkeiten und nachgewiesener Fristtauglichkeit.*

Schritt 9: Patch-, Update- und Supportlogik je Produktfamilie festlegen

Art. 13 Abs. 8 und 9 CRA verlangen, dass die Supportperiode unter Berücksichtigung der Art des Produkts sowie der erwarteten Nutzungsdauer festgelegt wird. Sie beträgt grundsätzlich mindestens zehn Jahre, sofern die erwartete Nutzungsdauer nicht kürzer ist. Für Produkte mit zehn bis zwanzig Jahren Lebenszeit ist das eine der inhaltlich anspruchsvollsten Anforderungen und abhängig von Supportzusagen eingekaufter Komponenten und Drittbibliotheken.

Erforderlich: Wie lange werden Sicherheitsupdates je Produktfamilie bereitgestellt? Nach welcher Logik werden Patches klassifiziert? Wie wird mit Komponenten umgegangen, deren Hersteller-Support vor der eigenen Supportperiode ausläuft?

Konkretes Ergebnis: *Dokumentierte Supportperiode und Patchlogik je Produktfamilie; intern freigegeben, mit Produktmanagement und Vertrieb abgestimmt.*

Schritt 10: Dokumentationstemplates für Risikoanalyse, Tests, Nutzerinformationen und Advisories vereinheitlichen (Anhang VII CRA)

Anhang VII CRA definiert, was zur technischen Dokumentation gehören muss: Produktbeschreibung, Risikoanalyse, Sicherheitsanforderungen und umgesetzte Maßnahmen, Testergebnisse, SBOM, EU-Konformitätserklärung, Nutzerinformationen sowie Angaben zu Schwachstellenbehandlung und Update-Mechanismen.

In vielen Unternehmen liegen diese Informationen verstreut in Entwicklungstools, Ticketsystemen und E-Mails und sind nicht auf Nachweisfähigkeit ausgelegt. Ziel: einheitliche Templates je Dokumentationsart, definierte Ablagestruktur, klare Verantwortlichkeiten für Pflege und Aktualisierung.

Konkretes Ergebnis: *Dokumentationstemplate nach Anhang VII CRA für priorisierte Produktfamilien; definierte Ablagestruktur und Verantwortlichkeiten; begonnene Dokumentation für die wichtigsten Produkte.*

Rollen und internes Zusammenspiel

Wichtig: Begriffe wie OEM, White Label oder Integrator beschreiben typische Umsetzungssituationen, ersetzen aber nicht die rechtliche Einordnung der Marktrolle je Produktfamilie.

Funktion	**Typischer Beitrag zur CRA-Umsetzung**
Geschäftsführung	Priorisierung, Ressourcen, Governance, Eskalation schwerer Sicherheitsereignisse
Produktmanagement	Produktinventur, Zielmärkte, Supportperiode, Roadmap, Nutzerinformationen
Entwicklung	Security by Design, technische Maßnahmen, SBOM, Test- und Build-Prozesse
IT-/OT-Security	Risikobewertung, Security Controls, Schwachstellenmanagement, Meldeunterstützung
Qualität/Compliance	Dokumentationsstandards, Nachweisführung, Konformitätslogik, Auditfestigkeit
Einkauf/Supplier Management	Lieferantenabfragen, Sicherheitsanforderungen, Support- und Security-Informationen von Zulieferern

Weiterführende Materialien

Der Leitfaden soll bewusst kompakt bleiben. Für vertiefende Fragen stehen folgende Unterlagen zur Verfügung:

Quelle	Inhalt und Einsatzzweck
Verordnung (EU) 2024/2847	Volltext des Cyber Resilience Act über EUR-Lex.
EU-FAQ Version 1.2 (Jan. 2026)	Auslegungshilfe zu Scope-, Übergangs- und Rollenfragen; wichtig für KMU. Kein Rechtscharakter.
Durchführungs-VO 2025/2392	Technische Beschreibungen für wichtige und kritische Produktkategorien.
BSI TR-03183 Teil 1 – 3	Prüflogik für Risikobewertung (Teil 1), SBOM-Mindestinhalte (Teil 2), Schwachstellenmeldungen und Benachrichtigungen (Teil 3).
BSI Management-Blitzlicht CRA	Sehr kompakte Managementeinordnung; gut für erste Orientierung auf Leitungsebene.
OT-Security im ind. Mittelstand (Allianz Industrie 4.0/Fraunhofer IAO, 2025)	Weiterführende Perspektive auf industrielle Sicherheitsorganisation, Basis-Level und Roadmap.
ENISA Standards Mapping	Spiegelung von CRA-Anforderungen gegen bestehende Normen (z. B. IEC 62443).
ATHENE/Fraunhofer SIT Whitepaper	Technische Umsetzungshinweise zu SBOM, Security Testing und Risikomanagement.
BITMi/IHK / Heuking/DATEV	Management-, KMU- und Compliance-Perspektiven für den praktischen Einstieg.

Quellenverzeichnis

Quellenmarker im Text werden in eckigen Klammern ausgewiesen (z. B. [Q01]).

Offizielle EU- und ENISA-Quellen

Code	Quelle
[Q00]	Amtsblatt EU: Verordnung (EU) 2024/2847 (Cyber Resilience Act). https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402847
[Q01]	Europäische Kommission: Cyber Resilience Act – Implementation. 04.03.2026. https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation
[Q02]	Europäische Kommission: Cyber Resilience Act | Shaping Europe's digital future. 03.12.2025. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[Q03]	Europäische Kommission: Draft Commission guidance on the Cyber Resilience Act. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959
[Q04]	Europäische Kommission: Commission publishes feedback draft guidance to assist companies applying the CRA. 03.03.2026.
[Q05]	Europäische Kommission: Cyber Resilience Act – Manufacturers. 04.03.2026. https://digital-strategy.ec.europa.eu/en/policies/cra-manufacturers
[Q06]	ENISA / JRC: Cyber Resilience Act Requirements Standards Mapping. 04.04.2024. https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping
[Q07]	ENISA: CRA implementation via EUCC and its applicable technical elements. 26.02.2025.
[Q08]	ENISA: SME Cyber Resilience Act Survey. https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/sme-cyber-resilience-act-survey
[Q19]	wEuropäische Kommission: FAQs on the Cyber Resilience Act, Version 1.2. 16.01.2026. (Bereitgestellte Unterlage)

Fachstudien, Whitepaper und Praxisquellen

Code	Quelle
[Q09]	ATHENE: White paper CRA: Empfehlungen zur Umsetzung technischer Anforderungen. https://www.athene-center.de/en/research/think-tank/cyber-resilience-act-cra
[Q10]	Fraunhofer SIT: Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht. 12.03.2024.
[Q11]	Fraunhofer SIT: Cyber Resilience Act – Risk Management. 06.2025.
[Q12]	BITMi: Cyber Resilience Act – Einordnung und Leitfaden für mittelständische Unternehmen. 01.03.2026.
[Q13]	IHK Köln: Cyber Resilience Act (CRA): Digitale Dienste und Produkte müssen gesichert werden.
[Q14]	Heuking: Cyber Resilience Act: Wer ist betroffen und was Unternehmen jetzt wissen müssen. 09.04.2026.
[Q15]	DATEV: EU-Kommission veröffentlicht Draft Guidance zur Anwendung des CRA. 11.03.2026.
[Q16]	ONEKEY: IoT & OT Cybersecurity Report 2025. 03.09.2025.
[Q17]	Linux Foundation: Unaware and Uncertain: The Stark Realities of CRA Readiness in Open Source. 2025.
[Q24]	Allianz Industrie 4.0 BW/Fraunhofer IAO: OT-Security im industriellen Mittelstand. 06.2025.
[Q25]	Allianz Industrie 4.0 BW: Leitfaden Cyber-Bündnis, Anhang 1. 08.2023.

Ergänzende technische Grundlagen (BSI)

Code	Quelle
[Q20]	BSI: Cyber Resilience Act – Management-Blitzlicht. 11.2024. (Bereitgestellte Unterlage)
[Q21]	BSI: TR-03183 Teil 1: General requirements, Version 0.10.0. 12.09.2025. (Bereitgestellte Unterlage)
[Q22]	BSI: TR-03183 Teil 2: Software Bill of Materials (SBOM), Version 2.1.0. 20.08.2025. (Bereitgestellte Unterlage)
[Q23]	BSI: TR-03183 Teil 3: Vulnerability Reports and Notifications, Version 1.0.0. 20.08.2025. (Bereitgestellte Unterlage)

Anlage B

Für die Leitungsebene

Entscheidungsgrundlage, Quick Check und Management-Agenda

Zielgruppe	Geschäftsführung, Bereichs- und Produktleitungen
Zweck	Kurzes Entscheidungs- und Orientierungsdokument: Was bedeutet der CRA für unser Unternehmen und was muss das Management jetzt in die Wege leiten?
Ergänzung	Anlage A (Umsetzungsteams): Reifegradanalyse, Gap-Analyse, priorisierte 10 Schritte, Rollen, Materialien

Hinweis:
Dieses Hauptdokument ist bewusst kurz gehalten. Es dient der Leitungsebene als Entscheidungsgrundlage. Die operativen Details – Reifegradanalyse, Gap-Analyse, priorisierte Umsetzungsschritte und Rollenübersicht – finden sich in Anlage A für die Umsetzungsteams.

Management Summary

Wenn Sie Software, vernetzte Geräte oder Komponenten mit digitalen Funktionen in der EU verkaufen, betrifft Sie der CRA mit hoher Wahrscheinlichkeit. Der CRA ist kein isoliertes Compliance-Thema, sondern betrifft Produktentwicklung, Support und Lieferkette zugleich. Für viele Unternehmen – gerade kleine und mittlere Betriebe – ist der erste Schritt nicht vollständige Regelkonformität, sondern Klarheit: Welche Produkte sind betroffen, welche Rolle nimmt das Unternehmen ein, und welche Mindestanforderungen müssen bis September 2026 bzw. Dezember 2027 erfüllt sein?

Hauptaufgabe	Was das praktisch bedeutet
Betroffenheit zuerst klären	Produktinventur, Remote-Anteile, Firmware, Engineering-Tools und separat vermarktete Softwaremodule systematisch erfassen – je Produktfamilie, nicht nur auf Unternehmensebene.
Rollen sauber benennen	Je Produktfamilie klären: Stellen wir das Produkt selbst her (Hersteller), kaufen wir es außerhalb der EU ein und bringen es in den EU-Markt (Importeur) oder verkaufen wir nur weiter (Händler)? Besonders bei Eigenmarkenprodukten (White-Label/OEM: fremdes Produkt, eigener Name) explizit prüfen, das macht Sie zum Hersteller mit vollem Pflichtenumfang.
Meldefähigkeit bis 11.09.2026 absichern	Wenn eine Sicherheitslücke in einem Ihrer Produkte aktiv ausgenutzt wird oder ein schwerer Sicherheitsvorfall eintritt, müssen Sie das behördlich melden: innerhalb von 24 Stunden eine Erstmeldung, innerhalb von 72 Stunden eine Folgemeldung. Wer meldet? Wer entscheidet? Das muss intern geklärt und dokumentiert sein.
Technik und Dokumentation zusammen-denken	SBOM (Software-Stückliste: eine Liste aller Softwarekomponenten im Produkt), Risikoanalyse, Tests, Nutzerinformationen und Update-Prozesse müssen schrittweise nachweisbar werden; strukturiert und priorisiert, nicht alles auf einmal.
Nicht alles ist gleich dringend	Must-haves zuerst umsetzen. Nice-to-haves bewusst als nächste Reifestufe planen. Die priorisierte Umsetzungslogik findet sich in Anlage A sowie in der Kurzstudie.

Warum das Management jetzt handeln muss

CRA-Readiness entsteht nicht als Nebenprodukt laufender Facharbeit. Sie braucht einen benannten Owner auf Leitungsebene, der Prioritäten setzt, Ressourcen freigibt und im Ernstfall eskalationsfähig ist. Ohne diese Verankerung bleibt das Thema ein Projekt ohne Mandat – fachlich gut gemeint, aber ohne die nötige Durchsetzungskraft. Zudem gelten Meldepflichten bereits ab 11. September 2026, also unabhängig vom Hauptstichtag Dezember 2027.

Quick Check: Bin ich vom CRA betroffen?

Bitte prüfen Sie die folgenden Aussagen zunächst je Produktfamilie, nicht nur auf Unternehmensebene. Auch bei reinen B2B- oder Integrationsprodukten sollte die Einordnung dokumentiert werden – sie sind nicht automatisch ausgenommen.

Prüffrage – je Produktfamilie prüfen, nicht nur auf Unternehmensebene	**Ja**	**Teils**	**Nein**
Wir bringen Hardware, Software, Firmware oder digitale Komponenten auf den EU-Markt.	❑	❑	❑
Das Produkt hat eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netzwerk.	❑	❑	❑
Unser Produkt nutzt Cloud-Dienste oder andere Datenverarbeitung „auf Distanz" (z. B. ein Server, der Daten auswertet, damit das Gerät funktioniert) – entwickelt vom Hersteller oder in seiner Verantwortung.	❑	❑	❑
Wir vertreiben das Produkt unter eigenem Namen oder eigener Marke.	❑	❑	❑
Wir integrieren Drittkomponenten oder Open-Source-Komponenten mit Sicherheitsrelevanz.	❑	❑	❑
Wir können die Marktrolle je Produkt eindeutig benennen (Hersteller/Importeur / Händler).	❑	❑	❑
Interpretation: Mehrere Antworten mit ‚Teilweise' oder ‚Nein' bedeuten nicht automatisch Nichtkonformität, sie zeigen aber, wo die Lücken sind, die das Management priorisieren und mit Ressourcen unterlegen muss. Die detaillierte Reifegradanalyse (Self-Check) für die Umsetzungsteams findet sich in Anlage A.			

Management-Agenda: Was bis wann sichergestellt sein muss

Der CRA verlangt keine vollständige Konformität von Tag eins, aber er verlangt, dass bestimmte Mindestfähigkeiten zu den jeweiligen Stichtagen belastbar vorhanden sind. Die folgende Übersicht zeigt, was die Leitungsebene bis wann sicherstellen muss.

Zeitraum	Was das Management sicherstellen muss	Priorität
Sofort	Eine Person auf Leitungsebene als CRA-Verantwortliche/n benennen (z. B. Geschäftsführer, Produktleiter). Ein kleines Kernteam einsetzen: Produktmanagement + Entwicklung + ggf. IT-Security. Konkret anfangen: Alle Produkte auflisten, bei denen Software oder Netzwerkverbindung eine Rolle spielt – das ist die Produktinventur.	Hoch
bis Sommer 2026	Öffentliche Kontaktseite für Sicherheitsmeldungen einrichten (z. B. security@meinefirma.de); CVD-Policy erstellen – das ist eine kurze Richtlinie, die beschreibt, wie Ihr Unternehmen mit gemeldeten Sicherheitslücken umgeht (Eingang bestätigen, bewerten, beheben, kommunizieren); Zuständige Person benennen; Budgets für die dringendsten Maßnahmen freigeben.	Hoch
bis 11.09.2026	Die Fähigkeit, aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle fristgerecht zu melden, muss organisatorisch verankert sein: Frühwarnung binnen 24 Stunden, Folgemeldung binnen 72 Stunden sowie Abschlussbericht nach den jeweils geltenden Fristen. Verantwortliche Person benennen, Ablauf dokumentieren.	Hoch
bis Ende 2026	SBOM-Pilot starten (SBOM = Stückliste aller Software-Komponenten Ihres Produkts, vergleichbar mit einer Zutatenliste); Lieferanten zu sicherheitsrelevanten Komponenten befragen; erste Risikobewertungen und Dokumentation für priorisierte Produkte anstoßen. Verantwortlich: Produktmanagement und Entwicklung.	Mittel-Hoch
bis 11.12.2027	Konformitäts- und Supportfähigkeit für Produkte mit digitalen Elementen sicherstellen, die ab dem 11.12.2027 neu auf dem EU-Markt bereitgestellt bzw. in Verkehr gebracht werden; bei vor dem Stichtag in Verkehr gebrachten Produkten insbesondere dann, wenn nach dem Stichtag eine wesentliche Änderung erfolgt.	Hoch

Hinweis: Die Fristen verschieben nicht den Handlungsbedarf, sondern definieren, bis wann Mindestfähigkeiten vorhanden sein müssen. Insbesondere die Meldefähigkeit ab September 2026 gilt auch für Bestandsprodukte

Vier Fragen für die Leitungsebene

	Vier Fragen, die die Geschäftsführung nach diesem Dokument klar beantworten können sollte:
1	Sind wir vom CRA betroffen und wenn ja, mit welchen Produkten und in welcher Rolle?
2	Was müssen wir bis wann sicher im Griff haben und was kann auf einer zweiten Reifestufe folgen?
3	Wo liegen unsere größten Lücken und welche davon sind vor dem September-Stichtag 2026 wirklich kritisch?
4	Welche nächsten Schritte sind fachlich sinnvoll und organisatorisch realistisch umsetzbar?

Nächste Schritte und Übergang zur operativen Umsetzung

Der sinnvollste nächste Schritt ist kein sofortiges Großprojekt, sondern ein sauber moderierter Startpunkt. Dazu werden Management und Umsetzungsteam gemeinsam aktiv:

Empfohlener erster Schritt: Moderiertes Kick-off

1. Dieses Dokument gemeinsam lesen (Geschäftsführung + Produktverantwortliche) und Betroffenheit, Zeitplan und Handlungsbedarf klären.
2. Quick Check (oben) für die wichtigsten Produktfamilien ausfüllen – am besten gemeinsam mit Produktmanagement und Entwicklung, nicht alleine.
3. Die zwei bis drei größten Baustellen benennen und direkt zuweisen: Wer ist für Produktinventur zuständig? Wer richtet die Security-Kontaktadresse ein? Wer klärt die Marktrolle?
4. Umsetzungsteam beauflagen, mit Anlage A (Reifegradanalyse, Gap-Analyse, 10 Schritte) die operative Detailarbeit aufzusetzen.

Die detaillierten Umsetzungsgrundlagen – Reifegradanalyse (Self-Check), Gap-Analyse, priorisierte 10 Schritte, Rollen- und Funktionsübersicht, Must-haves/Nice-to-haves und weiterführende Materialien – finden sich in Anlage A: Umsetzungsleitfaden für Produktverantwortliche und Teams.

Allianz Industrie 4.0 Baden-Württemberg
VDMA e. V. Baden-Württemberg
Kronenstraße 3
70173 Stuttgart

Tel.: +49 711 22801-20
E-Mail: info@i40-bw.de
Internet: www.i40-bw.de

Gefördert durch
Baden-Württemberg
Ministerium für Wirtschaft,
Handwerk und Tourismus

Mit Unterstützung von:
VDMA