EIN TRUSTTROIAI-WERKZEUG

Board Assurance Checklist.

Fünfzehn Kontrollen, die Ihr Vorstand vor jeder CRA-Prüfung, jedem Audit und jeder Investor-Konversation zur Hand haben sollte. Board-Perspektive statt Legal-Perspektive.

VERSION	SPRACHE	KONTROLLEN	BASIS
1.0 · August 2026	Deutsch	15 in 5 Bereichen	CRA · Anhang I und VII

Diese Checklist übersetzt die grundlegenden CRA-Anforderungen in eine Sprache, die ein Vorstand versteht und beantworten kann. Sie ist **kein Ersatz** für die technische Dokumentation nach Anhang VII, sondern das Vorlage-Instrument, das der Vorstand vor jedem Release-Zyklus, jedem Audit und jeder Investor-Prüfung zur Hand hat.

INHALT

01 Risikomanagement und Security by Design

02 Governance und Dokumentation

03 Vulnerability und Patch Management

04 Produktlebenszyklus

05 Awareness und Skills

BEREICH 1 VON 5

Risikomanagement und Security by Design

Ob Ihr Produkt CRA-konform entwickelt wurde, entscheidet sich nicht in der Konformitätsbewertung, sondern in der Design-Phase.

Kontrolle 1-1 Documented Risk Assessment

BOARD-FRAGE

Können Sie die Cybersicherheits-Risikobewertung für Ihr wichtigstes Produkt in unter fünf Minuten vorzeigen, mit Datum, Verantwortlichem und Trigger-Regeln?

NACHWEIS-MUSTER

Versionskontrolliertes Dokument im Repository oder Wiki, mit Prozess-Beschreibung, Auslöser-Katalog und Verantwortlichkeits-Zuordnung.

QUELLE · CRA Article 13(2)

Kontrolle 1-2 Threat Modelling as Release Gate

BOARD-FRAGE

Ist das Threat Modelling ein Release-Gate, das nicht übersprungen werden kann, oder eine Empfehlung, die im Zeitdruck entfällt?

NACHWEIS-MUSTER

Release-Checkliste mit Threat-Modelling-Punkt und dokumentierten Ausnahmen mit Genehmiger und Ablaufdatum.

QUELLE · CRA Annex I, Part 1

Kontrolle 1-3 Supply Chain Risk Register

BOARD-FRAGE

Wissen Sie im Fall eines kritischen CVE innerhalb von 24 Stunden, welche Ihrer Produkte betroffen sind?

NACHWEIS-MUSTER

SBOM pro Release, automatisch gegen CVE-Feeds abgeglichen, mit Verantwortlichem für die Triage.

QUELLE · CRA Annex I, Part 2 (PT2.1)

BEREICH 2 VON 5

Governance und Dokumentation

Die technische Dokumentation nach Anhang VII muss zehn Jahre aufbewahrt werden. Prüfen Sie, ob sie lebt oder beim ersten Audit als Fassade zusammenbricht.

Kontrolle 2-1 Current Technical File

BOARD-FRAGE

Spiegelt Ihre technische Dokumentation die derzeit ausgelieferte Produktversion wider, oder die Version von vor drei Releases?

NACHWEIS-MUSTER

Versionskontrolliertes Dokument mit Zeitstempel der letzten Aktualisierung, verknüpft mit dem aktuellen Release-Tag.

QUELLE · CRA Article 31, Annex VII

Kontrolle 2-2 Named Cyber-Compliance Owner

BOARD-FRAGE

Wer trifft bei Ihnen die Meldepflicht-Entscheidung nach Artikel 14 innerhalb von 24 Stunden, wenn heute Nacht ein Zero-Day auftritt?

NACHWEIS-MUSTER

Benannte Person mit dokumentierter Vertretungs-Regelung, Zugang zur ENISA-Meldeplattform bereits eingerichtet und getestet.

QUELLE · CRA Article 14, ab 11. September 2026

Kontrolle 2-3 Board-Level Risk Integration

BOARD-FRAGE

Steht Produkt-Cybersicherheit auf der Tagesordnung Ihrer regelmäßigen Geschäftsleitungs-Prüfung, oder existiert sie parallel in einem Tools-Team?

NACHWEIS-MUSTER

Protokolle der letzten drei Geschäftsleitungs-Sitzungen mit Cybersicherheits-Tagesordnungspunkt, Cybersicherheitsrisiken im Unternehmens-Risikoregister.

QUELLE · CRA Article 13(1), Article 64

BEREICH 3 VON 5

Vulnerability und Patch Management

Vulnerability-Management ist die Domäne, in der Konformität in Echtzeit sichtbar wird. Prüfen Sie, ob Sie im Ernstfall handlungsfähig sind.

Kontrolle 3-1 Public Vulnerability Disclosure Policy

BOARD-FRAGE

Können externe Sicherheitsforscher Sie erreichen, oder müssen sie über den allgemeinen Support-Eingang gehen?

NACHWEIS-MUSTER

Veröffentlichte CVD-Richtlinie auf der Produktwebsite, security.txt-Datei auf den öffentlichen Domänen, dokumentierter Test-Report mindestens einer echten Meldung.

QUELLE · CRA Annex I, Part 2 (PT2.5, PT2.6)

Kontrolle 3-2 Vulnerability SLA Tracked and Met

BOARD-FRAGE

Kennen Sie Ihre eigene Zeit von Vulnerability-Meldung bis Patch-Release, und liegt sie öfter innerhalb Ihrer SLA als außerhalb?

NACHWEIS-MUSTER

Vulnerability-Tracking-Board mit Schweregrad, Verantwortlichem, Zielterminen und tatsächlicher Behebungszeit, Trend-Auswertung der letzten drei Monate.

QUELLE · CRA Annex I, Part 2 (PT2.2, PT2.7)

Kontrolle 3-3 Article 14 Reporting Playbook Tested

BOARD-FRAGE

Wurde Ihr Meldepflicht-Prozess mindestens einmal an einem realen Sicherheitsereignis getestet, oder ist er ein Papier-Prozess?

NACHWEIS-MUSTER

Dokumentierte Meldepflicht-Entscheidung für mindestens ein Ereignis, mit Zeit-Stempel und Begründung, auch bei Nicht-Meldepflicht.

QUELLE · CRA Article 14, ab 11. September 2026

BEREICH 4 VON 5

Produktlebenszyklus

Der Unterstützungszeitraum ist die längste vertragliche Verpflichtung im CRA. Prüfen Sie, ob Sie diese Verpflichtung mit Ressourcen und Prozessen unterlegen können.

Kontrolle 4-1 Support Period Decision Record

BOARD-FRAGE

Ist das Ende-Datum des Unterstützungszeitraums für jedes Ihrer Produkte zum Kaufzeitpunkt sichtbar, und ist die Wahl begründet?

NACHWEIS-MUSTER

Support Period Decision Record pro Produkt mit Begründung der Dauer, Enddatum sichtbar auf Produktseite oder Datenblatt.

QUELLE · CRA Article 13(8), Article 13(19)

Kontrolle 4-2 Secure Update Mechanism

BOARD-FRAGE

Werden Ihre Sicherheitsupdates kryptographisch signiert, sicher verteilt und mit Rollback-Möglichkeit ausgeliefert, oder sind sie ein einfaches Datei-Ersetzen?

NACHWEIS-MUSTER

Dokumentierter Update-Prozess mit Signierung, Integritätsprüfung, Rollback-Testfall aus dem letzten Release-Zyklus.

QUELLE · CRA Annex I, Part 1 (PT1.2.c), Part 2 (PT2.7, PT2.8)

Kontrolle 4-3 End-of-Life Communication Plan

BOARD-FRAGE

Wissen Ihre Nutzer, was passiert, wenn der Unterstützungszeitraum endet, und gibt es einen Migrations-Pfad?

NACHWEIS-MUSTER

End-of-Life-Plan-Vorlage mit Kommunikations-Fahrplan, Migrations-Anleitung und dokumentierten früheren EOL-Kommunikationen.

QUELLE · CRA Article 13, Annex II

BEREICH 5 VON 5

Awareness und Skills

Ohne kompetentes Team bleiben alle anderen Kontrollen Papier. Prüfen Sie, ob die Menschen, die die Konformität herstellen sollen, die Voraussetzungen dafür haben.

Kontrolle 5-1 Secure Coding Baseline Enforced

BOARD-FRAGE

Existiert ein Secure-Coding-Standard für Ihren Haupt-Stack, ist er in der CI-Pipeline durchgesetzt, und wird er tatsächlich befolgt?

NACHWEIS-MUSTER

Einseitige Basis-Datei im Repository, SAST-Regeln, die zu den verbotenen Mustern passen, PR-Checkliste mit Verweis auf die Basis.

QUELLE · CRA Annex I, Part 1 (PT1.2.a), Part 2 (PT2.3)

Kontrolle 5-2 Peer Review for Security-Sensitive Changes

BOARD-FRAGE

Können sicherheitsrelevante Änderungen an Authentifizierung, Kryptografie oder externen Schnittstellen ohne ein zweites Paar Augen in Produktion gehen?

NACHWEIS-MUSTER

CODEOWNERS-Datei mit sicherheitsrelevanten Pfaden, geschützte Branches mit PR-Review-Anforderung, Beleg der Durchsetzung im letzten Release.

QUELLE · CRA Annex I, Part 2 (PT2.3)

Kontrolle 5-3 Continuous Learning Loop

BOARD-FRAGE

Wenn ein Vorfall passiert, wird die Erkenntnis in Design und Prozess zurückgeführt, oder bleibt sie im Gedächtnis der Beteiligten?

NACHWEIS-MUSTER

Post-Incident-Review-Vorlage, mindestens ein Backlog-Element aus einer Review im letzten Quartal, Aktualisierung der Risikobewertung dokumentiert.

QUELLE · CRA Recital 15, Annex I Part 2 (PT2.3)

WENN SIE EINE LÜCKE SEHEN

Die Checklist zeigt Lücken. Der Inspektor macht sie handhabbar.

Jede der fünfzehn Kontrollen entspricht einer oder mehreren aktiven Prüfungen im Inspektor. Wenn Sie eine Kontrolle mit "nicht belegt" markieren müssten, erscheint sie im Inspektor als konkretes Ticket in Ihrem Jira-Projekt, mit signierten Werkstücken zur direkten Umsetzung.

Der Inspektor liest nur, was Ihr Team ohnehin sehen kann. Die Installation ist kostenfrei. Jeder Skill trägt die Signatur einer Compliance-Expertin oder eines Compliance-Experten über Cronos.

Inspektor für Jira installieren →

Über dieses Dokument. Die Board Assurance Checklist ist eine TrustTroiAI-Ressource, gebaut auf Basis des Cyber Resilience Act (Verordnung EU 2024/2847) und der ENISA Secure by Design and Default Playbook v1.0 (CC BY 4.0). Dieses Dokument ist ein Orientierungs-Instrument, keine Rechtsberatung und kein Konformitätsbewertungsverfahren.