

CRA SME Operating Manual

Praxisnaher Weg für kleine und mittlere Hersteller

Dokumenttyp: Praxisnaher Weg für kleine und mittlere Hersteller

Version: V1.1 · Status: Public Release · Datum: 30.07.2026

Owner: Martin Bischoff · 4T2 Solutions GmbH

Public



Dokumentkontrolle

Feld	Wert
Dokumentname	CRA SME Operating Manual
Version	V1.1
Status	Public Release
Vertraulichkeit	Public
Owner	Martin Bischoff
Publikationszweck	Publizierte Version

Inhaltsverzeichnis

Zweck.....	6
Anwendungshinweis.....	6
Änderungen gegenüber V1.0.....	6
Kennzeichnung der Regeltypen.....	7
So benutzen Sie dieses Manual.....	7
Dokumentfamilie V1.1.....	7
Management Brief.....	9
Was wirtschaftlich auf dem Spiel steht.....	9
Fünf Entscheidungen der Geschäftsleitung.....	9
Erwartetes Ergebnis nach 180 Tagen.....	9
Quick Start: 30, 90 und 180 Tage.....	10
In den ersten 30 Tagen.....	10
Bis 90 Tage.....	10
Bis 180 Tage.....	10
Einleitung.....	10
Produktsicherheit muss auch für kleinere Hersteller machbar bleiben.....	10
Die drei gesetzlichen EU-Grössenklassen.....	11
Basic, Intermediate und Advanced zeigen einen Weg.....	11
Ein Prozess für alle KMU.....	13
Sieben Modelle bilden ein Betriebssystem.....	13
So bleibt das Modell praktisch.....	13
Bestehendes nutzen, CRA gezielt ergänzen.....	14
Vier Fragen führen durch das Manual.....	14
1. Was gilt für unser Unternehmen und Produkt?.....	14
1.1 Geschäftsführung startet und schützt die Entscheidung.....	14
1.2 Welche CRA-Rolle haben wir?.....	15
1.3 Fällt unser Produkt unter den CRA?.....	16
1.4 Sind wir Kleinunternehmen, kleines oder mittleres Unternehmen?.....	17
1.5 Ist unser Produkt Standard, wichtig oder kritisch?.....	17
1.6 Welche Termine gelten?.....	18
1.7 Wo stehen wir gemäss ENISA?.....	18
1.8 Welche Risikoverstärker gelten?.....	18

1.9 Was tun wir in 30, 90 und 180 Tagen?.....	19
2. Wie bringen wir ein CRA-fähiges Produkt auf den Markt?.....	19
2.1 Produkt einmal aufnehmen und eindeutig identifizieren.....	19
2.2 Produktrisiken beurteilen.....	20
2.3 Security by Design und Security by Default umsetzen.....	21
2.4 Komponenten und Lieferanten beherrschen.....	22
2.5 Eine versionierte Software Bill of Materials erzeugen und verwenden.....	22
2.6 Komponenten- und Schwachstellenscans automatisieren.....	23
2.7 Sicherheitsprüfungen vor Release und Update durchführen.....	24
2.8 Technische Dokumentation erzeugen, nicht nachträglich zusammensuchen.....	25
2.9 Konformitätsbewertungsweg entscheiden.....	25
2.10 Ein einziges Release Gate verwenden.....	26
2.11 Serien- und Produktionskonformität erhalten.....	27
3. Wie halten wir das Produkt im Support sicher?.....	28
3.1 Supportdauer begründen und finanzieren.....	28
3.2 Erreichbaren Sicherheitskontakt betreiben.....	28
Kurze Policy für koordinierte Schwachstellenoffenlegung.....	29
3.3 Ein kleines PSIRT als Bereitschaftsfunktion organisieren.....	29
3.4 Schwachstellen entgegennehmen und entscheiden.....	29
3.5 Gesetzliche Meldung auslösen.....	30
3.6 Sicherheitsupdate entwickeln und sicher verteilen.....	32
3.7 Nutzer und Kunden verständlich informieren.....	33
3.8 Produkt halten, korrigieren, zurücknehmen oder zurückrufen.....	33
3.9 Änderungen und neue Versionen erneut beurteilen.....	34
3.10 Support kontrolliert beenden.....	34
4. Wie betreiben und verbessern wir das Modell?.....	35
4.1 Verantwortung mit wenigen Rollen abbilden.....	35
4.2 Denselben Prozess schrittweise verbessern.....	36
4.3 Daten einmal erfassen und wiederverwenden.....	36
Was muss wann gepflegt werden?.....	37
4.4 Externe Unterstützung gezielt einsetzen.....	38
4.5 Tragbare Werkzeuge auswählen.....	38
4.6 ENISA-Assessment wiederholen und wenige Massnahmen wählen.....	38
4.7 Management prüft Wirksamkeit und Ressourcen.....	39
4.8 NIS2 Supplier Assurance getrennt, aber wiederverwendbar beantworten.....	40
4.9 Rechtsstand und externe Informationen beobachten.....	40

4.10 Das Modell in erreichbaren Schritten einführen.....	41
Derselbe Ablauf bei 10, 50 und 100 Mitarbeitenden.....	42
4.11 Wissen, Kompetenz und Awareness sichern.....	42
Prozess- und Nachweis-Landkarte.....	42
Kapitel 1: Anwendbarkeit und Planung.....	44
Kapitel 2: Produkt und Release.....	45
Kapitel 3: Support und Schwachstellen.....	46
Kapitel 4: Betrieb und Verbesserung.....	47
Arbeitsvorlagen und Anhänge.....	47
Anhang A: Verbindliche Feldkataloge.....	48
A.1 Produktregister.....	48
A.2 Anwendbarkeit und Klassifikation.....	48
A.3 ENISA Assessment und Verbesserungsplan.....	49
A.4 Produktrisikobeurteilung.....	49
A.5 Komponenten-, Lieferanten- und SBOM-Nachweis.....	49
A.6 Release Gate.....	49
A.7 PSIRT- und Schwachstellenfall.....	49
A.8 Support und End of Support.....	49
A.9 Managementprüfung.....	50
A.10 Lieferantennachweis für regulierte Kunden.....	50
Anhang B: Methodischer Hintergrund.....	50
Offizielle Rechtsquellen und ihre Funktion.....	50
Umsetzungsmethoden und nicht bindende Hilfen.....	51
Glossar.....	51
Bekannte Einschränkungen.....	52
Haftungs- und Anwendungshinweis.....	54
Copyright und offene Lizenz.....	54
Transparenz zur Erstellung.....	54

Zweck

Kleine und mittlere Hersteller müssen die Anforderungen des Cyber Resilience Act (CRA) in bestehende Produkt-, Entwicklungs-, Release- und Supportprozesse integrieren, ohne eine zusätzliche Konzernorganisation aufzubauen. Der CRA verlangt keine kopierte Grossunternehmensstruktur, wohl aber wirksame Produktentscheidungen: sichere Entwicklung, beherrschte Komponenten, nachvollziehbare Freigaben, erreichbare Schwachstellenbehandlung und finanzierbaren Support.

Es beschreibt einen gemeinsamen Mindestprozess für Kleinstunternehmen sowie kleine und mittlere Hersteller. Rollenbündelung ist zulässig. Umfang und Tiefe von Rollentrennung, Kontrollen, Prüfungen und Automatisierung wachsen jedoch mit Produktkomplexität, Portfolio, Exposition und Risiko. Basic ist kein pauschales Zielmodell für einen Hersteller mit komplexem oder risikoreichem Portfolio.

Der Mindestprozess ist ein verbundenes Betriebssystem, keine Sammlung unabhängiger Checklisten. Anwendungsbereich und Rolle eröffnen den Produktweg. Produktisiko steuert Sicherheitsanforderungen, Komponentenentscheide, Tests und Release. Support, Schwachstellen, Änderungen und neue Rechtsquellen können frühere Entscheide wieder öffnen. Die Geschäftsführung stellt dafür Ressourcen bereit und entscheidet über wesentliche Risiken und Marktfolgen; sie kann Herstellerverantwortung nicht an eine Fachperson, einen Importeur oder einen Dienstleister übertragen.

Anwendungshinweis

Dieses Manual ist keine Rechtsberatung und keine Produktkonformitätserklärung. Ein Unternehmen muss Anwendbarkeit, Rolle, Produktklasse und Konformitätsweg für das reale Produkt entscheiden. Der Cyber Resilience Act und die anwendbaren offiziellen Rechtsakte sind verbindlich.

Rechts- und Informationsstand: 30. Juli 2026. Normenstatus, Plattformzugang, ergänzende Rechtsakte und offizielle Umsetzungshinweise sind vor jeder produktbezogenen Entscheidung erneut zu prüfen.

Änderungen gegenüber V1.0

V1.1 verbessert Verständlichkeit und praktische Anwendung, ohne die Kontrollarchitektur zu verändern. Die bisherige unklare Sammelbezeichnung für Prozessangaben wurde durch einheitliche Prozessübersichten ersetzt. Missverständliche Rollenformulierungen und vermeidbare Anglizismen wurden präzisiert. Drei zentrale Entscheidungswege werden zusätzlich als Arbeitsdiagramme dargestellt. Die Meldebereitschaft wurde mit den veröffentlichten Betriebsinformationen zur Single Reporting Platform vom 17. Juli 2026 abgeglichen. Ein beobachteter repräsentativer KMU-Anwendertest bleibt eine nachgelagerte Wirksamkeitsmassnahme.

Kennzeichnung der Regeltypen

Kennzeichnung	Bedeutung
CRA-Pflicht	unmittelbar aus der Verordnung oder einem anwendbaren Rechtsakt abgeleitete Anforderung
Empfohlene Mindestkontrolle	praktikabler Umsetzungsweg dieser Dokumentfamilie; nicht wörtlich gesetzlich vorgeschrieben
Risikobasierte Vertiefung	zusätzliche Tiefe aufgrund von Produkt, Exposition, Komplexität oder Befund
Unternehmensentscheidung	bewusst strengere interne Regel oder gewählte Kontrollarchitektur

Fehlt eine Kennzeichnung im Fliesstext, führen Rechtsanker und Quellenliste die rechtliche Einordnung. Interne Steuerungsregeln dürfen nicht als behördlich anerkannte CRA-Methode dargestellt werden.

So benutzen Sie dieses Manual

Beginnen Sie mit Kapitel 1 und öffnen Sie nur den Arbeitsbereich, den Ihr nächster Entscheid benötigt. Jedes Kapitel nennt sein Ergebnis. Die Prozesslandkarte zeigt Verantwortung, Stellvertretung, Freigabesperre und Rechtsanker. Die Feldkataloge des Operating Kits werden in vorhandenen Produkt-, Ticket-, Build-, Release- oder Dokumentationssystemen umgesetzt; sie verlangen keine neue zentrale Anwendung.

1. Produkt oder Produktversion über die stabile Produkt-ID auswählen.
2. anstehende Entscheidung und zugehörigen Arbeitsbereich bestimmen.
3. nur die Pflichtfelder und Nachweise dieses Arbeitsbereichs aktualisieren.
4. Freigabe, Freigabesperre oder Marktbereitstellungsstopp dokumentieren.
5. Ergebnis über stabile IDs mit Risiko, SBOM, Fall und Release verbinden.

Dokumentfamilie V1.1

Bestandteil	Funktion	Status
CRA SME Operating Manual V1.1	führender Umsetzungsweg innerhalb dieser Dokumentfamilie	Prozess und Entscheidungsregeln
CRA SME Starter Toolkit V1.1	Referenz-PDF, Starter Workbook und Feldkatalog	bei Anwendung dieses Modells methodisch erforderliche Mindestfelder
ENISA CRA Maturity Model Reifegradbewertung und Verbesserungsplan Tool		offizielles nicht bindendes Originalwerkzeug
Family Manifest	Versionen, Quellen, Gates und kompatible Ausgaben	technische Familiensteuerung

Manual und Toolkit werden gemeinsam versioniert. Eine Vorlage ist nur vollständig, wenn ihre Versionsnummer zur Manual-Version passt. Bestehende Systeme dürfen das Format ersetzen, müssen aber die als Muss bezeichneten Felder, Entscheide und Nachweise erhalten.

Das Starter Workbook ist ein zeitlich begrenztes Onboarding-, Lern- und Migrationswerkzeug für ein Pilotprodukt oder ein kleines Portfolio. Bei ungefähr zehn Produkten, hoher Release-Frequenz, vielen n:m-Beziehungen oder paralleler Fallarbeit werden die kontrollierten Felder in führende Systeme wie Jira, Git, CI/CD, DMS oder Service Desk übertragen. Das Workbook darf dann weder ein Schattenregister noch die führende Portfoliosteuerung bilden.

Vom verbindlichen Recht zur täglichen Produktarbeit

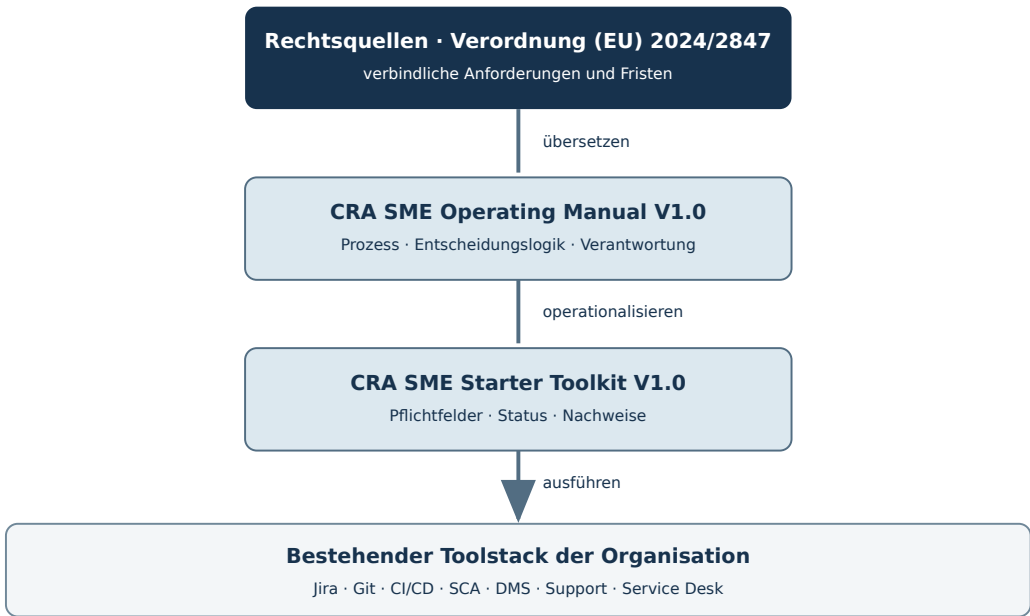


Abbildung 1 – Rechtsquellen führen die Aussage, Manual und Toolkit übersetzen sie in den bestehenden Toolstack.

Rechtsquelle	Manual	Starter Toolkit	ENISA-Werkzeug
bestimmt die rechtliche Aussage	erklärt Entscheidung, Verantwortung und Eskalation	führt Status, Pflichtfelder und Nachweise	bewertet Reifegrad und priorisiert Verbesserungen

Abbildung 2 – Manual, Toolkit, Rechtsquellen und Reifegradwerkzeug haben unterschiedliche Aufgaben. Rechtsquellen führen die rechtliche Aussage. Das Manual erklärt, das Toolkit dokumentiert, und ENISA unterstützt die Verbesserung, ohne Konformität zu beweisen.

Die methodischen Grundlagen für Leserführung und Prozessdarstellung stehen im Anhang.

Management Brief

Was wirtschaftlich auf dem Spiel steht

Der CRA verbindet Produktsicherheit mit Marktzugang und der Fähigkeit, Produkte weiterhin bereitzustellen. Fehlende Produktkenntnis, nicht beherrschte Komponenten, unzureichende Release-Nachweise oder ein nicht tragfähiger Supportweg können Releases verzögern, Marktbereitstellung stoppen, Nachrüstung verteuern und Rücknahme- oder Rückrufentscheide auslösen. Supportdauer, Signierschlüssel, Buildfähigkeit, Lieferantenabhängigkeiten und Schwachstellenbereitschaft sind deshalb auch Finanzierungs- und Portfoliofragen.

Fünf Entscheidungen der Geschäftsleitung

1. Wer verantwortet den CRA-Pfad und wer übernimmt die Stellvertretung?
2. Welche Produkte und Marktwege werden zuerst betrachtet?
3. Welche Risiken oder fehlenden Fähigkeiten stoppen Release oder Marktbereitstellung?
4. Wie lange kann jedes Produkt technisch und finanziell unterstützt werden?
5. Welche Kompetenzen werden intern aufgebaut und welche extern bezogen?

Erwartetes Ergebnis nach 180 Tagen

Ergebnis	Erkennbarer Zustand
kontrollierter Release	Produkt, Risiko, SBOM, Tests, Dokumentation und Entscheid sind verbunden
erreichbarer Schwachstellenprozess	Kontakt, Triage, Meldeweg und Stellvertretung sind getestet
nachvollziehbare Produktakte	eine Product ID führt zu den aktuellen Nachweisen
finanzierte Supportfähigkeit	Personal, Build, Schlüssel, Tests und Kommunikation sind tragfähig
entscheidungsfähiges Management	wesentliche Befunde enden mit Entscheid, Owner, Termin und Abnahmekriterium

Quick Start: 30, 90 und 180 Tage

Der Einstieg priorisiert Handlungsfähigkeit vor Vollausbau. Ein kleiner Hersteller darf Abläufe zunächst einfach halten, solange gesetzliche Fristen, Releaseblocker und wesentliche Produktrisiken nicht verschoben werden.

In den ersten 30 Tagen

- Produkte, Versionen, Product Owner und Stellvertretung bestimmen;
- Scope, Wirtschaftsakteurrolle und EU-Marktweg klären;
- erreichbaren Sicherheitskontakt und Meldebereitschaft einrichten;
- den nächsten relevanten Release als Pilot auswählen;
- kritische Blocker, Supportlücken und externe Fachbedarfe erfassen.

Ergebnis nach 30 Tagen: Verantwortliche, Pilotprodukt und dringende Blocker sind sichtbar.

Bis 90 Tage

- Produktrisiko und Release Gate für das Pilotprodukt anwenden;
- erste produktbezogene SBOM erzeugen und prüfen;
- Schwachstellenfunde triagieren und mit der Produktversion verbinden;
- PSIRT- und Meldeweg praktisch üben;
- Geschäftsleitung über Ressourcen und offene Sperren entscheiden lassen.

Ergebnis nach 90 Tagen: Das Pilotprodukt besitzt einen kontrollierten Release- und Schwachstellenweg.

Bis 180 Tage

- technische Dokumentation und Konformitätsweg vervollständigen;
- Support-, Update-, Build-, Signier- und Wiederherstellungsfähigkeit bestätigen;
- wiederholbare Reviews, Regulatory Watch und Revalidierung betreiben;
- Pilotbefunde auf das Portfolio übertragen, ohne unnötige Parallelregister zu bauen.

Einleitung

Produktsicherheit muss auch für kleinere Hersteller machbar bleiben

Der Cyber Resilience Act wirkt auf viele kleine Unternehmen zunächst kaum umsetzbar. Die Pflichten betreffen Risiken, Entwicklung, Komponenten, technische Dokumentation, Schwachstellen, Meldungen, Updates und die gesamte Supportdauer. Ein Unternehmen mit zehn oder zwanzig Mitarbeitenden kann dafür keine verkleinerte Rechts-, Compliance-, Qualitäts- und Product-Security-Organisation eines Grossunternehmens aufbauen.

Grosse Hersteller beginnen häufig nicht bei null. Andere Regulierungen, komplexe Lieferketten, Markterwartungen und langjährige Qualitätsanforderungen haben sie bereits zu formalen Freigaben, Wartungsprozessen, Lieferantenkontrollen und spezialisierten Rollen gezwungen. Dieser Vorsprung kann zu einer Markthürde für kleinere Anbieter werden. Er bedeutet aber nicht, dass ein kleines

Unternehmen dieselbe Organisation kopieren muss.

Der KMU-Weg verfolgt deshalb ein anderes Ziel: gleiche erforderliche Produktsicherheitswirkung mit einem einfacheren, nachvollziehbaren Betrieb. Rollen dürfen gebündelt, Register gemeinsam geführt und Fachleistungen gezielt extern bezogen werden. Verantwortung, Stellvertretung, Entscheidung und Nachweis müssen trotzdem sichtbar bleiben.

Die drei gesetzlichen EU-Grössenklassen

Die Aufteilung Kleinst, klein und mittel stammt aus der EU-Definition für kleine und mittlere Unternehmen (KMU) und wird auch von der Agentur der Europäischen Union für Cybersicherheit (ENISA) verwendet. Sie ist keine gesetzlich vorgeschriebene CRA-Prozessstruktur.

EU-Kategorie	Mitarbeitende	Finanzielle Grenze
Kleinstunternehmen	weniger als 10	höchstens EUR 2 Mio. Jahresumsatz und/oder Bilanzsumme
Kleines Unternehmen	weniger als 50	höchstens EUR 10 Mio. Jahresumsatz und/oder Bilanzsumme
Mittleres Unternehmen	weniger als 250	höchstens EUR 50 Mio. Jahresumsatz und/oder EUR 43 Mio. Bilanzsumme

Partnerunternehmen und verbundene Unternehmen können die Berechnung verändern. Die Mitarbeitendenzahl allein ist deshalb nicht immer ausreichend. Die Grössenklasse ist insbesondere für Unterstützungsangebote und das vorgesehene vereinfachte Format der technischen Dokumentation für Kleinst- und kleine Unternehmen relevant. Sie reduziert nicht das erforderliche Cybersicherheitsniveau des Produkts.

Die Definition stammt zwar aus dem Jahr 2003, ist für den CRA aber keine historische Hintergrundquelle. Artikel 3 Nummer 19 CRA verweist ausdrücklich auf den Anhang der Empfehlung 2003/361/EG. Die Erwägungsgründe 4 und 5 verlangen, diesen Anhang einschliesslich der Regeln für Partnerunternehmen und verbundene Unternehmen vollständig anzuwenden. Der CRA von 2024 macht diese Definition damit zur aktuellen Referenz für seine KMU-Begriffe.¹

Offizielle Grundlagen:

- [Cyber Resilience Act](#), insbesondere Artikel 3 Nummer 19, Artikel 26 und 33 sowie die Erwägungsgründe 4 und 5;
- [Empfehlung 2003/361/EG](#), Anhang, ausschliesslich als vom CRA ausdrücklich einbezogene KMU-Definition.

Basic, Intermediate und Advanced zeigen einen Weg

Das ENISA-Excel bewertet 25 Fragen in fünf Domänen. Jede Frage verwendet fünf Antwortstufen. Für den Verbesserungsplan fasst ENISA die Ergebnisse in drei Bänder:

¹ Verordnung (EU) 2024/2847, Artikel 3 Nummer 19 sowie Erwägungsgründe 4 und 5; Anhang der Empfehlung 2003/361/EG.

ENISA-Band	Wert	Arbeitsbedeutung
Basic	1,0 bis 2,5	Verantwortung und einen tragfähigen Mindestablauf herstellen
Intermediate	2,6 bis 3,9	den Ablauf dokumentieren, wiederholen und konsistent anwenden
Advanced	4,0 bis 5,0	Wirksamkeit messen, gezielt steuern und fortlaufend verbessern

Dieser Weg folgt einer aus Produktion, Softwareentwicklung und Qualitätsmanagement bekannten Reifegradidee. Auch Modelle wie Capability Maturity Model Integration (CMMI) beschreiben Entwicklung nicht als einmaliges Grossprojekt, sondern als stufenweisen Aufbau: von reaktiver Arbeit über beherrschte und definierte Abläufe bis zu Messung und kontinuierlicher Verbesserung. CMMI ist hier nur eine verständliche Analogie. Dieses Manual übernimmt weder das CMMI-Modell noch dessen Appraisal- oder Zertifizierungslogik.

Der praktische Grundsatz lautet:

Zuerst zuverlässig handeln. Dann wiederholbar arbeiten. Danach messen und verbessern.

Ein Unternehmen soll nicht alles gleichzeitig perfektionieren. ENISA empfiehlt, mit dem aktuellen Reifegrad zu beginnen, wenige Massnahmen für die nächsten drei bis sechs Monate auszuwählen und besonders risikoreiche Lücken zuerst zu schliessen.

Das bedeutet nicht, dass gesetzliche Pflichten bis zu einem höheren Reifegrad warten dürfen. Ein Unternehmen mit Basic muss beispielsweise eine fällige Meldung trotzdem fristgerecht einreichen. Es darf den Meldeprozess zunächst einfach organisieren: benannte Personen, Stellvertretung, kurze Entscheidungshilfe und getesteter Zugang.

Reifegrad und Konformität beantworten unterschiedliche Fragen. Basic kann für ein überschaubares Produkt rechtlich vollständig sein, wenn alle anwendbaren Pflichten wirksam erfüllt und nachgewiesen sind. Advanced kann dagegen nicht konform sein, wenn auch nur eine notwendige Produktentscheidung, Massnahme oder Nachweis fehlt.

Unternehmensgrösse	ENISA-Reifegrad	Produktrisiko
bestimmt begrenzte rechtliche oder organisatorische Folgen	zeigt, wie stabil der Prozess arbeitet	bestimmt notwendige Kontroll- und Prüftiefe
entfernt keine anwendbare Pflicht	beweist keine Konformität	wirkt unabhängig von Grösse und Reifegrad

Abbildung 3 – Unternehmensgrösse, Reifegrad und Produktrisiko beantworten verschiedene Fragen. Alle drei Eingaben führen in denselben Mindestprozess; nur die angemessene Umsetzungstiefe verändert sich.

Offizielle Grundlagen:

- [ENISA SME Cyber Resilience Maturity Assessment Model](#);
- originales ENISA CRA Maturity Model Tool;
- [CMMI Levels of Capability and Performance](#) als nicht normativer Vergleich.

Ein Prozess für alle KMU

Kleinst-, kleine und mittlere Unternehmen verwenden denselben Mindestprozess. Sie treffen dieselben gesetzlichen Entscheidungen und benötigen dieselben Nachweisarten. Unterschiede entstehen durch Produktanzahl, Komplexität, verfügbare Rollen, Automatisierung und Risiko, nicht automatisch durch die Mitarbeitendenzahl.

Jeder Prozess zeigt:

1. welches Ergebnis erforderlich ist;
2. welche wenigen Schritte notwendig sind;
3. wer verantwortlich ist und wer die Stellvertretung übernimmt;
4. welcher Nachweis gespeichert wird;
5. wie sich Basic zu Intermediate und Advanced entwickelt;
6. welcher Risikoverstärker zusätzliche Tiefe verlangt.

Das Manual verwendet keine verkürzte Compliance-Spur. Auch das vereinfachte Format der technischen Dokumentation verändert nur die Form des Nachweises, nicht den gemeinsamen Produktprozess oder das erforderliche Sicherheitsniveau.

Sieben Modelle bilden ein Betriebssystem

Der gemeinsame Prozess besteht aus sieben zusammenhängenden Steuerungsmodellen:

1. Scope, Rolle und Marktweg führen zu einem autorisierten Start.
2. Produktrisiko führt über Sicherheitsanforderungen und Evidence zum Release-Entscheid.
3. Komponenten und SBOM bleiben mit Build, Produktversion und Support verbunden.
4. Eine Sicherheitsinformation führt vom frühesten Kenntniszeitpunkt zu Meldung, Korrektur und Nutzerinformation.
5. Produkt-, Lieferanten-, Bedrohungs- oder Rechtsänderungen öffnen betroffene Entscheide erneut.
6. Supportfähigkeit, End of Support und Betriebseinstellung werden als ein Ressourcen- und Kontinuitätsmodell gesteuert.
7. Managementprüfung verbindet Ergebnisse mit Risiko-, Ressourcen- und Marktentscheiden.

Diese Modelle verhindern, dass ein formal abgeschlossenes Release später vom Schwachstellenprozess, von fehlender Buildfähigkeit oder von einer Rechtsänderung abgekoppelt wird. Jedes Modell benennt Eingang, Entscheidung, verantwortliche Rolle, Nachweis, Eskalation und Rücksprung.

So bleibt das Modell praktisch

Ein neuer Inhalt wird nur aufgenommen, wenn er eine anwendbare Pflicht erfüllt, eine konkrete Entscheidung ermöglicht oder wiederverwendbare Nachweis erzeugt. Zuerst wird er als Feld, Marktbereitstellungsstopp-Regel oder Verweis in einem vorhandenen Arbeitsbereich umgesetzt. Ein neues Register oder ein zusätzlicher Prozess ist nur zulässig, wenn die Aufgabe im bestehenden Ablauf nicht eindeutig ausgeführt und nachgewiesen werden kann.

Das führende Arbeitsmittel folgt der tatsächlichen Komplexität. Zuerst werden die vorhandenen Produkt-, Ticket-, Release-, Build-, Support- und Dokumentationssysteme um die fehlenden CRA-

Felder, Gates, Eskalationen und Nachweis-Links ergänzt. Ein kontrolliertes Workbook ist nur ein optionaler Starter für sehr kleine, wenig veränderliche Bestände. Eine neue Anwendung wird erst geprüft, wenn die bestehenden Werkzeuge den vollständigen CRA-Pfad nachweislich nicht tragen.

Bestehendes nutzen, CRA gezielt ergänzen

Der Standardweg lautet: bestehender Prozess, CRA-Lücke, kleine Ergänzung, verlinkte Nachweis. Das Product Register erhält CRA-Scope und Supportende. Das Ticketsystem erhält CRA-Kennzeichnung, Produktversion, Frist und Entscheid. Das Release Management erhält ein Gate für Risiko, SBOM, Triage, Tests, Dokumentation und Support. Kontinuierliche Integration und Bereitstellung (Continuous Integration and Continuous Delivery, CI/CD) erzeugt und archiviert SBOMs sowie Scanergebnisse. Security-Mailbox oder Service Desk erhalten dokumentierten Kenntniszeitpunkt, Hauptverantwortung, Stellvertretung und Eskalation. Wiki oder Dokumentenmanagementsystem (DMS) bewahren die freigegebenen technischen Nachweise.

Der CRA schreibt kein Jira, keine bestimmte Pipeline und keine zentrale Datenbank vor. Stabile IDs und Links müssen aber Produktversion, Build, SBOM, Fund, Fall, Release und Nachweis nachvollziehbar verbinden.

Im Lesetext stehen deutsche Handlungsbegriffe zuerst. Englische Bezeichnungen bleiben nur als stabile Feld-, Rollen- oder Systemnamen erhalten, wenn sie die Umsetzung in bestehenden Werkzeugen erleichtern. Die Prozesssprache verwendet Nachweis, kontrollierter Datensatz, Freigabesperre, Marktbereitstellungsstopp und Übergabe an eine Fachstelle. Release Gate bleibt als definierter Fachbegriff bestehen.

Vier Fragen führen durch das Manual

1. Was gilt für unser Unternehmen und Produkt?
2. Wie bringen wir ein CRA-fähiges Produkt auf den Markt?
3. Wie halten wir das Produkt im Support sicher?
4. Wie betreiben und verbessern wir das Modell?

1. Was gilt für unser Unternehmen und Produkt?

Am Ende dieses Kapitels liegen Unternehmensklasse, Marktrolle, Produktstatus, vorläufige Produktklasse, ENISA-Ausgangswert und ein erster Verbesserungsplan vor.

1.1 Geschäftsführung startet und schützt die Entscheidung

Die Geschäftsführung benennt eine verantwortliche Person und eine Stellvertretung. Sie legt fest, welche Produkte zuerst betrachtet werden und wer einen Release bei ungeklärter CRA-Anwendbarkeit oder einem nicht akzeptierten Produktrisiko stoppen darf.

Vorgehen:

1. Produktportfolio und nächsten geplanten Release auswählen.
2. CRA-Verantwortung und Stellvertretung schriftlich benennen.
3. Nachweis-Ablage und Produkt-ID festlegen.

4. offene Rechts-, Produkt- oder Ressourcenfragen erfassen.
5. Termin für die erste Managementprüfung festlegen.

Nachweis: Management-Startentscheid (Management Start Decision) im bestehenden Führungs- oder Ablagesystem.

Entwicklung	Sichtbares Ergebnis
Basic	Owner, Stellvertretung, Produkt und nächster Termin sind benannt
Intermediate	Entscheidung wird für alle Produkte gleich angewendet und regelmässig überprüft
Advanced	Portfolio, Risiken, Ressourcen und Wirksamkeit werden mit geeigneten Kennzahlen gesteuert

Risikoverstärker: ungeklärte Herstellerrolle, kritisches Produkt, kurzfristiger Release oder fehlende Verantwortung. In diesen Fällen bleibt der Release auf Freigabesperre.

1.2 Welche CRA-Rolle haben wir?

Ein Unternehmen entscheidet seine Rolle nach den tatsächlichen Handlungen. Eigenmarke, wesentliche Änderung oder erneute Bereitstellung können eine Herstellerrolle auslösen. Importeur, Distributor, Bevollmächtigter und Open-Source-Steward haben eigene Pflichtpfade.

Vorgehen:

1. Rechtseinheit, Produktname und EU-Marktweg erfassen.
2. Hersteller, Importeur, Distributor und weitere Rollen prüfen.
3. Eigenmarke und wesentliche Änderungen ausdrücklich beurteilen.
4. bedingte Rollenpfade nur bei tatsächlichem Trigger aktivieren.
5. unklare Rollenentscheidung an Legal oder eine geeignete externe Fachperson übergeben.

Ein Schweizer Hersteller hält zusätzlich fest, über welchen Lieferweg das Produkt den EU-Markt erreicht, welcher Wirtschaftsakteur in der EU eingebunden ist und welcher operative Meldeweg gilt. Diese Entscheidung folgt den tatsächlichen Rollen und der Lieferkette. Das Manual unterstellt deshalb nicht pauschal, dass immer ein Bevollmächtigter oder immer ein Importeur erforderlich ist. Solange Marktweg und Rolle ungeklärt sind, bleibt die EU-Marktbereitstellung auf Freigabesperre.

Die operative Schnittstelle zum EU-Wirtschaftsakteur enthält mindestens Rechtseinheit, Rolle, Produkte, Kontakt und Stellvertretung, Pflichtunterlagen, Zugriff auf EU-Konformitätserklärung und technische Dokumentation, Melde- und Behördenweg, Reaktionszeit, Änderungsmitteilung und Ende der Zusammenarbeit. Importeur und Distributor bestätigen ihre CRA-Prüfpflichten im eigenen Verantwortungsbereich. Das Manual baut dafür keinen vollständigen Parallelprozess auf; fehlende Bestätigung oder Erreichbarkeit sperrt den EU-Marktweg.

Nachweis: Entscheid zur Wirtschaftsakteurrolle (Economic Role Decision) mit Begründung, Quelle, Prüfer und Datum.

Basic dokumentiert den Entscheid pro Produkt. Intermediate verwendet eine wiederholbare Entscheidungshilfe. Advanced überwacht Rollenänderungen über das Portfolio. Die rechtliche Definition bleibt in jeder Stufe gleich.

1.3 Fällt unser Produkt unter den CRA?

Der Hersteller bestimmt die Grenze des Produkts mit digitalen Elementen einschliesslich Software, Hardware und relevanter Remote-Datenverarbeitung. Ausnahmen werden nicht pauschal, sondern anhand ihrer Voraussetzungen entschieden.

Vorgehen:

1. Produkt, Version, Funktionen, Schnittstellen und Remote-Dienste beschreiben.
2. Bereitstellung im Rahmen einer gewerblichen Tätigkeit, entgeltlich oder unentgeltlich, sowie den Bezug zum EU-Markt prüfen.
3. geltend gemachte Ausnahme mit offizieller Fundstelle begründen.
4. Open-Source-Komponenten von der kommerziellen Bereitstellung des Gesamtprodukts unterscheiden.
5. Scope-Entscheidung genehmigen oder zur Klärung sperren.

Für Produkte im Anwendungsbereich der Verordnung (EU) № 168/2013 wird zusätzlich die begrenzte Ausnahme der Delegierten Verordnung (EU) 2025/1535 geprüft. Die Ausnahme wird nicht auf andere Fahrzeuge, Komponenten oder Produktgruppen übertragen.²

Für bestimmte Funkanlagen gilt bis zum Regimewechsel zusätzlich die RED-Cybersicherheitsregelung. Die Delegierte Verordnung (EU) 2026/339 hebt die Delegierte Verordnung (EU) 2022/30 mit Wirkung vom 11. Dezember 2027 auf. Der Grund ist, dass die grundlegenden CRA-Anforderungen ab diesem Datum dieselben horizontalen Cybersicherheitsbereiche abdecken und eine parallele Doppelregelung vermieden werden soll. Funkanlagen, die vom 1. August 2025 bis zum 10. Dezember 2027 in Verkehr gebracht werden und unter die Delegierte Verordnung (EU) 2022/30 fallen, bleiben für diesen Zeitraum der entsprechenden RED-Marktüberwachung unterstellt. Der Regulatory Watch dokumentiert deshalb Inverkehrbringungsdatum, anwendbares Regime und Übergangsentscheid.³

Nachweis: Anwendbarkeitsentscheid (Product Applicability Decision) und gegebenenfalls Exclusion Decision.

Risikoverstärker: Remote-Datenverarbeitung, Plattformprodukt, komplexe Integration, freie und quelloffene Software mit kommerziellem Kontext oder unklare Ausnahme.

2 Delegierte Verordnung (EU) 2025/1535. Die Ausnahme gilt nur innerhalb ihres definierten Produkt- und Rechtsbereichs.

3 Delegierte Verordnung (EU) 2026/339, insbesondere Erwägungsgründe 3 bis 5 und Artikel 1. Die Aufhebung der Delegierten Verordnung (EU) 2022/30 wirkt ab 11. Dezember 2027; die Marktüberwachung für zuvor erfasste Funkanlagen bleibt unberührt.

Scope-Hinweis	Nächster Entscheid
freie und quelloffene Software	kommerzielle Tätigkeit, Monetarisierung und Rolle des Herstellers oder Open-Source-Stewards prüfen
Remote-Datenverarbeitung	prüfen, ob sie für eine Produktfunktion notwendig ist und in der Herstellerverantwortung liegt
Medizinprodukt, Fahrzeug, Luftfahrt- oder Marineprodukt	konkrete sektorale Ausnahme und Produktgrenze anhand der aktuellen amtlichen Rechtsquelle prüfen
bestimmte Funkanlage	bis 10. Dezember 2027 RED-Übergangsregime und danach CRA-Regime dokumentieren

Die Tabelle ist ein Triage-Einstieg. Ein behaupteter Ausschluss benötigt immer eine produktbezogene Begründung und Fundstelle.

1.4 Sind wir Kleinstunternehmen, kleines oder mittleres Unternehmen?

Das Unternehmen wendet gemäss Artikel 3 Nummer 19 und Erwägungsgrund 5 CRA den Anhang der Empfehlung 2003/361/EG vollständig an. Es erfasst Mitarbeitende, Jahresumsatz, Bilanzsumme sowie relevante Partner- und verbundene Unternehmen. Die genehmigte Einstufung wird jährlich und bei strukturellen Änderungen erneut geprüft.

Nachweis: KMU-Klassifikationsdatensatz mit Bezugsjahr und Berechnungsgrundlage.

Die Einstufung erzeugt keine andere Prozessvariante. Sie zeigt, welche Unterstützungsmassnahmen oder vereinfachten Dokumentationsformen genutzt werden dürfen.

1.5 Ist unser Produkt Standard, wichtig oder kritisch?

Die Produktklasse steuert den zulässigen Konformitätsbewertungsweg. Das Unternehmen prüft Anhang III, Anhang IV und die verbindlichen technischen Beschreibungen. Eine Marketingbezeichnung oder ein ähnliches Produkt ersetzt diese Prüfung nicht.

Vorgehen:

1. Kernfunktion und bestimmungsgemässe Verwendung beschreiben.
2. sonstiges, wichtiges Klasse I, wichtiges Klasse II oder kritisches Produkt prüfen.
3. verbindliche Produktbeschreibung und aktuelle Rechtsquelle speichern.
4. vorläufigen Konformitätsweg bestimmen.
5. Klassifikation bei wesentlicher Änderung erneut öffnen.

Nachweis: Product Klassenentscheid.

Produkt und EU-Marktweg definiert	Rolle und CRA-Scope entschieden	Kategorie, Termine und Fachübergaben geschlossen	autorisierter Start
fehlt eine eindeutige Produktgrenze, bleibt der Weg gesperrt	Unklarheit führt zur Fachübergabe	offener Sektor- oder Konformitätsentscheid blockiert	Management bestätigt Owner, Ressourcen und nächsten Schritt

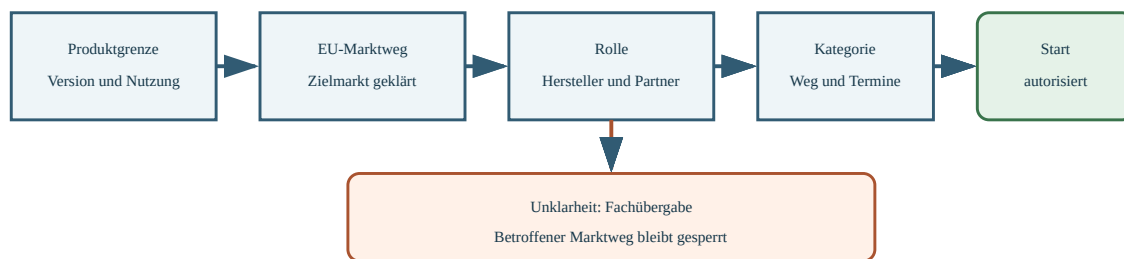


Abbildung 4 – Der Produktweg beginnt erst nach einem begründeten Entscheid über Anwendungsbereich und Rolle.

Jede ungeklärte Stufe führt zur Freigabesperre und kontrollierten Fachübergabe.

Risikoverstärker: möglicher Treffer in Anhang III oder IV, sicherheitskritische Kernfunktion, privilegierter Zugang oder verpflichtende Drittbewertung.

1.6 Welche Termine gelten?

Das Unternehmen führt eine Produktzeitachse. Sie enthält mindestens die Anwendung der Meldepflichten ab 11. September 2026, die allgemeine CRA-Anwendung ab 11. Dezember 2027,⁴ produktbezogene Release-Termine, Supportdauer und interne Vorlaufzeiten.

Nachweis: Produkt-Konformitätszeitplan (Product Konformitätszeitplan). Regulatory Watch bestätigt den Rechtsstand vor jeder verbindlichen Terminentscheidung.

1.7 Wo stehen wir gemäss ENISA?

Das Unternehmen verwendet das originale ENISA-Excel. Es legt Produkt- und Organisationsscope, Assessment-Datum und verantwortliche Personen fest. Antworten stützen sich auf vorhandene Nachweis und nicht auf Absichten.

Vorgehen:

1. alle 25 Fragen beantworten;
2. fehlende Nachweis sichtbar kennzeichnen;
3. Basic, Intermediate oder Advanced übernehmen;
4. besonders niedrige Domänen und gesetzlich dringende Lücken bestimmen;
5. das unveränderte Assessment archivieren.

Nachweis: ENISA CRA Maturity Model Tool mit Assessment Scope und Datum.

1.8 Welche Risikoverstärker gelten?

Ein Risikoverstärker verlangt zusätzliche Tiefe, auch wenn das Unternehmen klein oder sein ENISA-Wert Basic ist. Relevante Auslöser sind unter anderem:

- wichtiges oder kritisches Produkt;

⁴ Verordnung (EU) 2024/2847, Artikel 71: Kapitel IV gilt seit 11. Juni 2026, Artikel 14 ab 11. September 2026 und die Verordnung im Übrigen ab 11. Dezember 2027.

- hohe Schadenswirkung oder privilegierter Zugang;
- starke Internetexposition;
- lange Supportdauer oder viele Produktvarianten;
- komplexe Lieferkette;
- wiederholte Schwachstellen oder Vorfälle;
- Drittbewertung;
- wesentliche Änderung;
- erhöhte vertragliche Kundenanforderungen;
- ungeklärter Drittstaat-EU-Marktweg oder EU-Wirtschaftsakteur.

Nachweis: Risikoverstärker-Entscheid (Risk Override Decision) mit Wirkung auf Prüfung, Review, Rollen und Freigabe.

1.9 Was tun wir in 30, 90 und 180 Tagen?

Der Verbesserungsplan begrenzt gleichzeitig aktive Massnahmen. Gesetzlich fällige und hochriskante Lücken kommen zuerst.

Zeitraum	Typisches Ergebnis
30 Tage	Produkte, Rollen, Kontakt, ENISA-Ausgangswert und akute Blocker sind bekannt
90 Tage	Risikobeurteilung, Start der Software Bill of Materials (SBOM), Release Gate und Product-Security-Incident-Response-Bereitschaft funktionieren
180 Tage	technische Dokumentation, Supportprozess und wiederholbare Reviews sind etabliert

Jede Massnahme hat Owner, Termin, Ergebnis, Nachweis und Abnahmekriterium. Ein langer Wunschzettel ohne Priorisierung ist kein Verbesserungsplan.

2. Wie bringen wir ein CRA-fähiges Produkt auf den Markt?

Am Ende dieses Kapitels liegt ein dokumentierter Release-Entscheid vor. Risiken, Komponenten, Sicherheitsanforderungen, Tests, technische Dokumentation und Konformitätsweg sind nachvollziehbar verbunden.

2.1 Produkt einmal aufnehmen und eindeutig identifizieren

Prozessübersicht

Auslöser	Verantwortlich	Stellvertretung	Ergebnis	Freigabesperre
neues Produkt, neue Version oder wesentliche Änderung	Product Owner	Quality/ Compliance	eindeutig identifizierte Produktversion	keine Freigabe ohne Product ID

Das Product Register ist der gemeinsame Einstieg. Es identifiziert die konkrete Produktversion, ihre Verantwortung und ihren aktuellen Lebenszyklusstatus. Die vollständigen Pflichtfelder stehen in der Product-Register-Vorlage oder im bestehenden Produktsystem. Andere Arbeitsbereiche referenzieren die Product ID, statt Stammdaten erneut zu erfassen.

Basic kann eine kontrollierte Tabelle verwenden. Intermediate führt definierte Pflichtfelder und Änderungsregeln. Advanced verbindet Portfolio, Build-, SBOM- und Fallinformationen technisch, ohne neue Schattenregister zu erzeugen.

Nachweis: genehmigter Produktregister.

2.2 Produktrisiken beurteilen

Die Risikobeurteilung betrachtet das reale Produkt, seine Verwendung und den gesamten Lebenszyklus. Eine allgemeine Unternehmensrisikoliste genügt nicht.

Vorgehen:

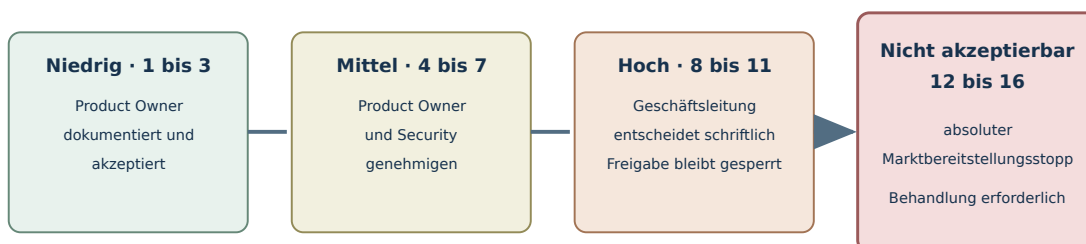
1. Produktgrenze, Nutzung, Nutzer und Betriebsumgebung bestätigen.
2. Schutzgüter, Bedrohungen, Fehlgebrauch und mögliche Auswirkungen bestimmen.
3. bestehende und geplante Sicherheitsmassnahmen zuordnen.
4. verbleibendes Risiko und notwendige weitere Behandlung entscheiden.
5. Ergebnisse in Design, Komponentenwahl, Tests, Nutzerinformation und Support überführen.
6. bei Änderungen, neuen Bedrohungen oder Schwachstellen aktualisieren.

Nachweis: Product Cybersecurity Risk Assessment mit Risk Owner und Genehmigung.

Das KMU verwendet eine einfache, begründbare Vierer-Skala. Eintrittswahrscheinlichkeit und Schadensauswirkung werden jeweils von 1 bis 4 bewertet. Das Produkt beider Werte ergibt die Ausgangs- und nach Massnahmen die Restrisikoklasse:

Wert	Klasse	Entscheidungsregel
1 bis 3	niedrig	Product Owner darf mit dokumentierter Begründung akzeptieren
4 bis 7	mittel	Product Owner und Security genehmigen Behandlung und Termin
8 bis 11	hoch	Freigabesperre bis Behandlung oder schriftlichem Entscheid der Geschäftsführung
12 bis 16	nicht akzeptierbar	keine Marktbereitstellung; Behandlung oder Produktänderung erforderlich

Produktrisiko bestimmt Befugnis und Sperrwirkung



Grundregel: Mit dem Risiko steigt die Entscheidungsebene. Nicht akzeptierbare Risiken sind nicht freigabefähig.

Abbildung 5 – Mit steigendem Produktrisiko steigen Entscheidungsbefugnis und Sperrwirkung.

Die Zahlen ersetzen keine fachliche Begründung. Ein gesetzlicher Verstoß, eine bekannte aktiv ausgenutzte Schwachstelle ohne wirksame Massnahme oder eine nicht erfüllte anwendbare Produkteigenschaft bleibt unabhängig vom Zahlenwert ein Marktbereitstellungsstopp-Kriterium. Die Skala ist eine interne Entscheidungshilfe. Der CRA schreibt weder diese Bewertungsmethode noch diese Schwellenwerte vor. Restrisiken ab Klasse hoch dürfen nur die Geschäftsführung gemeinsam mit Product Owner und Security akzeptieren; nicht akzeptierbare Risiken dürfen nicht akzeptiert werden.

Stufe	Wahrscheinlichkeit	Auswirkung
1	unter realistischen Bedingungen kaum zu erwarten	geringe, lokal begrenzte Beeinträchtigung ohne wichtige Daten oder Funktionen
2	möglich, aber nur mit besonderen Voraussetzungen	begrenzte Beeinträchtigung mit gut verfügbarer Wiederherstellung
3	unter der vorgesehenen Nutzung realistisch	erhebliche Beeinträchtigung wichtiger Daten, Funktionen oder mehrerer Nutzer
4	bereits beobachtet, leicht auslösbar oder sehr wahrscheinlich	Safety-Bezug, privilegierter Zugriff, systemweite Kompromittierung oder existenzielle Wirkung

Override: Auswirkung 4 führt unabhängig vom Multiplikationswert mindestens zur Klasse hoch. Bekannte ausnutzbare Schwachstellen, aktive Ausnutzung und nicht erfüllte anwendbare CRA-Anforderungen werden nicht durch die Matrix heruntergestuft.

Entwicklung	Sichtbares Ergebnis
Basic	wichtigste Risiken, Massnahmen und verbleibende Risiken sind dokumentiert
Intermediate	Risikobeurteilung steuert Design, Komponenten und Tests bei jedem Release
Advanced	Wirksamkeit und Veränderungen werden systematisch überwacht und verbessert

Risikoverstärker: hohe Schadenswirkung, komplexe Architektur, sensible Daten, privilegierter Zugriff oder unklare Bedrohungslage.

2.3 Security by Design und Security by Default umsetzen

Der Product Owner und Engineering übersetzen Risiken in prüfbare Sicherheitsanforderungen. Die Risikobeurteilung bestimmt, welche Eigenschaften aus Anhang I anwendbar sind. Die Anhang-I-Checkliste in der Arbeitsvorlage oder im bestehenden Anforderungsmanagement verbindet jede Eigenschaft mit Anforderung, Designentscheid und Test.

Vorgehen:

1. jede relevante Anhang-I-Eigenschaft als anwendbar oder begründet nicht anwendbar entscheiden;
2. daraus prüfbare Produktanforderungen ableiten;

3. Verantwortung und Testmethode festlegen;
4. sichere Standardwerte vor dem Release prüfen;
5. Abweichungen mit Risiko und Freigabe dokumentieren.

Nachweis: Risiko-Anforderungsmatrix, Design Decisions und Test Nachweis.

Basic stellt die wichtigsten Anforderungen und sicheren Voreinstellungen her. Intermediate integriert sie wiederholbar in Entwicklung und Review. Advanced verwendet gemeinsame Prinzipien, automatisierte Prüfungen und Wirksamkeitsdaten.

2.4 Komponenten und Lieferanten beherrschen

Der Hersteller bleibt für das Gesamtprodukt verantwortlich. Der Komponentenrecord im bestehenden System für Software Composition Analysis (SCA), SBOM-Verwaltung oder Komponentenmanagement hält Herkunft, Einsatz und Wartbarkeit der konkreten Version fest. Dadurch kann der Hersteller eine ungepflegte oder unbekannte Abhängigkeit vor dem Release erkennen.

Vorgehen:

1. freigegebene Quellen und Auswahlkriterien festlegen;
2. Integrität und Version bei Integration prüfen;
3. nicht unterstützte oder unbekannte Komponenten eskalieren;
4. Lieferantenzusagen und notwendige Sicherheitsinformationen dokumentieren;
5. Schwachstellen an Maintainer melden und das eigene Produktrisiko unabhängig behandeln.

Nachweis: Komponenten- und Lieferantendatensatz (Component and Supplier Record).

Risikoverstärker: nicht gepflegte Komponente, proprietäre Blackbox, privilegierte Funktion, einzelne kritische Bezugsquelle oder fehlende Updatefähigkeit.

2.5 Eine versionierte Software Bill of Materials erzeugen und verwenden

Eine Software Bill of Materials (SBOM) ist mehr als eine einmalig erzeugte Datei. Sie muss zu einer bestimmten Produktversion gehören, maschinenlesbar, auffindbar und überprüfbar sein.

KMU-Mindestprozess:

1. SBOM möglichst im reproduzierbaren Build erzeugen;
2. Produkt, Version und Erzeugungszeit zuordnen;
3. direkte und transitive Komponenten soweit technisch möglich erfassen;
4. Format und Pflichtfelder prüfen;
5. Datei unverändert mit dem Release archivieren;
6. SBOM für Schwachstellenabgleich und Behördenanfragen verfügbar halten.

Der Mindestdatensatz enthält SBOM-Format und -Version, Produkt-ID und Release-Version, Komponentennamen, Komponentenversion, Lieferant oder Herkunft, eindeutigen Komponentenbezeichner soweit verfügbar, Abhängigkeitsbeziehung, Hash soweit erzeugbar, Lizenz soweit bekannt, Erzeugungszeitpunkt und Generatorversion. Unbekannte Versionen werden nicht leer gelassen, sondern als Qualitätsfehler mit Owner und Termin geführt. Eine Betroffenheitsaussage, beispielsweise im VEX-Format, verweist auf Advisory, Produktversion,

Status, technische Begründung, Prüfer und Gültigkeitsdatum. Sie ersetzt weder SBOM noch Produktrisiko.

CycloneDX in JavaScript Object Notation (JSON) ist der erste Referenzpfad; Software Package Data Exchange (SPDX) bleibt interoperabel möglich. Die endgültige Formatwahl wird gegen den aktuellen CRA-Rechts- und Standardisierungsstand geprüft.

Entwicklung	Sichtbares Ergebnis
Basic	in der Einführung zuerst das risikoreichste oder nächste freizugebende Produkt; vor jedem CRA-relevanten Release eine maschinenlesbare SBOM für jede betroffene Produktversion
Intermediate	versionierte SBOM je Release und wiederholbare Qualitätsprüfung
Advanced	automatisierte Erzeugung, Verbrauch, Lieferantenintegration und Qualitätskennzahlen

Nachweis: archivierte SBOM, Generatorversion und SBOM Quality Check.

2.6 Komponenten- und Schwachstellenscans automatisieren

Ein Scanner liefert Hinweise, keine Freigabeentscheidung. Falsch-positive, nicht erreichbare oder für die konkrete Version irrelevante Treffer benötigen dokumentierte Triage.

Die gemeinsame Priorität verhindert unterschiedliche Begriffe in Scanner, Tickets und Release Gate:

Priorität	Praktische Bedeutung	Mindestreaktion
P1 kritisch	aktive Ausnutzung, unmittelbare schwere Wirkung oder nicht beherrschter kritischer Pfad	sofort eskalieren; Release oder Marktbereitstellung sperren; Meldeprüfung starten
P2 hoch	realistisch ausnutzbar und hohe Auswirkung, aber noch keine bestätigte aktive Ausnutzung	vor Release behandeln; Ausnahme nur befristet, begründet und mit Kompensationsmassnahme
P3 mittel	begrenzte Auswirkung oder erschwerte Ausnutzung	terminierte Behandlung und Überwachung
P4 niedrig	geringe praktische Wirkung	dokumentieren, bündeln oder begründet akzeptieren

Entscheidungsbild für die Freigabe:

Schritt 1: Priorität	Schritt 2: zulässiger Weg	Schritt 3: Release-Entscheid
P1	Betroffenheit ausschliessen oder wirksam beseitigen	bis dahin Freigabesperre oder Marktbereitstellungsstopp
P2	beheben oder eng befristete Ausnahme mit Kompensation und Fixtermin	gemeinsame Genehmigung oder Freigabesperre
P3/P4	risikobasiert behandeln, terminieren oder akzeptieren	dokumentierter Release-Entscheid

CVSS, EPSS, Lieferantenbewertung und Scanner-Severity sind Eingaben. Produktbetroffenheit, Exposition, Erreichbarkeit und Auswirkung bestimmen gemeinsam die Priorität. Vorhandene

Severity-Werte aus Komponenten- und Schwachstellenscans müssen in die Triage übernommen und auf ihre Quelle zurückgeführt werden. Sie dürfen weder verworfen noch ungeprüft in P1 bis P4 übersetzt werden. CVSS beschreibt technische Schwere, EPSS eine statistische Ausnutzungswahrscheinlichkeit; beide ersetzen weder Produktkontext noch den dokumentierten Entscheid.

Referenzpunkte:

- bei Aufnahme oder Änderung einer Abhängigkeit;
- im Merge- oder Buildprozess;
- vor dem Release;
- regelmässig während der Supportdauer;
- nach kritischer Warnung oder neuem Bedrohungswissen.

Der Triage-Datensatz im bestehenden Fall- oder Ticketsystem verbindet den Fund mit Produktversion, Komponente, Produktrisiko und Entscheid. Im Manual bleibt die Bearbeitungskette sichtbar.

Die Bearbeitung folgt einer einzigen Kette:

1. freizugebende Produktversion und zugehörige SBOM bestimmen;
2. Fund mit Komponente und Advisory abgleichen;
3. tatsächliche Betroffenheit feststellen;
4. Exposition oder technische Erreichbarkeit beurteilen;
5. Ausnutzbarkeit und mögliche Auswirkung in das Produktrisiko übernehmen;
6. Fix, weitere Analyse oder begründete Risikoakzeptanz entscheiden;
7. Ergebnis an Release Gate oder unterstützte Produktversion zurückgeben.

Nur relevante Funde werden vertieft. Das Unternehmen erstellt nicht für jede Komponente vorsorglich ein eigenes Risikodossier.

Basic kann einen kostenlosen lokalen Scanner regelmässig ausführen. Intermediate integriert den Scan in Build und Release. Advanced korreliert SBOM, Advisories, Erreichbarkeit und Bearbeitungskennzahlen.

Nachweis: Scan Report plus Vulnerability Triage-Datensatz. Ein Rohbericht allein erfüllt das Release Gate nicht.

2.7 Sicherheitsprüfungen vor Release und Update durchführen

Die Testtiefe folgt Produktrisiko, Architektur und Änderung. Der Testplan verbindet jede wesentliche Sicherheitsanforderung mit Methode, Ergebnis und Abnahmekriterium.

Mindestens prüfen:

- sichere Voreinstellungen;
- Authentisierung und Berechtigung;
- Daten- und Kommunikationsschutz;
- Update- und Rückfallmechanismus;
- Integrität von Software und Konfiguration;

- relevante Schnittstellen und Angriffsflächen;
- Behebung bekannter ausnutzbarer Schwachstellen.

Ein Test ist nur abgenommen, wenn erwartetes Ergebnis, reale Produktversion, Testumgebung, Ergebnis, Tester, Datum und verlinkter Nachweis vorliegen. P1 verhindert den Release ohne Ausnahme, bis die Betroffenheit verlässlich ausgeschlossen oder das Risiko wirksam beseitigt ist. P2 verhindert den Release, solange es nicht behoben oder durch Geschäftsführung, Produkt- und Sicherheitsverantwortung befristet, begründet, mit Kompensationsmassnahme und festem Behebungstermin genehmigt ist. P3 und P4 folgen der normalen risikobasierten Behandlung. Fehlgeschlagene anwendbare Sicherheitsanforderungen und nicht reproduzierbare Testergebnisse führen immer zu Freigabesperre.

Basic führt dokumentierte Kernprüfungen aus. Intermediate verwendet einen wiederholbaren Testplan und geeignete Automatisierung. Advanced misst Testabdeckung, Fehlermuster und Wirksamkeit. Der Product Owner entscheidet im Testplan anhand von Produktrisiko, Exposition und Änderungstiefe, ob eine unabhängige Prüfung oder ein Penetrationstest erforderlich ist. Die Entscheidung und ihr Kriterium werden im Release Gate referenziert.

Nachweis: Test Plan, Test Report und geschlossene oder genehmigte Findings.

2.8 Technische Dokumentation erzeugen, nicht nachträglich zusammensuchen

Die technische Dokumentation wird während Entwicklung und Release aufgebaut. Ein Index technische Dokumentation zeigt, ob die Unterlagen für die konkrete Produktversion vollständig und auffindbar sind. Die Anhang-VII-Checkliste in der Arbeitsvorlage oder im bestehenden Dokumentenmanagementsystem enthält die Pflichtinhalte und verweist auf die vorhandenen Release-Nachweise.

Kleinst- und kleine Unternehmen dürfen das vorgesehene vereinfachte Format erst verwenden, wenn der einschlägige Durchführungsrechtsakt und das konkrete Formular bestätigt sind. Vereinfacht bedeutet kürzer und klarer, nicht unvollständig.

Nachweis: Index technische Dokumentation mit Version, Owner, Review und Ablageorten.

2.9 Konformitätsbewertungsweg entscheiden

Die für Konformität benannte Person bestimmt den Weg anhand der bestätigten Produktklasse und des aktuellen Status harmonisierter Normen, gemeinsamer Spezifikationen oder Zertifizierungsschemata. Bei unklaren oder risikoreichen Fällen zieht sie externe Rechts- oder Konformitätsexpertise bei. Eine eigene Quality- oder Legal-Abteilung ist nicht vorausgesetzt.

Vorgehen:

1. Produktklasse bestätigen.
2. zulässige Verfahren bestimmen.
3. Voraussetzungen einer Selbstbewertung belegen.
4. erforderliche notifizierte Stelle frühzeitig einplanen.
5. Normen- und Rechtsstatus zum Entscheidungsdatum speichern.
6. Sprache, Dokumente und externe Abhängigkeiten bestätigen.

Bei wichtigen und kritischen Produkten prüft das Unternehmen ausdrücklich, ob fehlende oder nur teilweise anwendbare harmonisierte Normen, gemeinsame Spezifikationen oder einschlägige Zertifizierung den Weg über eine notifizierte Stelle auslösen. Je nach Produktklasse kommen insbesondere Modul B mit anschliessendem Modul C oder Modul H in Betracht. Modul B allein ist kein vollständiger Konformitätsweg. Fehlende Standards, Kapazität einer notifizierten Stelle, Vorlaufzeit und Kosten werden als Release-Planungsrisiko an die Geschäftsführung eskaliert.

Produktklasse	Praktische Wegentscheidung
sonstiges Produkt	Interne Kontrolle nach Modul A ist grundsätzlich möglich; anwendbare Anforderungen und gewählte Standards müssen trotzdem belegt sein.
wichtiges Produkt Klasse I	Modul A ist nur unter den Voraussetzungen von Artikel 32 Absatz 2 möglich; andernfalls Modul B mit C, Modul H oder ein dort zugelassener Zertifizierungsweg.
wichtiges Produkt Klasse II	Modul B mit C, Modul H oder ein nach Artikel 32 Absatz 3 zugelassener Zertifizierungsweg.
kritisches Produkt	Das nach Artikel 8 verlangte europäische Cybersicherheitszertifizierungsschema; solange es nicht anwendbar ist, ein Weg nach Artikel 32 Absatz 3.

Diese Tabelle ist eine Arbeitshilfe, keine produktbezogene Rechtsentscheidung. Die verantwortliche Rolle prüft Artikel 32 und den aktuellen Normen- und Zertifizierungsstand zum Entscheidungsdatum. Unklarheit führt zur Übergabe an eine Fachstelle und Freigabesperre, nicht zu einer frei gewählten Selbstbewertung.

Nachweis: Konformitätswegentscheid und Assessment Nachweis.

Kein Reifegrad und kein Scan ersetzt die Konformitätsbewertung.

2.10 Ein einziges Release Gate verwenden

Das Release Gate bündelt die notwendigen Ergebnisse. Es erzeugt genau einen Entscheid: Release, Freigabesperre oder Marktbereitstellungsstopp.

Pflichtfragen:

- Sind Scope, Rolle und Produktklasse genehmigt?
- Ist die Risikobeurteilung aktuell?
- Sind Sicherheitsanforderungen und Tests abgeschlossen?
- Gehören SBOM und Scanergebnisse zur freizugebenden Version?
- Sind kritische Findings geschlossen oder ausdrücklich blockiert?
- Sind technische Dokumentation und Konformitätsweg vollständig?
- Sind Supportdauer, Product-Security-Bereitschaft und Updatefähigkeit betriebsbereit?
- Sind Produktidentifikation, Nutzerinformation, Erklärung und CE-Kennzeichnung vorbereitet?

Basic verwendet eine kurze genehmigte Checkliste. Intermediate zieht Nachweis wiederholbar über stabile IDs zusammen. Advanced automatisiert Statussignale, behält aber einen verantwortlichen Freigabeentscheid.

Nachweis: Release Gate-Datensatz mit Entscheider, Datum, Produktversion und offenen Bedingungen.

Das Gate hält fest, ob die reguläre technische Dokumentation oder nach verbindlicher Verfügbarkeit das gesetzlich zulässige vereinfachte Format verwendet wird. Diese Wahl erzeugt weder einen Fast Track noch geringere inhaltliche Produktsicherheitspflichten.⁵

Für Nutzerinformation, EU-Konformitätserklärung und CE-Kennzeichnung gilt ein eigener Pflichtblock im Release Gate. Er bestätigt Produkt- und Herstelleridentifikation, Supportdauer, Sicherheitskontakt, sichere Installation, Nutzung, Update und Ausserbetriebnahme, erforderliche Zielmarktsprachen, genehmigte EU-Konformitätserklärung und die produktgerechte Anbringung der CE-Kennzeichnung. Fehlender Pflichtinhalt oder fehlende Sprachfassung führt zu Freigabesperre. Anhang II, Artikel 28 bis 30 sowie Anhänge V und VI CRA bilden den verbindlichen Prüfkatalog.

Der Ablauf ist kurz: Die für Konformität benannte Person erstellt den Anhang-II-Inhaltscheck, der Product Owner bestätigt Produkt und Supportangaben, Engineering bestätigt sichere Installation, Nutzung, Updates und Ausserbetriebnahme, die zuständige Freigaberolle genehmigt Zielmarktsprachen und EU-Konformitätserklärung, danach wird die CE-Kennzeichnung gemäss Produktform angebracht und als Release-Nachweis archiviert.

Die vollständige EU-Konformitätserklärung folgt Artikel 28 und Anhang V CRA. Alternativ kann dem Produkt die vereinfachte EU-Konformitätserklärung nach Artikel 13 Absatz 20 und Anhang VI beiliegen; sie enthält die genaue Internetadresse der vollständigen Erklärung. Beide Varianten werden in den erforderlichen Zielmarktsprachen bereitgestellt.

Produktisiko	Anforderungen und Design	Komponenten, Build und SBOM	Tests und Findings	Dokumentation und Konformität	Support und Release
bestimmt Behandlung	macht Behandlung prüfbar	bindet technische Realität an die Version	bestätigt oder öffnet frühere Entscheide	belegt den aktuellen Marktweg	endet in Release, Freigabesperre oder Marktstopp

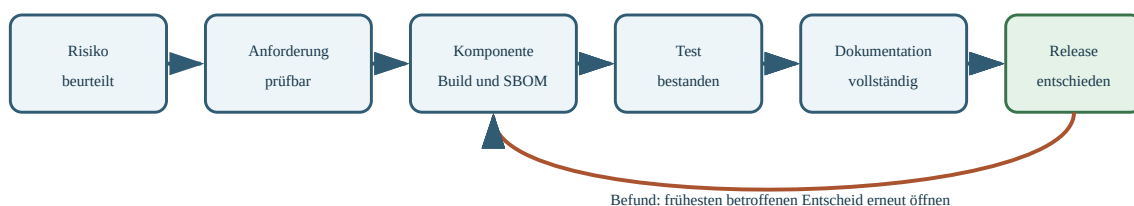


Abbildung 6 – Ein Release ist das Ergebnis einer verbundenen Nachweiskette.

Befunde, Änderungen oder fehlende Supportfähigkeit springen zum frühesten betroffenen Entscheid zurück.

2.11 Serien- und Produktionskonformität erhalten

Bei Hardware und Serienprodukten bestätigt die benannte Produktverantwortung, dass jede produzierte Einheit der bewerteten Produktversion entspricht. Änderungen an Bauteilen, Lieferanten,

⁵ Verordnung (EU) 2024/2847, Artikel 33 Absatz 5. Das vereinfachte Format betrifft die Dokumentationsform und nicht das erforderliche Produktsicherheitsniveau.

Fertigung, Design, Konfiguration, Normen oder Zertifikaten öffnen eine Impact-Prüfung und bei Bedarf Risikobeurteilung, Tests und Konformitätsweg erneut.

Muss-Felder: bewertete Version, Stücklisten- oder Buildstand, freigegebene Lieferanten, Produktionsprüfung, Abweichung, Änderungsentscheid, Prüfer und Nachweis. Eine nicht genehmigte Abweichung führt zur Freigabesperre. Diese Regel setzt Artikel 13 Absatz 14 CRA für Produkte aus einer Serie praktisch um.

Eine Abweichung wird nicht nur lokal in der Produktion behandelt. Die Impact-Prüfung benennt ausdrücklich, welche früheren Entscheide sie erneut öffnet: Produktrisiko, Sicherheitsanforderungen, Komponenten- und SBOM-Stand, Tests, technische Dokumentation, Konformitätsweg, Nutzerinformation, Support oder Release. Erst wenn alle betroffenen Gates erneut entschieden sind, darf die Variante in die Serie zurückkehren.

3. Wie halten wir das Produkt im Support sicher?

Am Ende dieses Kapitels besteht ein erreichbarer und getesteter Prozess eines Product Security Incident Response Team (PSIRT). Im KMU ist dies eine Bereitschaftsfunktion, nicht zwingend eine Abteilung. Das Unternehmen kann Schwachstellen beurteilen, Updates bereitstellen, gesetzliche Meldungen auslösen und den Support kontrolliert beenden.

3.1 Supportdauer begründen und finanzieren

Der Hersteller bestimmt die Supportdauer anhand voraussichtlicher Nutzung, Nutzererwartung, Produktart, Zweck, Betriebsumgebung, Kernkomponenten und einschlägiger offizieller Guidance. Die Dauer beträgt grundsätzlich mindestens fünf Jahre, ausser die voraussichtliche Nutzung ist kürzer.⁶

Der Entscheid muss technisch und wirtschaftlich tragfähig sein. Er umfasst Personal, Buildfähigkeit, Signierschlüssel, Komponenteninformationen, Testumgebung und Kommunikationskanäle.

Nachweis: Support Period Decision mit Annahmen, Quellen, Enddatum und Review.

Basic dokumentiert Dauer und Verantwortliche. Intermediate prüft Annahmen bei Releases und Änderungen. Advanced steuert Verpflichtungen über das Portfolio und misst Updatefähigkeit.

3.2 Erreichbaren Sicherheitskontakt betreiben

Der Hersteller veröffentlicht einen zentralen Kontaktpunkt für direkte und schnelle Kommunikation. Der Kanal darf nicht ausschliesslich automatisiert sein.

KMU-Mindestprozess:

1. überwachte Adresse oder geeignetes Portal bereitstellen;
2. primäre Rolle und Stellvertretung benennen;
3. Eingänge bestätigen und im Fallregister erfassen;
4. vertrauliche Kommunikation ermöglichen;

⁶ Verordnung (EU) 2024/2847, Artikel 13 Absätze 8 bis 10. Die Supportdauer beträgt grundsätzlich mindestens fünf Jahre, ausser die voraussichtliche Nutzung ist kürzer.

5. Kanal regelmässig testen.

Der Eingang wird so organisiert, dass ein potenziell meldepflichtiger Fall ohne vermeidbare Verzögerung erkannt, mit einem dokumentierten Kenntniszeitpunkt versehen und eskaliert werden kann. Dazu gehören eine Abwesenheits- und Wochenendregelung. Eine permanente interne 24/7-Spezialfunktion ist damit nicht vorausgesetzt.

Nachweis: Contact Point-Datensatz und Testnachweis.

Kurze Policy für koordinierte Schwachstellenoffenlegung

Die veröffentlichte Policy nennt Sicherheitskontakt, erwartete Mindestangaben, zulässige Testgrenzen, sicheren Übermittlungsweg, Eingangsbestätigung, Vertraulichkeit, Statusrückmeldung und Grundsätze der koordinierten Veröffentlichung. Sie verspricht keine Prämie und keinen starren Veröffentlichungstermin, wenn das Unternehmen dies nicht tragen kann. Jeder Eingang erhält eine Fall-ID und wird unabhängig von Form oder Absender sachlich triagiert. Verantwortlich ist die benannte Sicherheitsfunktion; Stellvertretung und Eskalation entsprechen dem PSIRT-Ablauf.

3.3 Ein kleines PSIRT als Bereitschaftsfunktion organisieren

Ein kleines Unternehmen benötigt nicht zwingend eine dauerhafte Spezialabteilung. Es benötigt eine funktionierende Bereitschaft:

- benannte Fallverantwortung und Stellvertretung;
- erreichbarer Intake;
- kurze Triage- und Eskalationshilfe;
- Zugriff auf Produkt-, Build-, SBOM- und Kundeninformationen;
- vorab geklärte externe Fachunterstützung;
- verantwortliche Management- und Meldeentscheidung;
- einfacher Übungsrhythmus;
- getesteter Zugang zur Meldeplattform und vorab geklärte externe Hilfe.

Basic kann dies mit einer primären Person, einer Stellvertretung und einem Fallregister abbilden; weitere Verantwortungen dürfen gebündelt sein. Intermediate verwendet dokumentierte Abläufe und Tabletop-Übungen. Advanced misst Reaktionszeiten, Muster und Wirksamkeit.

Nachweis: PSIRT Readiness-Datensatz, Kontaktliste und Übungsprotokoll.

3.4 Schwachstellen entgegennehmen und entscheiden

Jeder Fall erhält eine eindeutige ID. Security entscheidet, ob das Produkt betroffen ist, welche Auswirkung möglich ist und ob Korrektur, Meldung oder Nutzerinformation notwendig wird. Der Fallrecord im bestehenden Ticket- oder PSIRT-System führt die technischen Pflichtfelder.

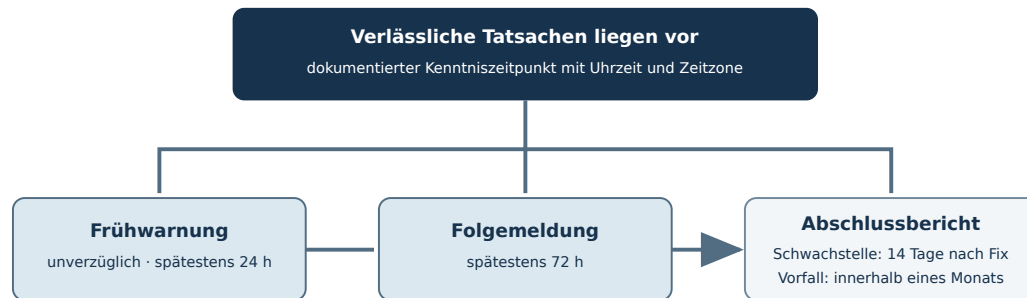
Der Hersteller informiert betroffene Komponenten-Maintainer angemessen, behandelt aber das Risiko seines eigenen Produkts unabhängig weiter.

Nachweis: PSIRT and Vulnerability Case-Datensatz. Seine Pflichtfelder stehen in der Arbeitsvorlage oder im bestehenden Fallsystem; im Manual bleibt die Entscheidungskette sichtbar.

3.5 Gesetzliche Meldung auslösen

Aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle folgen Artikel 14. Der Meldenachweis verbindet den dokumentierten Kenntniszeitpunkt und gesetzlichen Trigger mit der jeweils fälligen Meldestufe und ihrer Übermittlungsbestätigung.

Artikel 14 CRA: eine Uhr, zwei Trigger, klare Fristen



Parallel weiterführen:

technische Triage · Korrektur · Test · Verteilung · Nutzerinformation · Wirksamkeitskontrolle
Interne oder externe Prüfung verschiebt den Kenntniszeitpunkt nicht.

Abbildung 7 – Der dokumentierte Kenntniszeitpunkt startet die gesetzliche Fristenkette nach Artikel 14 CRA.

Die Entscheidungskarte verwendet die gesetzlichen Kriterien:

Frage	Ja	Nein oder unklar
Liegt eine Schwachstelle vor und gibt es verlässliche Belege, dass ein böswilliger Akteur sie ohne Erlaubnis eines Systemeigentümers ausgenutzt hat?	aktiv ausgenutzte Schwachstelle; Meldekette öffnen	technische Triage fortsetzen; Unklarheit sofort eskalieren
Beeinträchtigt ein Vorfall oder kann er Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit wichtiger Daten oder Funktionen beeinträchtigen?	schwerer Sicherheitsvorfall; zweite gesetzliche Frage prüfen Meldekette öffnen	
Hat der Vorfall zur Einführung oder Ausführung bössartigen Codes im Produkt oder im System eines Nutzers geführt oder kann er dazu führen?	schwerer Sicherheitsvorfall; Begründung dokumentieren und Fall weiter behandeln	

Der Kenntniszeitpunkt ist der früheste dokumentierbare Zeitpunkt, zu dem dem Hersteller verfügbare und verlässliche Tatsachen vorliegen, welche die jeweilige gesetzliche Meldeschwelle erfüllen. Der Falldatensatz hält Tatsachen, Quelle, Uhrzeit, Zeitzone, Prüfer und Begründung fest. Eine interne oder externe Rechtsprüfung verschiebt diesen Zeitpunkt nicht.

KMU-Mindestprozess:

1. möglichen gesetzlichen Trigger sofort eskalieren;

2. dokumentierten Kenntniszeitpunkt unveränderbar erfassen;
3. aktiv ausgenutzte Schwachstelle oder schweren Sicherheitsvorfall entscheiden;
4. zuständiges koordinierendes CSIRT nach Artikel 14 Absatz 7 bestimmen und den Meldeweg über die Single Reporting Platform vorbereiten;
5. Frühwarnung und nachfolgende Berichte fristgerecht einreichen;
6. Receipt und übermittelte Inhalte archivieren;
7. Nutzerinformation separat entscheiden.

Die Fallkarte unterscheidet zwei Fristenkettens:

Trigger	Frühwarnung	Folgemeldung	Abschlussbericht
aktiv ausgenutzte Schwachstelle	unverzüglich, spätestens 24 Stunden nach Kenntnis	spätestens 72 Stunden nach Kenntnis, soweit die Information nicht bereits vorliegt	spätestens 14 Tage, nachdem eine Korrektur- oder Minderungsmaßnahme verfügbar ist
schwerer Sicherheitsvorfall	unverzüglich, spätestens 24 Stunden nach Kenntnis	spätestens 72 Stunden nach Kenntnis, soweit die Information nicht bereits vorliegt	innerhalb eines Monats nach der Vorfallmeldung

Zwischenberichte werden bearbeitet, wenn die zuständige Stelle sie verlangt. Die Fallverantwortung berechnet Fristen aus dem gespeicherten Kenntniszeitpunkt und lässt jede Übermittlung durch eine zweite vertretungsfähige Person kontrollieren. Artikel 14 CRA ist der Rechtsanker; Plattformmasken und nationale Zuständigkeiten werden vor der operativen Verwendung erneut geprüft.

Die zweite Prüfung darf keine fristgerechte Meldung verzögern. Ist die zweite Person nicht erreichbar, übermittelt die Fallverantwortung nach dem dokumentierten Notfallweg und lässt die nachträgliche Kontrolle protokollieren.

Für den Meldemitgliedstaat gilt die Reihenfolge aus Artikel 14 Absatz 7 CRA. Bei einer Hauptniederlassung in der Union ist der Staat massgeblich, in dem die Cybersicherheitsentscheide überwiegend getroffen werden. Kann dieser nicht bestimmt werden, folgt die gesetzliche Ersatzregel. Hersteller ohne Hauptniederlassung in der Union verwenden die Reihenfolge Bevollmächtigter, Importeur und Distributor. Der Datensatz speichert die angewandte Stufe, den CSIRT-Endpunkt, den Plattformtest und die Begründung. Unklarheit löst die vorbereitete Übergabe an eine Fachstelle aus, ohne die Meldung zu verzögern.

Die Meldepflichten gelten ab 11. September 2026. Operative Plattformdetails und Zugang werden vor diesem Datum praktisch getestet. ENISA beschreibt die Single Reporting Platform mit Stand 17. Juli 2026 als für den 11. September 2026 geplantes System, das vor dem Start Benutzer- und Sicherheitstests durchläuft. Für den Zugang ist ein EU-Login-Konto vorgesehen. Die Plattform leitet die Meldung gleichzeitig an das nach Artikel 14 Absatz 7 bestimmte koordinierende CSIRT und an ENISA. Bei einer vertretenden Person erfolgt die Validierung nach dem ersten Zugang und darf die erste Übermittlung nicht verhindern. Der veröffentlichte Produktivzugang und die aktuelle Liste der koordinierenden CSIRTs werden vor der Verwendung anhand der ENISA-Seite geprüft. Solange der produktive Endpunkt oder nationale Koordinator noch nicht abschliessend verfügbar ist, führt der Bereitschaftsnachweis den letzten Teststand, einen Owner, den erneuten Testtermin und einen

dokumentierten Fallback.⁷ Ein interner Zielwert darf nicht als gesetzliche Frist bezeichnet werden.⁸

Bei technischer Nichtverfügbarkeit dokumentiert die Fallverantwortung Zeitpunkt, Fehlermeldung, Übermittlungsversuche und unveränderte Meldeinhalte. Sie verwendet nur einen offiziell veröffentlichten nationalen elektronischen Endpunkt oder eine ausdrückliche aktuelle Weisung des zuständigen CSIRT beziehungsweise der ENISA-Hilfe. Ein direkter Kontakt zum CSIRT dient der Eskalation und Beweissicherung, gilt aber ohne offizielle Bestätigung nicht automatisch als Artikel-14-Übermittlung. Die Meldung wird über die Single Reporting Platform oder den offiziell dafür bestimmten Endpunkt unverzüglich nachgeholt. Diese Vorsorge ist eine empfohlene Mindestkontrolle; Artikel 14 Absatz 7 und Artikel 16 CRA führen den gesetzlichen Meldeweg.

Basic verwendet eine kurze Entscheidungskarte und zwei vertretungsfähige Zugänge. Intermediate übt den Ablauf und führt Vorlagen. Advanced integriert Fall-, Melde- und Wirksamkeitsdaten.

Nachweis: Reporting Decision, Timestamp, Submission und Receipt.

Kenntnis und Triage	gesetzliche Meldespur	technische Korrekturspur	gemeinsamer Abschluss
frühester dokumentierbarer Zeitpunkt bleibt unverändert	Frühwarnung, Folgemeldung und branchenspezifischer Abschlussbericht	untersuchen, beheben, testen, verteilen und Nutzer informieren	Receipts, Wirksamkeit, Marktentscheid und Lessons Learned

Abbildung 8 – Meldung und Produktkorrektur beginnen am selben unveränderten Kenntniszeitpunkt. Beide Spuren laufen parallel; eine zweite Prüfung darf weder Uhr noch Übermittlung verzögern.

3.6 Sicherheitsupdate entwickeln und sicher verteilen

Engineering behebt die Ursache, prüft die Korrektur und schützt den Updateweg. Sicherheitsupdates werden unverzüglich und grundsätzlich kostenlos bereitgestellt. Soweit technisch machbar, werden neue Sicherheitsupdates von Funktionsupdates getrennt.

Vorgehen:

- 1. Korrektur und betroffene Versionen bestimmen.
- 2. Fix, Regression, Updateintegrität und Rückfall prüfen.
- 3. Update sicher signieren und verteilen.
- 4. Nutzerhandlungen und bekannte Einschränkungen erklären.
- 5. Wirksamkeit und Verteilung überwachen.
- 6. Nachweis mit dem Schwachstellenfall verbinden.

Der Updateplan benennt Schlüssel-Owner, geschützten Speicher, Zugriff und Stellvertretung,

7 ENISA, Single Reporting Platform, aktualisiert am 17. Juli 2026 und geprüft am 30. Juli 2026. Die Betriebsinformation ist offiziell, aber nicht bindend; Artikel 14 und 16 CRA führen die rechtliche Aussage.

8 Verordnung (EU) 2024/2847, Artikel 14, Artikel 69 Absatz 3 und Artikel 71 Absatz 2. Artikel 71 Absatz 2 setzt Artikel 14 ab 11. September 2026 in Geltung; Artikel 69 Absatz 3 erfasst bestimmte bereits zuvor in Verkehr gebrachte Produkte.

Rotation, Widerruf sowie den Notfall bei Verlust oder Kompromittierung. Rollback auf bekannte verwundbare Versionen wird verhindert oder ausdrücklich risikobasiert kontrolliert. Eine Wiederherstellungsanweisung beschreibt, wie Signierdienst, Buildumgebung und Vertrauenskette nach einer Kompromittierung sauber neu aufgebaut werden. Fehlende Wiederherstellbarkeit ist ein Release-Freigabesperre.

Nachweis: Update Plan, Fix Verification und Distribution Datensatz.

3.7 Nutzer und Kunden verständlich informieren

Eine Nachricht sagt zuerst, welches Produkt betroffen ist und was der Nutzer tun muss. Sie erklärt Risiko, Update oder Workaround und nennt den Supportkontakt. Unnötiger Fachjargon und Verharmlosung erschweren eine richtige Reaktion und werden vermieden.

Zeitpunkt, Empfänger und Detailtiefe berücksichtigen Ausnutzungsrisiko, Meldeanforderungen und koordinierte Offenlegung. Die Nachricht wird auf Finden, Verstehen und Handeln getestet.

Nachweis: Nutzerinformationsdatensatz (User Communication Record). Er verbindet den genehmigten Text mit Zielgruppe, Kanal, Veröffentlichungszeitpunkt und Freigabe.

Bei einer veröffentlichten Sicherheitskorrektur verbindet der Fallrecord technische Massnahme, betroffene Version und Nutzerhandlung. Die vollständigen Advisory- und Veröffentlichungsfelder stehen in der Arbeitsvorlage oder im bestehenden Fallsystem.

3.8 Produkt halten, korrigieren, zurücknehmen oder zurückrufen

Bei bekannter oder vermuteter Nichtkonformität entscheidet die verantwortliche Geschäftsführung unverzüglich über:

- Freigabesperre für noch nicht freigegebene Versionen;
- Marktbereitstellungsstopp für weitere Marktbereitstellung;
- Korrektur oder Sicherheitsupdate;
- Rücknahme oder Rückruf;
- Behördenkooperation;
- Nutzer- und Kundeninformation;
- Bedingungen für Re-entry.

Nachweis: Corrective Action-Datensatz mit Entscheidung, Begründung, Owner und Abschluss.

Die benannte Konformitätsverantwortung prüft artikelgenau, ob zusätzlich eine Marktüberwachungsbehörde, notifizierte Stelle oder andere Stelle zu informieren ist. Das Manual unterstellt keine pauschale Selbstmeldung jeder Nichtkonformität. Der Datensatz hält Trigger, Behörde, Rechtsgrund, Frist, Inhalt und Übermittlungsnachweis fest. Betriebseinstellung und gesetzliche Artikel-14-Meldungen bleiben eigene Trigger.

3.9 Änderungen und neue Versionen erneut beurteilen

Das Unternehmen prüft bei Änderungen Kernfunktion, Architektur, Produktklasse, Herstellerrolle, Risiken, Komponenten, Support und Konformitätsweg. Eine wesentliche Änderung kann neue

Herstellerpflichten auslösen.

Basic verwendet einen Change Trigger im Release Gate. Intermediate führt eine wiederholbare Impact-Analyse. Advanced verbindet Produkt-, Komponenten- und Regulatory-Änderungen über das Portfolio.

Nachweis: Change and Substantial Modification Decision.

Die Impact-Prüfung beginnt nicht erst bei einer rechtlich wesentlichen Änderung. Jede Änderung an Produkt, Komponente, Lieferant, Kernfunktion, vorgesehener Nutzung, Bedrohung, Produktion, Supportfähigkeit, Norm oder Rechtsquelle wird zunächst gegen den Lebenszyklus geprüft. Sie öffnet nur die tatsächlich betroffenen Entscheide erneut. Ob zusätzlich eine wesentliche Änderung im Sinne des CRA vorliegt, ist eine eigene Rechtsfrage. Unklarheit wird an die Fachstelle übergeben und blockiert den betroffenen Marktweg; gewöhnliche Sicherheitsupdates werden nicht pauschal als wesentliche Änderungen behandelt.

Änderung	mögliche Rücksprünge	erneuter Entscheid
Produkt, Komponente, Lieferant, Nutzung, Bedrohung, Produktion, Support, Norm oder Recht	Scope/Rolle, Risiko, Anforderungen, SBOM/Build, Tests, Dokumentation/Konformität, Release oder Support	nur betroffene Gates erneut öffnen; wesentliche Änderung separat beurteilen

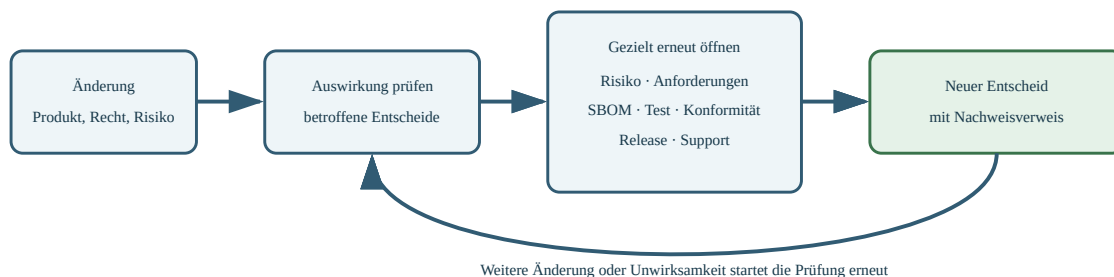


Abbildung 9 – Änderungen öffnen gezielt die betroffenen Entscheide.

Der neue Freigabeentscheid verweist auf die ersetzten früheren Entscheide.

3.10 Support kontrolliert beenden

Der Hersteller plant End of Support frühzeitig. Er veröffentlicht mindestens Monat und Jahr, informiert Nutzer soweit technisch machbar und dokumentiert:

- letzte unterstützte Version;
- letzte Sicherheitsupdates;
- bekannte verbleibende Risiken;
- Migrations- oder Ausserbetriebnahmehinweise;
- sichere Entfernung von Nutzerdaten;
- Aufbewahrung von technischer Dokumentation und Erklärungen;
- Fortbestand erforderlicher Updateverfügbarkeit;
- Vorgehen bei supportrelevanter Betriebseinstellung.

Nachweis: End-of-Support-Datensatz und Nutzerinformation.

Stellt der Hersteller seine Geschäftstätigkeit ein und kann deshalb CRA-Pflichten nicht mehr erfüllen, informiert er vor Wirksamwerden die relevanten Marktüberwachungsbehörden sowie soweit möglich die Nutzer. Der Vorsorgeplan benennt verantwortliche Person, Signierschlüssel, Update-Dateien, Build- und Testumgebung, technische Dokumentation, Kontaktkanal, Nutzerinformation und eine mögliche zulässige Übergabe. Diese Pflicht folgt Artikel 13 Absatz 23 CRA und ist nicht mit einem normalen Produkt-Supportende gleichzusetzen.

Bereits veröffentlichte Sicherheitsupdates bleiben mindestens zehn Jahre nach ihrer Bereitstellung oder für die verbleibende Supportdauer verfügbar, je nachdem, welcher Zeitraum länger ist. Bringt der Hersteller spätere, substanziell geänderte Versionen eines Softwareprodukts in Verkehr, darf er die Schwachstellenbehandlung auf die zuletzt in Verkehr gebrachte Version beschränken. Dann müssen Nutzer früherer Versionen kostenlosen Zugang zur letzten Version erhalten und dürfen keine zusätzlichen Kosten für die Anpassung ihrer Hard- oder Softwareumgebung tragen. Die konkrete Entscheidung und ihr Rechtsstand werden im Support-Datensatz dokumentiert.

4. Wie betreiben und verbessern wir das Modell?

Am Ende dieses Kapitels sind Rollen, gemeinsame Daten, externe Leistungen, Werkzeuge, Kompetenzen und Managementprüfung so organisiert, dass der Prozess dauerhaft funktioniert.

4.1 Verantwortung mit wenigen Rollen abbilden

Das Unternehmen benötigt Verantwortungen, nicht zwingend Stellen:

Verantwortung	Mindestaufgabe
Geschäftsführung	Ressourcen, Risikoakzeptanz, Freigabesperre/Marktbereitstellungsstopp und Wirksamkeit
Product Owner	Produktgrenze, Nutzung, Roadmap und Support
Engineering	Design, Komponenten, Build, Tests und Updates
Security/PSIRT	Intake, Triage, Eskalation, Meldung und Fallführung
Quality/Compliance	Dokumentation, Konformitätsweg, Release und Aufbewahrung
Legal-Handoff	unklare Rollen, Ausnahmen, Meldungen und Behördenfragen

Eine Person darf mehrere Verantwortungen tragen. Eine zweite vertretungsfähige Person prüft gesetzliche Meldungen, Akzeptanzen hoher Produktrisiken sowie Release-, Marktbereitstellungsstopp- und Re-entry-Entscheidungen. Weitere Vier-Augen-Prüfungen werden nur risikobasiert festgelegt.

Eine vom operativen Ersteller getrennte Prüfung ist erforderlich bei gesetzlichen Meldungen, hohen Restrisiken, Konformitätswegentscheidungen für wichtige oder kritische Produkte, P2-Ausnahmen, Marktbereitstellungsstopps, Re-entry sowie wesentlichen Änderungen. Fehlt intern eine geeignete unabhängige Person, wird eine fachkundige externe Prüfung eingesetzt. Diese Mindestkontrolle ist die Kontrollarchitektur dieses Modells und keine wörtliche CRA-Organisationsvorgabe.

Die Geschäftsführung genehmigt eine kurze Product Security Policy. Sie legt Scope, Verantwortung, Release-Marktbereitstellungsstopp, Schwachstellenannahme, gesetzliche Eskalation, Supportgrundsatz und jährliche Wirksamkeitsprüfung fest. Damit erhalten ENISA-Frage 1.1 und die operativen Kapitel einen gemeinsamen, schriftlichen Ausgangspunkt.

4.2 Denselben Prozess schrittweise verbessern

Merkmal	Basic	Intermediate	Advanced
Verantwortung	benannt und vertreten	dokumentiert und konsistent angewendet	regelmässig überprüft und wirksam gesteuert
Ablauf	einfach und ausführbar	wiederholbar und über Produkte vergleichbar	gemessen und fortlaufend verbessert
Nachweis	grundlegende Datensätze	vollständige, versionierte und verknüpfte Datensätze	Qualitäts- und Wirksamkeitsdaten
Werkzeuge	manuell oder leichtgewichtig	geeignete Automatisierung an wiederkehrenden Punkten	integrierte Automatisierung mit kontrollierten Ausnahmen
Review	ereignisbezogen	geplant und dokumentiert	risikobasiert und datenunterstützt

Ein höherer Reifegrad ist kein Selbstzweck. Der Zielzustand folgt Produktrisiko, Geschäftsziel und nachgewiesener Schwäche. Ein kleiner, überschaubarer Prozess darf dauerhaft einfach bleiben, wenn er zuverlässig und rechtzeitig wirkt.

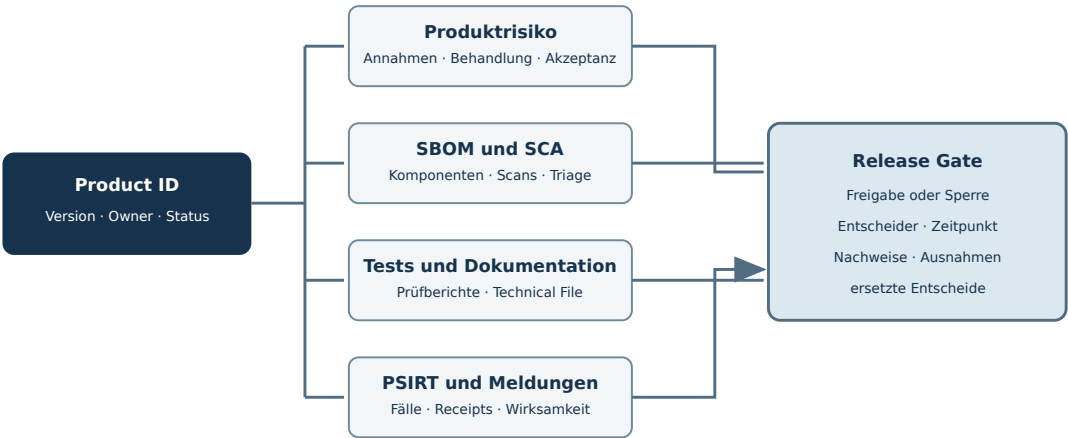
4.3 Daten einmal erfassen und wiederverwenden

Prozessübersicht

Auslöser	Verantwortlich	Stellvertretung	Ergebnis	Freigabesperre
neuer oder geänderter Datensatz	Quality/ Compliance	Product Owner	konsistenter Datensatz mit führenden Stammdaten	Widerspruch in IDs, Status oder Nachweisindex

Das führende lokale System verbindet alle Datensätze über stabile IDs. Product ID und Version bilden die führende Klammer. Jeder weitere Datensatz verweist auf diese Stammdaten und seine Nachweise, statt sie zu kopieren. Ein Workbook darf dieselben IDs für kontrollierten Import oder Export verwenden, bildet aber bei komplexen n:m- Beziehungen keine parallele führende Datenbasis.

Eine Product ID verbindet den vollständigen Audit Trail



Stabile Referenzen statt Kopien: Historie und genehmigte Entscheide bleiben unverändert nachvollziehbar.

Abbildung 10 – Eine führende Product ID verbindet Risiko, SBOM, Tests, Release und PSIRT zu einem prüfbaren Audit Trail.

Pflichtregeln:

- eine führende Produkt-ID;
- keine manuell kopierten Versionsstände in mehreren Registern;
- Owner und letzter Review sichtbar;
- Links oder Pfade auf Nachweis statt eingebetteter Dateikopien;
- kontrollierte Statuswerte;
- Änderungsverlauf für genehmigte Entscheidungen.

Was muss wann gepflegt werden?

Datentyp	Je Release	Jährlich	Nur bei Auslöser
Produktstammdaten	prüfen	Portfolio abgleichen	bei Produkt-, Rollen- oder Marktänderung aktualisieren
Risikobeurteilung	bei relevanter Änderung bestätigen	Wirksamkeit prüfen	neue Bedrohung, Schwachstelle oder Architekturänderung
SBOM und Buildnachweis	für jede betroffene Produktversion aktualisieren	nicht erforderlich	neue Komponente oder korrigierter Build
PSIRT-Fall	nicht pauschal	Übungen und Erreichbarkeit prüfen	Schwachstelle, Advisory oder Vorfall
Managementprüfung	nicht erforderlich	mindestens einmal	schweres Ereignis oder wesentliche Rechtsänderung
Support- und End-of-Support-Daten	beim Release bestätigen	Portfolio prüfen	geänderte Nutzung, Ressourcen oder Betriebseinstellung

Die Matrix verhindert, dass ein kleiner Hersteller bei jedem Release alle zehn Arbeitsbereiche neu ausfüllt. Unveränderte Stammdaten werden bestätigt, nicht kopiert.

4.4 Externe Unterstützung gezielt einsetzen

Prozessübersicht

Auslöser	Verantwortlich	Stellvertretung	Ergebnis	Stop-Kriterium
fehlende Kompetenz, Unabhängigkeit oder Kapazität	Product Owner	Geschäftsführung	abgegrenzter und abnahmefähiger Auftrag	unklarer Leistungsumfang oder fehlendes Abnahmekriterium

KMU können Rechtsprüfung, Penetrationstest, Toolbetrieb, Incident-Unterstützung oder Konformitätsbewertung einkaufen. Vor Beauftragung werden Scope, Kompetenz, Vertraulichkeit, Datenzugang, Reaktionszeit, Ergebnisformat und Abnahmekriterium festgelegt.

Der Hersteller behält Produktwissen und Entscheidungsverantwortung. Eine externe Bestätigung ohne nachvollziehbaren Nachweis schliesst keinen internen Datensatz.

4.5 Tragbare Werkzeuge auswählen

Prozessübersicht

Auslöser	Verantwortlich	Stellvertretung	Ergebnis	Freigabesperre
wiederkehrende manuelle Lücke oder Risikoverstärker	Engineering	Security	dokumentierter und reproduzierbarer Werkzeugtest	ungeklärter Datenabfluss oder nicht reproduzierbares Ergebnis

Ein Werkzeug wird nur empfohlen, wenn sein Referenzpfad geprüft ist:

- benötigte Funktion;
- unterstützte Produkt- und Pakettechnologie;
- Lizenz und tatsächliche Kosten;
- Datenabfluss und Datenschutz;
- Aktualisierung und Schwachstellen des Werkzeugs;
- Integrations- und Betriebsaufwand;
- Exportformat und Archivierung;
- menschliche Triage;
- reproduzierbarer Testfall.

Open Source kann Lizenzkosten reduzieren. Betrieb, Review und Pflege bleiben trotzdem notwendig.

4.6 ENISA-Assessment wiederholen und wenige Massnahmen wählen

Prozessübersicht

Auslöser	Verantwortlich	Genehmigung	Ergebnis	Stop-Kriterium
jährliche Prüfung, wesentliche Änderung oder erkennbare Unwirksamkeit	Security	Geschäftsführung	priorisierter Verbesserungsplan	gesetzlich dringende Lücke wird durch Reifegradplanung verzögert

Das Assessment wird mindestens jährlich, nach wesentlicher Änderung oder bei deutlicher Unwirksamkeit wiederholt. Das Unternehmen vergleicht nicht nur den Gesamtwert, sondern die fünf

Domänen und einzelne Fragen.

Der Verbesserungsplan enthält bewusst wenige parallele Massnahmen. Jede Massnahme hat:

- Bezug zur ENISA-Frage;
- gesetzliche oder risikobasierte Priorität;
- Owner und Termin;
- erwartetes Ergebnis;
- benötigte Nachweise;
- Wirksamkeitskriterium.

4.7 Management prüft Wirksamkeit und Ressourcen

Prozessübersicht

Auslöser	Entscheidung	Vorbereitung und Stellvertretung	Ergebnis	Stop-Kriterium
jährlicher Termin oder schweres Ereignis	Geschäftsführung	Product Owner	Entscheidung, akzeptiertes Risiko oder Massnahme je wesentlichem Befund	wesentlicher Befund ohne nachvollziehbare Entscheidung

Mindestens jährlich und bei schweren Ereignissen prüft die Geschäftsführung:

- Produktportfolio und offene Scope-Fragen;
- aktuelle Produktrisiken;
- Schwachstellen, Meldefälle und Updatezeiten;
- Supportverpflichtungen und End-of-Support;
- Release Holds, Abweichungen und überfällige Massnahmen;
- ENISA-Entwicklung;
- Kompetenz, Stellvertretung und externe Abhängigkeiten;
- Werkzeug- und Budgetbedarf;
- Regulatory-Watch-Änderungen.

Nachweis: Annual Management and Effectiveness Review mit Entscheiden und Massnahmen.

Ein Bericht ohne Entscheidung ist keine Managementprüfung. Zu jedem wesentlichen Befund hält die Geschäftsführung fest, ob sie Risiko behandelt, zusätzliche Ressourcen bereitstellt, eine Priorität ändert, externe Unterstützung beschafft, einen Release sperrt, die Marktbereitstellung stoppt oder einen früheren Lebenszyklusentscheid erneut öffnet. Owner, Termin und Abnahmekriterium sind verbindlich.

Materiale Unterkapazität wird nicht als Dauerzustand toleriert. Kann das Unternehmen Support, Build, Signierung, Tests, Schwachstellenannahme, Meldung oder Updateverteilung nicht mehr zuverlässig leisten, eskaliert die verantwortliche Rolle dies dokumentiert an die Geschäftsführung. Die Geschäftsführung trifft einen nachvollziehbaren Entscheid über Ressourcen, Produktumfang, Support, externe Hilfe oder Marktfolge. Ausbleibende Entscheidung schliesst den Befund nicht.

Entscheidungssignale	Challenge und Einordnung	Managemententscheid	Umsetzung	Wirksamkeitsprüfung
Portfolio, Risiko, Fälle, Support, Gate-Fehler, Kapazität und Rechtsänderung	operative Sicht, zweite Linie und unabhängige Prüfung bleiben getrennt	Risiko, Ressourcen, Priorität, externe Hilfe, Marktfolge oder Revalidierung	Owner, Termin und Abnahmekriterium	schliessen, nachsteuern oder erneut eskalieren

Abbildung 11 – Managementprüfung endet mit Entscheidung, Owner, Abnahmekriterium und Wirksamkeitsprüfung. Ein Bericht ohne nachvollziehbare Entscheidung schliesst keinen wesentlichen Befund.

4.8 NIS2 Supplier Assurance getrennt, aber wiederverwendbar beantworten

Prozessübersicht

Auslöser	Verantwortlich	Prüfung und Stellvertretung	Ergebnis	Freigabesperre
konkrete Kundenanfrage	Product Owner	Quality/ Compliance	freigegebene und nachvollziehbare Antwort	unbelegte, vertrauliche oder ausserhalb des freigegebenen Anwendungsbereichs liegende Aussage

Ein Kunde, der der Richtlinie über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau (NIS2) unterliegt, kann über den CRA hinaus organisatorische Nachweise, Vertragsrechte oder Zertifikate verlangen. Das Unternehmen trennt:

- CRA-Produktpflicht;
- NIS2- oder Anforderung aus dem Digital Operational Resilience Act (DORA) des Kunden;
- vertragliche Zusatzforderung;
- freiwillige Assurance.

Produktbezogene Nachweis zu sicherer Entwicklung, SBOM, Schwachstellenbehandlung, Updates und Support wird wiederverwendet. Organisationsthemen wie Business Continuity, Zugriffssteuerung oder Schulung werden ergänzt, wenn sie tatsächlich verlangt sind. Ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001 ist keine allgemeine CRA-Pflicht.

Das kontrollierte Mindestpaket enthält eine freigegebene Produktbeschreibung, Supportdauer, sicheren Kontakt, Aussage zum Entwicklungs- und Releaseprozess, SBOM-Verfügbarkeitsweg, Schwachstellen- und Updateprozess sowie die zulässige Konformitätsinformation. Vertrauliche SBOMs, Testberichte oder interne Risiken werden nicht automatisch herausgegeben. Der Supplier-Assurance-Datensatz dokumentiert Anfrage, Rechts- oder Vertragsgrund, Freigabe, Gültigkeit und offengelegte Nachweis.

4.9 Rechtsstand und externe Informationen beobachten

Prozessübersicht

Auslöser	Verantwortlich	Stellvertretung	Ergebnis	Freigabesperre
neue offizielle Quelle, Normenzitation, Behördeninformation oder relevantes Advisory	Quality/ Compliance	Security	dokumentierter Auswirkungsentcheid	releasekritische Änderung ist nicht behandelt

Regulatory Watch umfasst mindestens:

- CRA-Rechtsakte und Kommissionsguidance;
- harmonisierte Normen und Zitationsstatus;
- ENISA und Single Reporting Platform;
- nationale Umsetzung und Behördenzuständigkeit;
- relevante Produkt- und Komponentenadvisories;
- Schweizer Markt- und Rechtsentwicklung;
- Anforderungen wichtiger regulierter Kunden.

Jede Änderung erhält Datum, Quelle, Auswirkung, Owner und Entscheidung. Sie öffnet die früheste betroffene Phase oder den betroffenen Produktrecord.

Der Watch-Eintrag benennt nicht nur ein betroffenes Kapitel. Er ordnet die Änderung einem oder mehreren Lebenszyklusentscheiden zu: Scope und Rolle, Produktklasse, Produktrisiko, technische Anforderung, Konformitätsweg, Reporting, Support, Nutzerinformation oder Publikationsstatus. Dadurch wird eine neue Quelle nicht mit einem lokalen Textpatch abgearbeitet, wenn sie einen früheren Entscheid verändert.

4.10 Das Modell in erreichbaren Schritten einführen

Die Einführung beginnt nicht mit einem perfekten Toolstack.

1. Produkte, Rollen und Kontakt sichtbar machen.
2. Scope, Produktklasse und Fristen entscheiden.
3. ENISA-Ausgangswert bestimmen.
4. Risikobeurteilung und Release Gate zunächst für das risikoreichste oder nächste freizugebende Produkt einführen.
5. Komponentenrecord, SBOM und Scan-Triage aufbauen.
6. PSIRT-Bereitschaft und Meldung testen.
7. Support und technische Dokumentation vervollständigen.
8. wenige Verbesserungen umsetzen und Wirksamkeit prüfen.

Erst wenn der Ablauf funktioniert, werden weitere Produkte und Automatisierungen aufgenommen.

Derselbe Ablauf bei 10, 50 und 100 Mitarbeitenden

Beispiel	Rollen und Arbeitsmittel	Angemessene Entwicklung
etwa 10 Mitarbeitende	Geschäftsführung entscheidet; Product Owner koordiniert; Engineering und PSIRT-Verantwortung dürfen gebündelt sein; eine Stellvertretung und gezielte externe Hilfe sichern Ausfälle ab	vorhandenes Ticket- und Releaseverfahren um CRA-Felder und Gates ergänzen; optionales Starter-Workbook nur wenn noch keine geeignete Bestandslösung besteht
etwa 50 Mitarbeitende	Product Owner, Engineering, Quality und Security besitzen klarere Verantwortungen; Stellvertretungen und Reviews sind geplant	wiederholbare Build- und Release-Prüfungen, zentrale Datensätze, regelmässige PSIRT-Übung und definierte Lieferantenprüfung
etwa 100 Mitarbeitende	mehrere Produkte nutzen gemeinsame Verantwortungs- und Eskalationsregeln; unabhängige Prüfung wird risikobasiert getrennt	Portfoliosteuerung, integrierte Scans, konsistente Kennzahlen und zentrale Nachweis-Verknüpfung

Alle drei Beispiele verwenden denselben Kernprozess. Die Tabelle beschreibt keine gesetzlichen Grössenstufen und keine unterschiedlich vollständigen Compliance-Wege.

Die Unternehmensgrösse entscheidet nicht allein über das Werkzeug. Ein 20-Personen-Unternehmen mit 20 Produkten kopiert seine Open-Source-Komponenten nicht in ein CRA-Workbook. SCA-, SBOM- oder Buildsysteme führen die technischen Daten. Das vorhandene Ticketsystem steuert relevante Triage- und PSIRT-Fälle. Das Release Management entscheidet über Release, Freigabesperre oder Marktbereitstellungsstopp. Eine eigene CRA-Anwendung ist nur nötig, wenn diese Verknüpfung mit vertretbarem Aufwand nicht zuverlässig gelingt.

4.11 Wissen, Kompetenz und Awareness sichern

Für jede Verantwortung werden notwendige Fähigkeiten und vorhandene Kompetenz verglichen. Lücken werden durch Einweisung, Training, Wissensaustausch, Rekrutierung oder externe Fachunterstützung geschlossen.

Basic macht Verantwortung und notwendiges Wissen sichtbar. Intermediate liefert rollengerechte, dokumentierte Massnahmen. Advanced prüft Kompetenz und Trainingswirksamkeit regelmässig und passt sie an neue Produkte und Risiken an.

Nachweis: Role and Competence-Datensatz im Management-Review-Arbeitsbereich.

Die Geschäftsführung unterstützt eine offene Meldekultur. Mitarbeitende dürfen Produktfehler und Sicherheitsbedenken ohne Umweg melden; die verantwortliche Rolle bestätigt den Eingang und schützt eine sachliche Eskalation vor wirtschaftlichem Release-Druck. Diese Regel wird in Einweisung und Product Security Policy sichtbar und deckt den praktischen Kulturbezug der ENISA-Frage 5.3 ab.

Prozess- und Nachweis-Landkarte

Diese Landkarte verdichtet gemeinsame Angaben. Die Entscheidung und der nächste Schritt stehen

weiterhin im jeweiligen Unterkapitel. GF bedeutet Geschäftsführung, PO Product Owner, ENG Engineering, SEC Security oder PSIRT und Q/C Quality/Compliance. In Kleinstunternehmen dürfen Rollen gebündelt sein; die benannte Stellvertretung bleibt erhalten.

Kapitel 1: Anwendbarkeit und Planung

Abschnitt	Rolle / Backup	Sperre / Eskalation	Nachweis	Rechtsanker
1.1 Start	GF / PO	kein Owner, keine Ablage oder ungeklärter Release	Management-Startentscheid (Management Start Decision)	CRA Art. 13
1.2 Rolle	Q/C / GF	Rolle oder Schweizer EU-Marktweg ungeklärt	Entscheid zur Wirtschaftsakteurrolle (Economic Role Decision)	CRA Art. 3, 18 bis 22; VO (EU) 2019/1020
1.3 Scope	PO / Q/C	Ausnahme oder Produktgrenze ungeklärt	Anwendbarkeitsdatensatz	CRA Art. 2 und 3; Delegierte VO (EU) 2025/1535 bei L-Kategorie-Produkten
1.4 KMU	GF / Q/C	Partner- oder Verbunddaten fehlen	KMU-Klassifikationsdatensatz	CRA Art. 3 № 19, Art. 26 und 33, Erwägungsgründe 4 und 5; Anhang Empfehlung 2003/361/EG
1.5 Klasse	PO / Q/C	möglicher Anhang-III- oder IV-Treffer ungeklärt	Klassenentscheid	CRA Art. 7 bis 9, Anhänge III und IV
1.6 Termine	Q/C / PO	gesetzlicher Termin ohne Vorlauf	Konformitätszeitplan	CRA Art. 71
1.7 ENISA	SEC / PO	Bewertung ohne Nachweis	ENISA-Originaldatei	ENISA CRA Maturity Model Tool
1.8 Verstärker	PO / SEC	Verstärker ohne stärkere Massnahme	Risikoverstärker-Entscheid (Risk Override Decision)	CRA Anhang I; ENISA-Modell
1.9 Plan	GF / PO	gesetzliche Lücke wird nach Reifegradziel verschoben	Verbesserungsplan	ENISA Action Checklist

Kapitel 2: Produkt und Release

Abschnitt	Rolle / Backup	Sperre / Eskalation	Nachweis	Rechtsanker
2.1 Register	PO / Q/C	keine eindeutige Produktversion	Produktregister	CRA Art. 13 und Anhang VII
2.2 Risiko	PO / SEC	hohes nicht akzeptiertes Risiko	Produktrisikobeurteilung	CRA Art. 13, Anhang I und VII
2.3 Design	ENG / PO	anwendbare Eigenschaft ohne Anforderung oder Test	Risiko-Anforderungsmatrix	CRA Anhang I Teil I
2.4 Komponenten	ENG / SEC	unbekannte oder nicht gepflegte kritische Komponente	Komponenten- und Lieferantendatensatz (Component and Supplier Record)	CRA Art. 13, Anhang I Teil II
2.5 SBOM	ENG / SEC	keine geprüfte SBOM zur Release-Version	SBOM-Qualitätsprüfung	CRA Anhang I Teil II Nr 1; Anhang VII
2.6 Scan/Triage	SEC / ENG	relevanter Fund ohne Entscheid	Triage-Datensatz	CRA Anhang I Teil II
2.7 Tests	ENG / PO	Abnahmekriterium nicht erfüllt	Testplan und Prüfbericht	CRA Anhang I und VII
2.8 Dokumente	Q/C / PO	Pflichtinhalt oder Versionsbezug fehlt	Index technische Dokumentation	CRA Art. 31 und 33; Anhang VII
2.9 Konformität	Q/C / GF	Produktklasse, Normenstatus oder Stelle ungeklärt	Konformitätswegentscheid	CRA Art. 32 und 33
2.10 Release	PO / GF	Pflichtfrage ohne aktuelle Nachweis	Release Gate-Datensatz	CRA Art. 13, 28 bis 30
2.11 Serie	PO / Q/C	Produktionsabweichung ungeklärt	Serienkonformitätsdatensatz	CRA Art. 13 Abs. 14

Kapitel 3: Support und Schwachstellen

Abschnitt	Rolle / Backup	Sperre / Eskalation	Nachweis	Rechtsanker
3.1 Supportdauer	PO / GF	Dauer nicht begründet oder nicht finanzierbar	Support Period Decision	CRA Art. 13 Abs. 8 bis 10
3.2 Kontakt	SEC / PO	Kanal oder Backup nicht erreichbar	Contact Point-Datensatz	CRA Art. 13; Anhang II
3.3 PSIRT	SEC / PO	keine Eskalation oder kein Plattformzugang	PSIRT Readiness-Datensatz	CRA Art. 13 und 14
3.4 Triage	SEC / ENG	Betroffenheit oder aktive Ausnutzung ungeklärt	Vulnerability Case	CRA Art. 13 und 14
3.5 Meldung	SEC / GF	Trigger oder Awareness-Zeitpunkt ungeklärt	Reporting Decision und Receipt	CRA Art. 14 und 16
3.6 Update	ENG / PO	Fix nicht verifiziert oder Verteilung unsicher	Update and Distribution-Datensatz	CRA Art. 13; Anhang I Teil II
3.7 Information	PO / SEC	Nutzer kann notwendige Handlung nicht erkennen	Nutzerinformationsdatensatz (User Communication Record)	CRA Art. 13 und 14; Anhang II
3.8 Korrektur	GF / PO	Nichtkonformität ohne Sofortentscheid	Corrective Action-Datensatz	CRA Art. 13 Abs. 21 sowie Art. 54 bis 58
3.9 Änderung	PO / Q/C	Auswirkung oder Herstellerrolle ungeklärt	Change Decision	CRA Art. 3 und 22
3.10 Supportende	PO / GF	Veröffentlichung oder Updateverfügbarkeit fehlt	End-of-Support-Datensatz	CRA Art. 13 Abs. 9, 10, 19 und 23

Kapitel 4: Betrieb und Verbesserung

Abschnitt	Rolle / Backup	Sperre / Eskalation	Nachweis	Rechtsanker
4.1 Rollen	GF / PO	Verantwortung oder Stellvertretung fehlt	Product Security Policy und Verantwortungsmatrix	CRA Art. 13; ENISA 1.1
4.2 Reifegrad	GF / SEC	Reifegrad wird als Konformität verwendet	Maturity Decision	ENISA-Modell und Tool
4.3 Daten	Q/C / PO	widersprüchliche Stammdaten	Datensatz- und Nachweisindex	CRA Anhang VII
4.4 Externe Hilfe	PO / GF	Scope oder Abnahme unklar	Supplier Engagement-Datensatz	CRA Art. 13 und 32
4.5 Werkzeuge	ENG / SEC	unbekannter Datenabfluss oder unprüfbares Ergebnis	Tool Decision-Datensatz	ENISA- und Bundesamt-für-Sicherheit-in-der-Informationstechnik-Implementierungshilfen
4.6 ENISA-Plan	SEC / GF	zu viele oder nicht messbare Massnahmen	Assessment und Verbesserungsplan	ENISA-Modell und Tool
4.7 Managementprüfung	GF / PO	wesentlicher Befund ohne Entscheid	Management Review	ENISA-Modell
4.8 Supplier Assurance	PO / Q/C	unbelegte oder unzulässige Aussage	Assurance Package-Datensatz	CRA; NIS2 Art. 21 als Kundenkontext
4.9 Regulatory Watch	Q/C / SEC	Rechtsänderung ohne Auswirkungsentscheid	Regulatory Change-Datensatz	offizielle CRA- und ENISA-Quellen
4.10 Einführung	GF / PO	Skalierung vor stabilem Mindestprozess	Implementation Plan	ENISA Action Checklist
4.11 Kompetenz	GF / PO	kritische Rolle ohne Fähigkeit oder Backup	Competence-Datensatz	ENISA-Modell, Fragen 5.1 bis 5.3

Arbeitsvorlagen und Anhänge

Welche Vorlage geöffnet wird, hängt vom Arbeitsschritt ab:

Arbeitsbereich	Einsatzpunkt	Ergebnis
Product Register	Produkt oder Version beginnt	eindeutiger Scope und Status
Applicability and Classification	Marktweg, Rolle oder Produkt ändert sich	genehmigte Anwendbarkeits- und Klassenentscheidung
ENISA Assessment and Verbesserungsplan	Start und Verbesserungsreview	Ausgangswert und wenige priorisierte Massnahmen
Product Cybersecurity Risk Assessment	Design, Änderung, Release oder neue Bedrohung	behandeltes Produktrisiko

Arbeitsbereich	Einsatzpunkt	Ergebnis
Component, Supplier and SBOM Datensatz	Komponente, Build, Scan oder Schwachstelle	versionierte Komponenten- und Triage-Nachweise
Release Gate	Produkt oder Update soll freigegeben werden	Release, Freigabesperre oder Marktbereitstellungsstopp
PSIRT and Vulnerability Cases	Sicherheitsmeldung, Fund oder Vorfall	Fall-, Melde- und Korrekturentscheid
Support and End of Support	Produktplanung, Release oder Supportende	tragfähige Supportentscheidung
Change and Revalidation	Produkt-, Lieferanten-, Bedrohungs-, Support- betroffene Entscheide erneut geprüft oder Rechtsänderung	
Management Review	jährlich oder nach schwerem Ereignis	Ressourcen- und Wirksamkeitsentscheid
Supplier Assurance	regulierter Kunde fragt Nachweis an	kontrolliertes, gültiges Antwortpaket

Das CRA SME Starter Toolkit V1.1 enthält für jeden Arbeitsbereich Auslöser, Pflichtfelder, Entscheid und Abnahmekriterium. Die Felder werden im bestehenden System oder bei Bedarf in einer einzelnen Startervorlage umgesetzt. Gemeinsame Angaben werden nur einmal geführt und über stabile IDs verlinkt.

Technische Dokumentation und EU-Konformitätserklärung bleiben mindestens zehn Jahre nach Inverkehrbringen oder für die Supportdauer verfügbar, je nachdem, welcher Zeitraum länger ist. Löschung oder Sperrung benötigt eine dokumentierte Fristprüfung und Freigabe. Langzeitzachweise bewahren lesbare Exportformate sowie notwendige Tool-, Generator-, Build- und Signaturinformationen. Produkt- oder Vertragspflichten können längere Fristen verlangen.

Anhang A: Verbindliche Feldkataloge

Jeder kontrollierte Datensatz enthält zusätzlich Datensatz-ID, Produkt-ID, Produktversion, Owner, Stellvertretung, Status, Erstell- und Änderungsdatum, Entscheid, Begründung, Nachweislinks, Freigabe und nächste Prüfung. Änderungen überschreiben keinen früheren Entscheid.

A.1 Produktregister

Pflichtfelder: Produkt-ID, Name, Version, Variante, Hersteller-Rechtseinheit, Product Owner, Stellvertretung, Produktgrenze, EU-Zielformate, Lebenszyklusstatus, Release-Datum, Supportbeginn und -ende sowie Links zu Repository, Build, Tickets und Dokumentation. Unklare Version oder Verantwortung führt zur Freigabesperre.

A.2 Anwendbarkeit und Klassifikation

Pflichtfelder: gewerbliche Bereitstellung entgeltlich oder unentgeltlich, EU-Bezug, Produktgrenze, Remote-Datenverarbeitung, Herstellerrolle, weitere Wirtschaftsakteure, Schweizer EU-Marktweg, Ausnahme und Fundstelle, Produktklasse, Rechtsaktversion, Normenstatus, Konformitätsweg und nächste Prüfung. Ungeklärter Scope, Marktweg, Anhang-III-/IV-Treffer oder Konformitätsweg führt zur Übergabe an eine Fachstelle und Freigabesperre.

A.3 ENISA Assessment und Verbesserungsplan

Pflichtfelder: Assessment-Version, Scope, Datum, 25 Antworten, Nachweis pro Antwort, Domänenwerte, Reifegradband, priorisierte Lücke, Massnahme, Owner, Termin, Abnahmekriterium und Abschlussnachweis. Gesetzlich fällige und hochriskante Lücken kommen zuerst; Reifegrad ist kein Konformitätsentscheid.

A.4 Produktrisikobeurteilung

Pflichtfelder: Risiko-ID, Schutzgut, Bedrohung, Fehlgebrauch, Schwachstelle, Auswirkung und Wahrscheinlichkeit von 1 bis 4, Ausgangswert, Massnahmen, Owner, Termin, Restrisikowert, Akzeptanzbefugnis und Nachweise. Hohe Restrisiken benötigen Geschäftsführung, Product Owner und Security. Nicht akzeptierbare Risiken dürfen nicht freigegeben werden.

A.5 Komponenten-, Lieferanten- und SBOM-Nachweis

Pflichtfelder: Produkt- und Build-ID, SBOM-Format und -Version, Komponentename, Version, Lieferant oder Herkunft, eindeutiger Bezeichner, direkte oder transitive Beziehung, Hash soweit erzeugbar, Lizenz soweit bekannt, Supportstatus, Erzeugungszeitpunkt, Generatorversion, Qualitätsstatus und Nachweislink. Eine Betroffenheitsaussage ergänzt Advisory, Status, Exposition oder Erreichbarkeit, Begründung, Prüfer und Gültigkeit.

A.6 Release Gate

Pflichtfelder: Produkt-, Build- und Release-ID, Scope, Klasse, Risikostatus, SBOM- und Triage-Status, Tests, Dokumentationsindex, Normenstatus mit Datum, Konformitätsweg, Nutzerinformation, Zielmarktsprachen, EU-Konformitätserklärung, CE-Kennzeichnung, Supportdauer, PSIRT-Bereitschaft, Entscheider und Zeitpunkt. Der Entscheid lautet Freigabe, Freigabesperre oder Marktbereitstellungsstopp. Eine unbeantwortete Pflichtfrage verhindert die Freigabe. P1 darf nicht akzeptiert werden. P2 benötigt die eng begrenzte gemeinsame Ausnahmeentscheidung mit Kompensationsmassnahme und Fixtermin.

A.7 PSIRT- und Schwachstellenfall

Pflichtfelder: Fall-ID, Eingangszeit und Kanal, Produktversion, Komponente, Quelle, Betroffenheit, Exposition, Erreichbarkeit, Auswirkung, Priorität P1 bis P4, aktive Ausnutzung, schwerer Vorfall, dokumentierter Kenntniszeitpunkt mit Zeitzone und Begründung, Owner, Stellvertretung, Massnahme, Meldeentscheid, Nutzerinformation, Fix, Abschluss und Nachweise. Unklarheit über Trigger oder Kenntniszeitpunkt wird nicht als Nein behandelt.

A.8 Support und End of Support

Pflichtfelder: Nutzungsdauer und Begründung, Supportbeginn und -ende, Personal, Komponenten- und Buildfähigkeit, Signierschlüssel, Testumgebung, Kontakt, Updateverfügbarkeit, letzte Version, Restrisiken, Nutzerinformation, Migration, Datenausserbetriebnahme und Freigabe. Fehlende Betriebsfähigkeit führt zur Freigabesperre.

A.9 Managementprüfung

Pflichtfelder: Portfolio, hohe Risiken, P1/P2-Fälle, Meldungen, Support, Ressourcen, Stellvertretungen, Tool- und Lieferantenprobleme, ENISA-Massnahmen, Wirksamkeitsbefunde, Entscheide, Owner und Termine. Jeder wesentliche Befund benötigt einen ausdrücklichen Entscheid und nächsten Schritt.

A.10 Lieferantennachweis für regulierte Kunden

Pflichtfelder: Kunde, Produktversion, Rechts- oder Vertragsgrund, angeforderter Nachweis, freigegebener Inhalt, Vertraulichkeit, Gültigkeitsdauer, Freigabe, Übermittlungsweg und Ablaufdatum. CRA-Nachweise, NIS2- oder DORA-Kundenanforderungen und freiwillige Aussagen bleiben getrennt; vertrauliche Inhalte werden nicht automatisch offengelegt.

Anhang B: Methodischer Hintergrund

Digital.gov führt die Leserorientierung: Informationen müssen relevant, auffindbar, verständlich und nutzbar sein. Die Playbook-Muster der Cybersecurity and Infrastructure Security Agency strukturieren operative Auslöser, Rollen, Entscheidungen, Eskalationen und kontrollierte Datensätze. Die CMMI-Analogie erklärt schrittweise Verbesserung, ohne Compliance-Stufen zu schaffen. Der 4T2 Governance Writing Standard verbindet diese offenen Methoden mit Schweizer Standarddeutsch und kontrollierter Terminologie. Diese Methoden helfen beim Schreiben und Prüfen; sie begründen keine CRA-Konformität.

Offizielle Rechtsquellen und ihre Funktion

Quelle	Funktion im Manual
Verordnung (EU) 2024/2847	verbindlich; führende und unmittelbar anwendbare CRA-Rechtsgrundlage für Scope, Rollen, Pflichten, Fristen, Konformität und Unterstützung; geprüft am 30. Juli 2026
Durchführungsverordnung (EU) 2025/2392 der Kommission vom 28. November 2025	in Kraft; verbindliche technische Beschreibung der wichtigen und kritischen Produktkategorien aufgrund von Artikel 7 Absatz 4 CRA; geprüft am 30. Juli 2026
Delegierte Verordnung (EU) 2025/1535	verbindlich; begrenzte Ausnahme für bestimmte Produkte im Anwendungsbereich der Verordnung (EU) № 168/2013; geprüft am 30. Juli 2026
Delegierte Verordnung (EU) 2026/881 der Kommission vom 11. Dezember 2025	seit 10. Mai 2026 in Kraft; eng begrenzte Ergänzung zu Artikel 14 Absatz 9 CRA für die verzögerte Weitergabe von Meldungen; keine allgemeine Fristverlängerung; geprüft am 30. Juli 2026

Quelle	Funktion im Manual
Delegierte Verordnung (EU) 2026/339 der Kommission vom 16. Februar 2026	in Kraft; hebt die Delegierte Verordnung (EU) 2022/30 zum 11. Dezember 2027 auf und dokumentiert den Übergang betroffener Funkanlagen von RED-Cybersicherheitsanforderungen zum CRA; geprüft am 30. Juli 2026
Verordnung (EU) 2019/1020	verbindlich, soweit anwendbar; ergänzende Marktüberwachungs- und EU-Wirtschaftsakteurregeln über Artikel 66 CRA und den konkreten EU-Marktweg; geprüft am 30. Juli 2026
Empfehlung 2003/361/EG , Anhang	nicht selbst die CRA-Grundlage; führt über Artikel 3 Nummer 19 CRA die KMU-Definition, aber keine Produktsicherheitspflichten; geprüft am 30. Juli 2026
FAQ der Europäischen Kommission zur CRA-Umsetzung	offizielle, nicht bindende Umsetzungshinweise; Version 1.3 vom 1. Juli 2026, Website geprüft am 30. Juli 2026
ENISA Single Reporting Platform	offizielle, nicht bindende Betriebsinformation; aktualisiert am 17. Juli 2026 und geprüft am 30. Juli 2026

Die Reihenfolge des Jahres ist kein Autoritätsmassstab. Entscheidend ist, ob der aktuelle CRA eine ältere Definition oder Regel ausdrücklich einbezieht. Nicht einbezogene ältere Dokumente dürfen keine CRA-Pflicht begründen.

Umsetzungsmethoden und nicht bindende Hilfen

- [ENISA SME Cyber Resilience Maturity Assessment Model](#)
- [Digital.gov Plain Language Guide](#)
- [CISA Incident and Vulnerability Response Playbooks](#)
- [ENISA CRA Maturity Model Tool](#)
- [ENISA SME CRA Survey Report](#)
- [ENISA Technical Advisory for Secure Use of Package Managers](#)
- [ENISA SBOM Adoption State of Play 2026](#)

Glossar

Begriff	Praktische Bedeutung
CRA	Cyber Resilience Act, Verordnung (EU) 2024/2847; gesetzliche Grundlage des Manuals
ENISA	Agentur der Europäischen Union für Cybersicherheit; ihr SME-Modell und Excel führen den praktischen Reifegradweg
KMU	kleine und mittlere Unternehmen einschliesslich Kleinunternehmen gemäss EU-Definition
Evidence (Nachweis)	nachvollziehbarer Beleg einer Entscheidung, Handlung oder Wirksamkeit

Begriff	Praktische Bedeutung
kontrollierter Datensatz (Datensatz)	versionierter Datensatz mit ID, Owner, Status, Datum und Nachweisverweis
SBOM	maschinenlesbares, versioniertes Verzeichnis der Softwarekomponenten eines Produkts
PSIRT	Product Security Incident Response Team; im KMU eine erreichbare Bereitschaftsfunktion, nicht zwingend eine Abteilung
dokumentierter Kenntniszeitpunkt	frühester dokumentierbarer Zeitpunkt, zu dem dem Hersteller verfügbare verlässliche Tatsachen vorliegen, welche die gesetzliche Meldeschwelle erfüllen; eine spätere Prüfung verschiebt ihn nicht
Release Gate	dokumentierter Entscheid Freigabe, Freigabesperre oder Marktbereitstellungsstopp für eine bestimmte Produktversion
NIS2	EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau; hier relevant für zusätzliche Kundenanforderungen
DORA	EU-Verordnung zur digitalen operationalen Resilienz im Finanzsektor; hier nur als möglicher Kundenkontext
CMMI	Reifegradmodell, das im Manual nur als Analogie für schrittweise Verbesserung dient
CE-Kennzeichnung	Kennzeichnung, mit der der Hersteller erklärt, dass das Produkt die anwendbaren Anforderungen der einschlägigen EU-Harmonisierungsrechtsakte erfüllt und er dafür Verantwortung übernimmt; die schriftliche Erklärung ist die EU-Konformitätserklärung
JSON, CycloneDX und SPDX	technische Formate oder Standards für maschinenlesbare SBOMs; die konkrete Wahl folgt Produkt und aktuellem Rechtsstand
CI/CD	automatisierte Integration, Prüfung und Bereitstellung von Softwareänderungen; hier ein möglicher Ort für SBOM-Erzeugung und Scans
SCA	Software Composition Analysis; Werkzeugklasse für Komponenten- und Schwachstellenanalyse, deren Ergebnisse eine fachliche Triage benötigen
DMS	Dokumentenmanagementsystem; möglicher kontrollierter Ablageort für freigegebene technische Nachweise
GF, PO, ENG, SEC und Q/C	Rollenabkürzungen der Prozesslandkarte für Geschäftsführung, Product Owner, Engineering, Security oder PSIRT sowie Quality/Compliance
Digital.gov Plain Language	offene Methode für leserorientierte, auffindbare, verständliche und testbare Information
CISA-Playbook-Muster	offene Strukturhilfe für Auslöser, Rollen, Entscheidungen, Eskalationen und Datensätze
4T2 Governance Writing Standard	interner Ausführungsstandard für Schweizer Standarddeutsch, kontrollierte Terminologie und die Verbindung von Management-, Fach- und Prozesssprache

Bekannte Einschränkungen

Das vereinfachte Dokumentationsformat, harmonisierte Normen und Plattformdetails bleiben unter Regulatory Watch. Ein repräsentativer externer KMU-Lesertest folgt vor der ersten planmässigen

Wirksamkeitsüberprüfung. Vor V1.1 konnten zwei umfangreiche Fachreviews, aber kein vollständiger beobachteter Test mit drei bis fünf repräsentativen KMU-Anwendern durchgeführt werden. Martin Bischoff hat diese Einschränkung für die Veröffentlichung bewusst akzeptiert. Sie begrenzt die Aussage zur extern nachgewiesenen Praxiserprobung, nicht die dokumentierte fachliche Prüfung. Der 20-Produkte-Skalierungsbefund ist geschlossen.

Bei Funkanlagen wird die Aufhebung der Delegierten Verordnung (EU) 2022/30 durch die Delegierte Verordnung (EU) 2026/339 zum 11. Dezember 2027 beobachtet. Daraus folgt keine allgemeine zusätzliche CRA-Pflicht.

Haftungs- und Anwendungshinweis

Dieses Manual und das zugehörige Starter Toolkit sind eine allgemeine, praxisorientierte Arbeitsgrundlage. Sie sind keine Rechtsberatung, keine technische Produktprüfung und keine Konformitätsbewertung. Anwendbarkeit, Wirtschaftsrolle, Produktklasse, Sektorschnittstellen, Konformitätsweg und Nachweise müssen für jedes reale Produkt und jeden Marktweg fachkundig entschieden werden. Verbindliche Rechtsakte und zuständige Behörden gehen diesem Dokument vor.

Copyright und offene Lizenz

Copyright © 2026 Martin Bischoff. Originaltext und 4T2-erstellte Grafiken dieser V1.1 stehen unter CC BY 4.0. Rechte Dritter sowie Namen, Logos und Marken von 4T2 bleiben ausgenommen.

Transparenz zur Erstellung

Martin Bischoff setzte generative AI für Strukturierung, Rechercheunterstützung, Formulierung, redaktionelle Prüfung und Grafikvorbereitung ein. Fachliche Freigabe, produktbezogene Entscheidungen und Veröffentlichung bleiben menschliche Verantwortung.