

Cybersecurity-Risikoanalyse für Maschinenbauer

Prozessleitfaden zur Durchführung einer
Threat Analysis and Risk Assessment (TARA)
nach IEC 62443 mit CRA- und MV-Compliance

Basierend auf: IEC 62443-3-2 (Security Risk Assessment for System Design)

Erweitert um: CRA (EU) 2024/2847 und MV (EU) 2023/1230

Methodik: IEC 62443-3-2, STRIDE, MITRE ATT&CK for ICS



Alpina Connect GmbH

www.alpinaconnect.com

Version 1.0 — März 2026

Nur zur Information, keine Rechtsberatung.



Inhaltsverzeichnis

Inhaltsverzeichnis	2
Einleitung	3
Zielgruppe	3
Warum jetzt?	3
Werkzeuge in diesem Prozess	3
Prozessübersicht	4
Zur Qualitätssicherung: Reviews im Prozess	5
Schritt-für-Schritt-Anleitung	5
Schritt 1 — Security Context definieren	5
Schritt 2 — Security Level Target festlegen	6
Schritt 3 — Architektur & Security Zones erstellen	7
Schritt 4 — Assets ermitteln	8
Schritt 5 — Bedrohungen identifizieren (STRIDE)	9
Schritt 6 — Risikobewertung (Ist-Zustand)	11
Schritt 7 — Risikobehandlung definieren	13
Hands-on Beispiel: Risikobehandlung am Beispiel eines IPC mit CNC-Steuerung	13
Schritt 8 — Restrisiko bewerten	15
Fortsetzung Beispiel: Restrisiko für A01_Sp_01 und A01_Ta_01	15
Schritt 9 — Compliance-Mapping (CRA/MV)	16
Schritt 10 — Dokumentation zusammenführen	18
Zusammenfassung	20

Einleitung

Dieses Dokument beschreibt einen pragmatischen, durchgehenden Prozess zur Durchführung einer Cybersecurity-Risikoanalyse (Threat Analysis and Risk Assessment, TARA) für Maschinenbauer. Der Prozess basiert auf der Methodik nach IEC 62443-3-2, ergänzt um die regulatorischen Anforderungen des Cyber Resilience Act (CRA) und der Maschinenverordnung (MV). Jeder Schritt ist mit konkreten Werkzeugen verknüpft und produziert ein dokumentiertes Ergebnis.

Zielgruppe

Entwicklungsleiter, Safety/Security-Verantwortliche, Projektleiter und Compliance-Manager bei Schweizer und EU-Maschinenbauern, die vernetzte Industrieprodukte (CNC-Maschinen, Verpackungsmaschinen, Automationsanlagen) entwickeln und in Verkehr bringen.

Warum jetzt?

Drei regulatorische Fristen konvergieren in den nächsten 24 Monaten:

Frist	Regulierung	Bedeutung
Sep. 2026	CRA Meldepflicht (Art. 14)	24h-Meldung bei aktiv ausgenutzten Schwachstellen
Jan. 2027	Maschinenverordnung	MV ersetzt MRL 2006/42/EG, Cybersecurity in Anh. III
Dez. 2027	CRA vollständig anwendbar	Alle Anforderungen aus Anhang I gelten

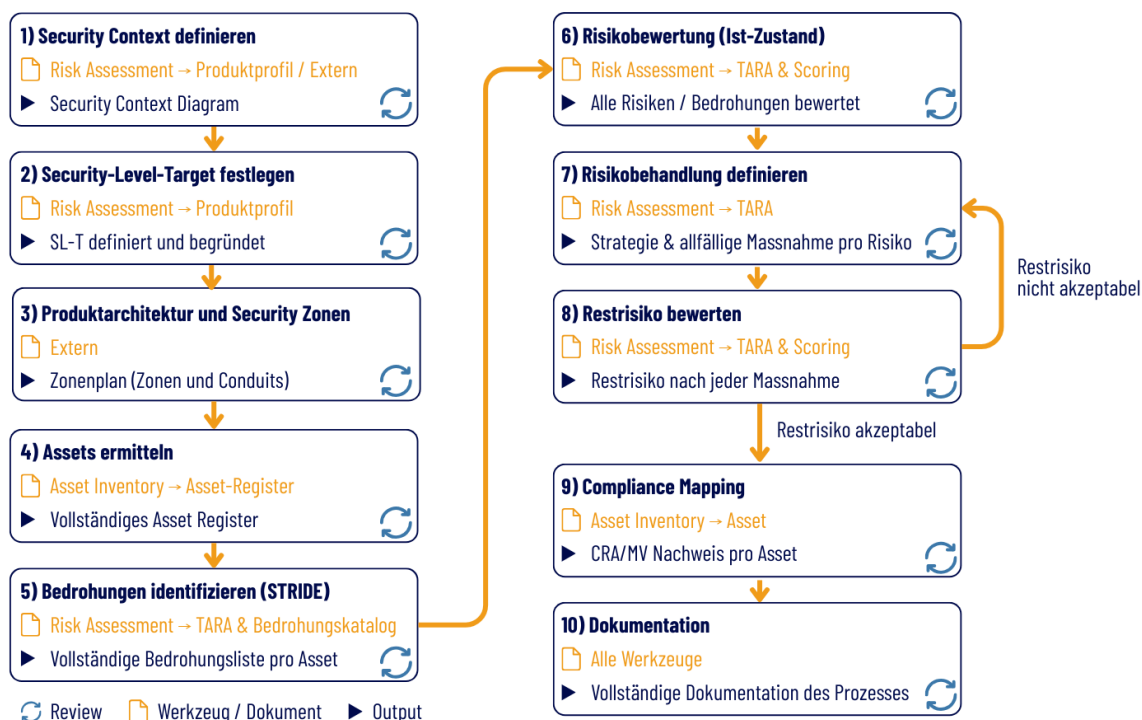
Werkzeuge in diesem Prozess

Der Prozess nutzt zwei separate Excel-Vorlagen, die aufeinander aufbauen:

Werkzeug	Zweck	Enthält
TARA-Vorlage(Risk Assessment)	Bedrohungsanalyse und Risikobewertung pro Produkt	Scoring-Dimensionen, Produktprofil, Bedrohungskatalog (125 Threats), TARA-Sheet, Dashboard
Asset Compliance Tool(Asset Inventory)	Regulatorische Compliance-Bewertung pro Asset	Asset-Register, 15 Asset-Compliance-Blätter, Dashboard, CRA×MV Referenz

Prozessübersicht

Der Prozess folgt einer 10-Schritte-Methodik. Die Schritte 1–8 basieren auf IEC 62443-3-2. Die Schritte 9–10 sind Alpina-Connect-Erweiterungen, die den regulatorischen Nachweis gegenüber CRA und MV sicherstellen. Jeder Schritt produziert ein dokumentiertes Ergebnis, das in die technische Dokumentation nach CRA Anhang VII einfließt.



#	Schritt	Werkzeug / Blatt	Output
1	Security Context definieren	TARA → Produktprofil	Security Context Diagramm
2	Security Level Target festlegen	TARA → Produktprofil	SL-T Definition und Dokumentation
3	Architektur & Security Zones	Netzwerkdigramm (extern)	Zonenplan mit Zones & Conduits
4	Assets ermitteln	Asset Inventory → Asset-Register	Vollständiges Asset-Register
5	Bedrohungen identifizieren (STRIDE)	TARA → TARA-Sheet + Katalog	Bedrohungsliste pro Asset
6	Risikobewertung (Ist-Zustand)	TARA → TARA-Sheet + Scoring	Bewertete Risiken
7	Risikobehandlung definieren	TARA → TARA-Sheet	Strategie + Massnahmen pro Risiko
8	Restrisiko bewerten	TARA → TARA-Sheet (Soll)	Residualrisiko + Test Cases
9	Compliance-Mapping (CRA/MV)	Asset Inventory → Asset-Blätter	CRA/MV-Nachweis pro Asset

#	Schritt	Werkzeug / Blatt	Output
10	Dokumentation zusammenführen	Alle Werkzeuge	Vollständige technische Dokumentation

Zur Qualitätssicherung: Reviews im Prozess

Ein zentraler Erfolgsfaktor für die Qualität und Vollständigkeit der TARA ist die systematische Überprüfung jedes Prozessschritts. Wir empfehlen, nach jedem Schritt die Ergebnisse von einer Person prüfen zu lassen, die nicht direkt am jeweiligen Arbeitsschritt beteiligt war. Dies kann eine interne Fachperson (z.B. aus Safety, Entwicklung oder Qualität) oder ein externer Berater sein.

Die Review-Praxis dient zwei Zwecken: Erstens werden Lücken und Inkonsistenzen früh erkannt, bevor sie sich durch den gesamten Prozess ziehen. Zweitens entsteht eine dokumentierte Prüfspur, die bei einem Audit oder einer Konformitätsbewertung den Nachweis der Sorgfalt erleichtert.

In diesem Dokument kennzeichnet das Symbol «✓ Review-Checkpoint» am Ende eines Schritts, dass ein Review empfohlen wird.

Schritt-für-Schritt-Anleitung

Schritt 1 — Security Context definieren

Ziel: Die physische und logische Umgebung der Maschine dokumentieren und die Systemgrenze klar abgrenzen.

Werkzeug: TARA-Vorlage → Blatt «Produktprofil»

Output: Security Context Diagramm mit dokumentierter Systemgrenze

Der Security Context bildet die Grundlage für alle weiteren Schritte. Er beschreibt, in welcher Umgebung die Maschine betrieben wird und wo die Grenze zwischen Ihrem Produkt und der Verantwortung des Betreibers liegt. Ohne einen klar definierten Security Context ist eine sinnvolle Risikoanalyse nicht möglich.

Beschreiben Sie die vorgesehene Einsatzumgebung: Wer hat physischen Zugang zur Maschine? In welchem Netzwerksegment steht sie? Welche externen Systeme kommunizieren mit der Maschine (MES, ERP, Cloud, Remote-Service)? Wo endet die Systemgrenze — was gehört zum Produkt, was zum Betreiber?

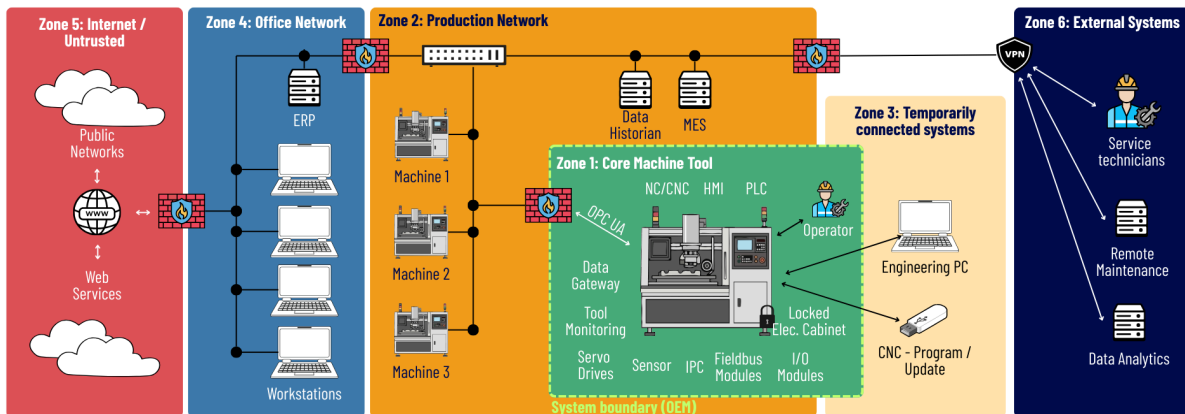
Der Security Context beantwortet zwei Kernfragen:

- **Physische Umgebung:** Zutrittskontrolle, Schaltschrankverriegelung, Bedienerpersonal, Aufstellungsort
- **Logische Umgebung:** Netzwerkposition, Firewalls, Protokolle, Cloud-Anbindung, Remote-Access

Nutzen Sie das Blatt «Produktprofil» in der TARA-Vorlage, um alle relevanten Informationen strukturiert zu erfassen. Das Blatt enthält Felder für allgemeine Produktangaben, die bestimmungsgemäße Verwendung, eine Checkliste für vorhersehbare Cyber-Fehlanwendungen (CRA Recital 22) und die digitale Architektur.

Vorhersehbare Cyber-Fehlanwendungen (Checkliste im Produktprofil):

- Maschine ohne Firewall/Segmentierung direkt im Firmennetz betrieben
- Default-Passwörter auf Steuerung, HMI oder Remote Access nicht geändert
- USB-Ports für beliebige Medien zugänglich, ohne Kontrolle
- Remote Access dauerhaft aktiv statt on-demand
- Keine Netzwerk-Überwachung / kein Logging aktiviert
- Sicherheitsupdates werden nicht eingespielt
- Bediener hat Admin-/Root-Rechte auf dem HMI-IPC



Praxistipp

Beginnen Sie mit einer Skizze auf Papier oder Whiteboard. Zeichnen Sie die Maschine in die Mitte und alle Systeme, die mit ihr kommunizieren, drumherum. Markieren Sie dann die Systemgrenze — alles innerhalb ist Ihre Verantwortung als OEM.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 2 — Security Level Target festlegen

Ziel: Das angestrebte Schutzniveau für die Maschine nach IEC 62443 definieren.

Werkzeug: TARA-Vorlage → Blatt «Produktprofil», Feld «Security Level Target»

Output: Dokumentiertes SL-T mit Begründung

IEC 62443 definiert vier Security Levels (SL-1 bis SL-4), die den Schutzgrad gegen unterschiedliche Angriffsprofile beschreiben. Für Werkzeugmaschinen empfiehlt der VDW (Verein Deutscher Werkzeugmaschinenfabriken) ein einheitliches Security Level Target von SL-T 2 als Minimum für das gesamte System.

SL	Schutz gegen	Angreiferprofil
SL-1	Zufälliger, unbeabsichtigter Zugriff	Keine böse Absicht
SL-2	Vorsätzlicher Angriff mit einfachen Mitteln	Geringer Aufwand, allgemeine Kompetenzen
SL-3	Angriff mit fortgeschrittenen Mitteln	Spezifisches Wissen, signifikante Ressourcen
SL-4	Angriff mit staatlichen/hochentwickelten Mitteln	Hohes Motivation, umfangreiche Ressourcen

SL-2 bedeutet: Die Maschine muss gegen vorsätzliche Angriffe geschützt sein, die mit einfachen Mitteln, geringem Aufwand und allgemeinen Kompetenzen durchgeführt werden. Für die Mehrzahl der Maschinenbauer ist dies der richtige Ausgangspunkt.

Dokumentieren Sie das gewählte SL-T im Produktprofil. Falls einzelne Zonen ein höheres SL-T erfordern (z.B. eine Safety-PLC, die SL-T 3 benötigt), halten Sie dies separat fest.

Praxistipp

Unterscheiden Sie zwischen dem Target (SL-T) und dem erreichten Level (SL-C, Capability). Das SL-T definieren Sie hier — ob und wie Sie es erreichen, zeigt die spätere Risikoanalyse.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 3 — Architektur & Security Zones erstellen

Ziel: Die Maschinenarchitektur in Security Zones unterteilen und Conduits (Zonenübergänge) identifizieren.

Werkzeug: Netzwerkdiagramm-Tool (z.B. draw.io, Visio) oder handschriftliche Skizze

Output: Architekturdiagramm mit markierten Security Zones und Conduits

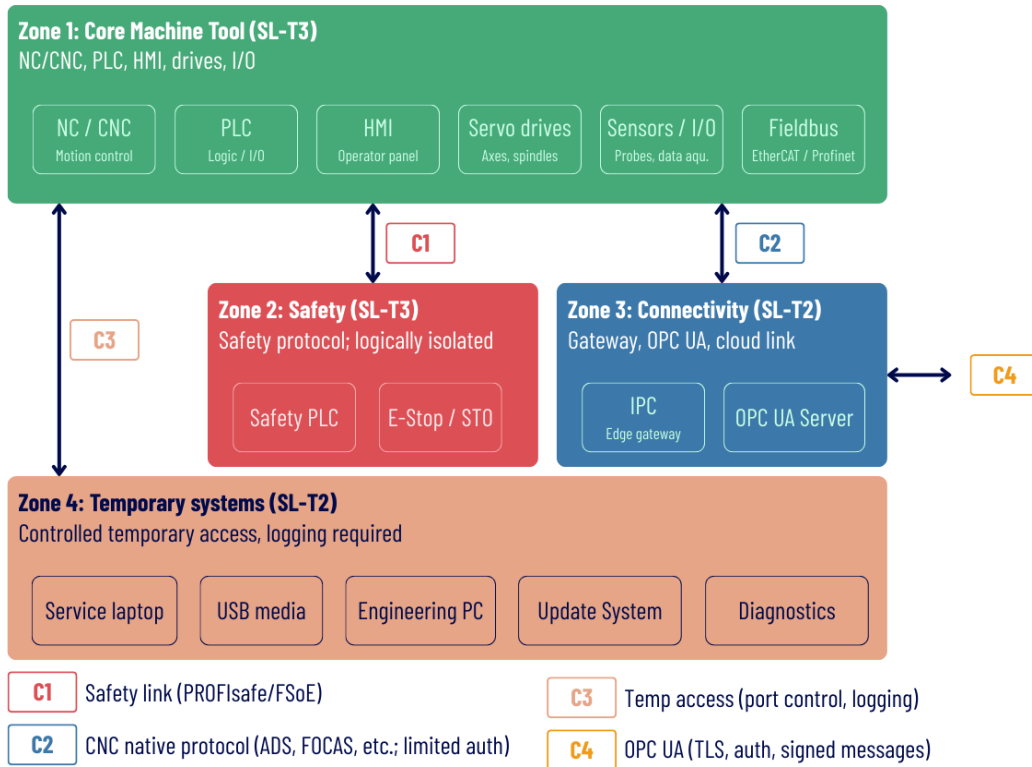
Erstellen Sie ein detailliertes Architekturdiagramm Ihrer Maschine mit allen digitalen Komponenten, Netzwerkverbindungen und Schnittstellen. Gruppieren Sie die Komponenten in Security Zones nach IEC 62443-3-2. Eine Zone ist eine Gruppierung von Assets, die das gleiche Sicherheitsniveau teilen. Ein Conduit ist ein logischer oder physischer Kommunikationskanal zwischen Zonen.

Folgende Zones sollten mindestens unterschieden werden:

- **Zone 1 — Kernmaschine:** NC/CNC, PLC, HMI, Antriebe, Sensoren, I/O-Module, Feldbus
- **Zone 2 — Safety:** Safety-PLC, Not-Halt, Schutztür-Verriegelung (logisch isoliert, ggf. SL-T 3)
- **Zone 3 — Connectivity/Edge:** Gateway, IPC, OPC UA Server, Cloud-Anbindung
- **Zone 4 — Temporär verbundene Systeme:** Service-Laptop, USB-Medien, Engineering-PC, Diagnose-Tools

Definieren Sie für jeden Conduit (Zonenübergang):

- Welche Protokolle werden verwendet (z.B. OPC UA, PROFINET, Ethernet/IP)?
- Welche Authentisierung und Verschlüsselung ist vorhanden?
- Ist die Verbindung permanent oder temporär?



Praxistipp

Markieren Sie in Ihrem Diagramm explizit die Systemgrenze (OEM-Verantwortung). Alles innerhalb der Systemgrenze muss in der TARA bewertet werden. Alles ausserhalb (z.B. Kundennetzwerk, MES) gehört zum Security Context aus Schritt 1.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 4 — Assets ermitteln

Ziel: Alle digitalen Assets der Maschine identifizieren und im Asset-Register erfassen.

Werkzeug: Asset Inventory (Excel) → Blatt «Asset-Register»

Output: Vollständig ausgefülltes Asset-Register

Erfassen Sie jedes digitale Asset Ihrer Maschine im Asset-Register. Ein Asset ist jede Komponente, die Software enthält, Daten verarbeitet oder über eine Netzwerkschnittstelle verfügt. Dieser Schritt konzentriert sich bewusst auf die Identifikation und Beschreibung der Assets — die Bewertung der Schutzziele (CIA) erfolgt später im Rahmen der Bedrohungsanalyse.

Für jedes Asset erfassen Sie im Register:

Feld	Beschreibung	Beispiel
Asset-ID	Eindeutige Kennung (A01, A02, ...)	A01
Bezeichnung	Klartextname des Assets	CNC-Steuerung Fanuc 0i-TF Plus

Feld	Beschreibung	Beispiel
Kategorie	Haupt-Assetklasse	Steuerung
Unterkategorie	Detaillierung	CNC-Steuerung
Hersteller (Eigen/Drittanbieter)	Wer stellt das Asset her?	Drittanbieter
Hersteller-Name	Firmenname	Fanuc
Version / Firmware	Aktuelle Version	v4.1
Beschreibung / Funktion	Was macht das Asset?	NC-Programmausführung, Achssteuerung
Schnittstellen	Kommunikationswege	Ethernet, RS-232, FOCAS2
Safety-relevant?	Ja/Nein	Nein
CRA-Pflicht beim Hersteller?	Komponenten-CRA-Konformität	Ja (Fanuc)
TARA-Referenz	Verknüpfung zu Threat-IDs	T001, T005, T012
Bemerkungen	Zusätzliche Informationen	SBOM bei Fanuc angefordert

Typische Asset-Kategorien im Maschinenbau:

- Steuerungen (CNC, PLC, Safety-PLC, Motion Controller)
- Betriebssysteme und Runtime-Umgebungen (Windows IoT, Linux, VxWorks)
- HMI-Software und Bedienpanels
- Netzwerkkomponenten (Switches, Router, Gateways)
- Firmware (Antriebe, Sensoren, I/O-Module)
- Applikationssoftware (CAM-Postprozessoren, Messsoftware)
- Cloud-Services und Remote-Access-Lösungen
- Schnittstellen und Protokolle (OPC UA, MQTT, FOCAS, DNC/FTP)

Wichtig für Drittkomponenten

Die CRA-Klassifizierungspflicht liegt beim Komponentenhersteller. Ihr Job als Integrator: Due Diligence — CRA-Konformität prüfen, SBOM einfordern, Update-Policy sicherstellen (CRA Recital 34). Dokumentieren Sie den Status im Feld «Bemerkungen».

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 5 — Bedrohungen identifizieren (STRIDE)

Ziel: Systematisch alle relevanten Bedrohungen pro Asset identifizieren und im TARA-Sheet erfassen.

Werkzeug: TARA-Vorlage → Blatt «TARA» + Blatt «Bedrohungskatalog»

Output: TARA-Sheet mit identifizierten Bedrohungen pro Asset und STRIDE-Kategorie

In diesem Schritt übertragen Sie die Assets aus dem Asset-Register (Schritt 4) in das TARA-Sheet und identifizieren für jedes Asset die relevanten Bedrohungen. Die Bewertung der Risiken erfolgt erst im nächsten Schritt — hier geht es ausschliesslich darum, die Bedrohungen systematisch zu erfassen.

Vorgehen:

- **1. Assets übertragen:** Tragen Sie die Asset-IDs und Bezeichnungen aus dem Asset-Register in die Spalte «Asset-ID» des TARA-Sheets ein. Pro Asset wird ein Block von Zeilen angelegt, gruppiert nach den sechs STRIDE-Kategorien.
- **2. Bedrohungskatalog nutzen:** Das Blatt «Bedrohungskatalog» enthält 125 vordefinierte, OT-spezifische Bedrohungen für 23 typische Maschinenbau-Assets. Nutzen Sie diesen Katalog als Ausgangspunkt und Inspiration. Wählen Sie die für Ihr Produkt relevanten Bedrohungen aus und übertragen Sie sie ins TARA-Sheet.
- **3. Ergänzen:** Prüfen Sie für jedes Asset, ob über den Katalog hinaus weitere produktspezifische Bedrohungen bestehen. Denken Sie insbesondere an kundenspezifische Schnittstellen, proprietäre Protokolle und Sonderanfertigungen.

Für die systematische Identifikation verwenden Sie die STRIDE-Methodik. STRIDE ist ein bewährtes Bedrohungsmodell, das sechs Kategorien von Bedrohungen definiert:

Kategorie	Bedrohungstyp	Schutzziel	Beispiel (Maschinenbau)
Spoofing	Identitätsmissbrauch	Authentizität	Angreifer nutzt Default-Passwort der CNC
Tampering	Datenmanipulation	Integrität	NC-Programm über Netzwerk verändert
Repudiation	Keine Nachvollziehbarkeit	Zurechenbarkeit	Parameter geändert, nicht nachvollziehbar
Info Disclosure	Informationsabfluss	Vertraulichkeit	Produktionsdaten über OPC UA abgezogen
Denial of Service	Verfügbarkeitsangriff	Verfügbarkeit	SPS durch Netzwerk-Flooding lahmgelegt
Elev. of Privilege	Rechtheausweitung	Autorisierung	Service-Zugang zu Admin-Rechten eskaliert

Aufbau des TARA-Sheets (linker Block — Asset & Bedrohung):

Spalte	Beschreibung
Asset-ID	Referenz zum Asset-Register (z.B. A01)
Threat-ID	Eindeutige Bedrohungskennung (z.B. A01_Sp_01 für Spoofing-Bedrohung 1 auf Asset A01)
Bedrohung	Kurzbeschreibung der Bedrohung
Schutzziel (C/I/A)	Welches Schutzziel ist betroffen?

Praxistipp

Arbeiten Sie asset-weise durch den Katalog. Gehen Sie für jedes Asset alle sechs STRIDE-Kategorien durch und fragen Sie sich: «Ist diese Art von Bedrohung für dieses Asset

relevant?» Wenn ja, übertragen Sie die Bedrohung. Wenn nein, dokumentieren Sie kurz, warum nicht (z.B. «keine Netzwerkschnittstelle vorhanden»).

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 6 — Risikobewertung (Ist-Zustand)

Ziel: Jede identifizierte Bedrohung quantitativ bewerten.

Werkzeug: TARA-Vorlage → Blatt «TARA» (Ist-Zustand, linke Seite) + Blatt «Scoring-Dimensionen»

Output: Vollständig bewertete Risiken im Ist-Zustand

Nachdem Sie in Schritt 5 die Bedrohungen identifiziert haben, bewerten Sie nun jede Bedrohung anhand von vier Dimensionen. Die Bewertung erfolgt für den Ist-Zustand — also die aktuelle Situation ohne zusätzliche Massnahmen. Das Blatt «Scoring-Dimensionen» in der TARA-Vorlage enthält detaillierte Beschreibungen und Praxisbeispiele für jede Stufe.

Die vier Bewertungsdimensionen:

1. Exposition — Wie erreichbar ist das Ziel?

Stufe	Wert	Beschreibung
Low (0.33)	0.33	Zugang zum Inneren des Schaltschranks erforderlich (Debug-Port, Speicherkarte hinter verschlossener Tür)
Medium (1.0)	1.00	Physische Anwesenheit an der Maschine, aber Zugriff von aussen möglich (USB, HMI-Panel, Service-Port)
High (1.67)	1.67	Netzwerkzugang reicht — kein physischer Zugang nötig (Web-HMI, OPC UA, Remote-Service, Cloud)

2. Exploitability — Wie komplex ist die Ausnutzung?

Stufe	Wert	Beschreibung
Low (0.33)	0.33	Erhebliche Expertise nötig: Zero-Day, Reverse Engineering, Spezialhardware
Medium (1.0)	1.00	Technisches Können und Standard-Tools: Custom-Scripts, Protokollanalyse, Social Engineering
High (1.67)	1.67	Trivial: Default-Credentials, öffentliche Exploits, USB-Stick mit Malware

3. Attractiveness — Wie motiviert ist der Angreifer?

Stufe	Wert	Beschreibung
Low (0.33)	0.33	Minimaler Wert: Nur nicht-sensible Betriebsdaten, kein Monetarisierungspfad

Stufe	Wert	Beschreibung
Medium (1.0)	1.00	Moderater Nutzen: Störpotenzial, begrenzter Datenzugang, Cryptomining
High (1.67)	1.67	Erheblicher Wert: Ransomware, Industriespionage, Sabotage, Pivot ins Werksnetz

4. Impact — Was ist die Worst-Case-Konsequenz?

Stufe	Wert	Beschreibung
Very low	1	Vernachlässigbar — System erholt sich automatisch
Low	2	Kurze Unterbrechung — Bediener quittiert Alarm, Service-Neustart
Medium	3	Maschinenrestart nötig, Support erforderlich, Ausschuss (erkennbar)
High	4	Stunden-/Tage-Ausfall, Datenverlust, unerkannte Prozessmanipulation
Critical	5	Physischer Schaden an Maschine/Person, Safety-Funktionen kompromittiert

Risikoberechnung:

Die drei Wahrscheinlichkeitsfaktoren (Exposition, Exploitability, Attractiveness) werden addiert und mit dem Impact-Wert multipliziert. Das Ergebnis ist ein Risikowert zwischen 1 und 25. Das TARA-Sheet berechnet diesen Wert automatisch.

$$\text{Risiko} = (\text{Exposition} + \text{Exploitability} + \text{Attractiveness}) \times \text{Impact}$$

Risikoklasse	Wertbereich	Bedeutung
Low	1–4	Akzeptabel — keine unmittelbare Massnahme erforderlich
Medium	5–9	Massnahmen empfohlen
High	10–15	Massnahmen erforderlich
Critical	16–25	Sofortige Massnahmen erforderlich

Override-Regeln:

- Impact = Critical → Gesamtrisiko mindestens High, unabhängig von anderen Dimensionen
- Impact = Critical UND Exposition = High → Gesamtrisiko = Critical
- Exploitability = High UND Impact ≥ High → eine Stufe hochsetzen

Praxistipp

Bewerten Sie den Ist-Zustand ehrlich — ohne Schönfärberei. Es geht darum, das tatsächliche Risikobild zu erfassen. Die Verbesserung kommt in den nächsten Schritten. Ein ehrliches Ist-Bild ist die Grundlage für gezielte, wirtschaftliche Massnahmen.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 7 — Risikobehandlung definieren

Ziel: Für jedes bewertete Risiko eine Behandlungsstrategie festlegen und bei Bedarf konkrete Massnahmen definieren.

Werkzeug: TARA-Vorlage → Blatt «TARA», Spalten «Strategy», «Begründung», «Massnahme» und «Beschreibung Umsetzung»

Output: Dokumentierte Risikobehandlungsstrategie und Massnahmen pro Risiko

Nach der Risikobewertung (Ist-Zustand) steht für jede Bedrohung ein Risikowert und eine Risikoklasse fest. Jetzt entscheiden Sie für jedes Risiko, wie Sie damit umgehen. Es stehen vier Strategien zur Verfügung:

Strategie	Beschreibung	Wann angemessen?	Erfordert
Mitigieren	Risiko durch technische oder organisatorische Massnahmen reduzieren	Risiko ist zu hoch, aber beherrschbar	Massnahme + Umsetzungsbeschreibung + Restrisikobewertung (Schritt 8)
Vermeiden	Bedrohungsquelle eliminieren (z.B. Schnittstelle entfernen)	Risiko ist nicht akzeptabel und Funktion ist verzichtbar	Massnahme + Umsetzungsbeschreibung + Restrisikobewertung (Schritt 8)
Transferieren	Risiko auf Dritte übertragen (z.B. Versicherung, Betreiberverantwortung)	Risiko kann nicht technisch gelöst werden	Begründung + Verweis auf Vertrag/Versicherung
Akzeptieren	Risiko bewusst in Kauf nehmen	Risiko ist niedrig oder Aufwand unverhältnismässig	Begründung (dokumentierte Entscheidung)

So nutzen Sie das TARA-Sheet für die Risikobehandlung:

- **Spalte «Strategy»:** Wählen Sie eine der vier Strategien (Akzeptieren, Transferieren, Mitigieren, Vermeiden).
- **Spalte «Begründung»:** Dokumentieren Sie, warum Sie diese Strategie gewählt haben. Bei «Akzeptieren» und «Transferieren» reicht diese Begründung als Dokumentation.
- **Spalte «Massnahme»:** Bei «Mitigieren» und «Vermeiden»: Beschreiben Sie die konkrete Massnahme.
- **Spalte «Beschreibung Umsetzung»:** Detaillieren Sie, wie die Massnahme technisch oder organisatorisch umgesetzt wird.

Hands-on Beispiel: Risikobehandlung am Beispiel eines IPC mit CNC-Steuerung

Ausgangslage: Für den Industrial PC (Asset A01) mit CNC-Steuerung wurden in Schritt 5 und 6 folgende Bedrohungen identifiziert und bewertet:

Threat-ID	Bedrohung	Risiko (Ist)	Klasse
A01_Sp_01	Default-Credentials auf Windows-Login	15	High
A01-Ta_01	NC-Programm über Netzwerk manipuliert	18	Critical
A01_Id_01	Produktionsdaten über OPC UA abgezogen	5	Medium
A01_Do_01	IPC durch Netzwerk-Flooding lahmgelegt	9	Medium

Risikobehandlungsentscheidungen:

A01_Sp_01 — Mitigieren: Risiko High (15). Default-Credentials sind ein bekanntes Problem und trivial ausnutzbar. Massnahme: Passwortwechsel bei Erstinbetriebnahme erzwingen (Setup-Wizard blockiert Betrieb bis individuelles Passwort gesetzt). Umsetzung: Anpassung der Windows-Gruppenrichtlinie, Integration in Inbetriebnahme-Checkliste.

A01-Ta_01 — Mitigieren: Risiko Critical (18). NC-Programm-Manipulation kann zu Ausschuss, Maschinenkollision oder Personengefährdung führen. Massnahme: Integritätsprüfung (Checksumme) für NC-Programme bei Übertragung. Zusätzlich: Netzwerksegmentierung, DNC-Zugriff nur über authentisierten Kanal. Umsetzung: Checksummen-Validierung in der Steuerungssoftware, VLAN-Konfiguration im Maschinenswitch.

A01_Id_01 — Akzeptieren: Risiko Medium (5). Produktionsdaten über OPC UA sind für die meisten Kunden nicht wettbewerbskritisch. OPC UA-Verschlüsselung ist verfügbar, wird aber vom Kunden konfiguriert. Begründung: Risiko ist moderat, Verschlüsselungsoption besteht, Konfiguration liegt in Betreiberverantwortung. Hinweis in Betriebsanleitung.

A01_Do_01 — Transferieren: Risiko Medium (9). DoS-Schutz auf Netzwerkebene liegt primär in der Verantwortung des Betreibers (Netzwerksegmentierung, Firewall). Begründung: OEM kann Netzwerkumgebung des Kunden nicht kontrollieren. Verweis auf Betriebsanleitung Abschnitt «Netzwerkempfehlungen» und Installationsvoraussetzungen.

Praxistipp

Nicht jedes Risiko muss mitigiert werden. Ein bewusst akzeptiertes Risiko mit dokumentierter Begründung ist besser als eine Massnahme, die nie umgesetzt wird. Der CRA verlangt Verhältnismässigkeit — aber auch Nachvollziehbarkeit.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 8 — Restrisiko bewerten

Ziel: Nach Definition der Massnahmen das verbleibende Risiko (Residualrisiko) bewerten und mit Test Cases validieren.

Werkzeug: TARA-Vorlage → Blatt «TARA» (Soll-Zustand, rechte Seite)

Output: Residualrisiko-Bewertung im TARA-Sheet mit Test Cases

Für jede Bedrohung, bei der Sie in Schritt 7 die Strategie «Mitigieren» oder «Vermeiden» gewählt haben, bewerten Sie nun erneut alle vier Dimensionen (Exposition, Exploitability, Attractiveness, Impact) — diesmal unter der Annahme, dass die definierten Massnahmen vollständig umgesetzt sind.

Spalten im TARA-Sheet (rechte Seite — Soll-Zustand):

Spalte	Beschreibung
Exposition (Soll)	Wie erreichbar ist das Ziel nach Umsetzung der Massnahme?
Exploitability (Soll)	Wie komplex ist die Ausnutzung nach Umsetzung?
Attractiveness (Soll)	Hat sich die Attraktivität für den Angreifer verändert?
Impact (Soll)	Hat die Massnahme den Worst-Case-Impact reduziert?
Residual Risk	Automatisch berechnet — Risikowert nach Massnahmen
Risikoklasse (Soll)	Automatisch — Low / Medium / High / Critical
Test Case	Beschreibung, wie die Massnahme geprüft werden kann
Datum	Wann wurde der Test durchgeführt?
Geprüft von	Name der prüfenden Person
Kommentar	Ergebnis des Tests, offene Punkte

Fortsetzung Beispiel: Restrisiko für A01_Sp_01 und A01_Ta_01

A01_Sp_01 — Default-Credentials (Mitigiert):

- Massnahme: Passwortwechsel bei Erstinbetriebnahme erzwungen
- Exposition (Soll): High → High (unverändert, da Netzwerkzugang bestehen bleibt)
- Exploitability (Soll): High → Medium (Default-Credentials eliminiert, aber Brute-Force noch möglich)
- Attractiveness (Soll): Medium → Medium (unverändert)
- Impact (Soll): High → High (unverändert)
- Residualrisiko: 13 (High) — akzeptabel, weitere Härtung über Account-Lockout empfohlen
- **Test Case:** Versuch, sich mit Default-Credentials (admin/admin, user/user) am IPC anzumelden. Erwartetes Ergebnis: Zugang wird verweigert. Zusätzlich: Prüfen, ob Setup-Wizard bei Erststart Passwortwechsel erzwingt.

A01_Ta_01 — NC-Programm-Manipulation (Mitigiert):

- Massnahme: Checksummen-Validierung + Netzwerksegmentierung



- Exposition (Soll): High → Medium (DNC nur noch über dediziertes VLAN erreichbar)
- Exploitability (Soll): Medium → Low (Checksumme muss umgangen werden)
- Attractiveness (Soll): High → High (unverändert — NC-Programme bleiben wertvoll)
- Impact (Soll): Critical → Critical (Manipulation führt weiterhin zu Kollision)
- Residualrisiko: 10 (High) — aufgrund Critical Impact mindestens High. Zusätzliche Massnahmen prüfen (z.B. digitale Signatur).
- **Test Case:** 1) NC-Programm mit absichtlich veränderter Checksumme übertragen — Steuerung muss Transfer ablehnen. 2) Netzwerksan aus dem Office-VLAN auf DNC-Port — Verbindung muss durch Firewall blockiert werden.

Falls das Residualrisiko bei einzelnen Bedrohungen noch als «High» oder «Critical» bewertet wird, haben Sie drei Optionen:

- Zusätzliche Massnahmen definieren und zurück zu Schritt 7 iterieren
- Das Restrisiko explizit akzeptieren und begründen
- Nicht akzeptable Restrisiken, die nur vom Betreiber adressiert werden können, in der Betriebsanleitung kommunizieren (CRA Anhang II + MV Anhang III, 1.7.4)

Praxistipp

Test Cases sind kein «Nice-to-have» — sie dokumentieren nachprüfbar, dass Ihre Massnahmen wirken. Planen Sie die Tests in die Entwicklung ein und führen Sie sie vor dem Inverkehrbringen durch. Ein Auditor wird nach genau diesen Nachweisen fragen.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 9 — Compliance-Mapping (CRA/MV)

Ziel: Pro Asset die Anwendbarkeit und Umsetzung jeder CRA- und MV-Anforderung dokumentieren.

Werkzeug: Asset Inventory (Excel) → Asset-Compliance-Blätter (Asset-01 bis Asset-15)

Output: Ausgefüllte Compliance-Blätter pro Asset mit CRA/MV-Nachweis

Dieser Schritt schliesst den Kreis zwischen der technischen Risikoanalyse (Schritte 5–8) und den regulatorischen Anforderungen. CRA Anhang VII Nr. 3 verlangt, dass die Risikobewertung die Anwendbarkeit jeder Anhang-I-Anforderung begründet. Wenn eine Anforderung nicht anwendbar ist, muss dies dokumentiert werden (CRA Recital 55).

Die Asset-Compliance-Blätter im Asset Inventory Tool sind mit dem Asset-Register verknüpft: Asset-01 entspricht dem ersten Asset (A01) im Register, Asset-02 dem zweiten (A02), usw.

Für jedes Asset und jede Anforderung füllen Sie folgende Felder aus:

Feld	Beschreibung	Beispiel
Anwendbar?	Ja / Nein / Teilweise (Dropdown)	Ja
Begründung	Insbesondere bei Nein/Teilweise: Warum nicht anwendbar?	Asset hat keine persistente Datenspeicherung



Feld	Beschreibung	Beispiel
Umsetzungsbeschreibung	Wie wird die Anforderung konkret erfüllt?	TLS 1.3 für alle OPC-UA-Verbindungen konfiguriert
Nachweis / Referenz	Verweis auf TARA-Threats, Testberichte, Dokumente	Siehe TARA A01_Sp_01, Test Case vom 15.03.2026
Status	Offen / In Arbeit / Umgesetzt	Umgesetzt
Verantwortlich	Wer ist zuständig?	M. Müller, Entwicklung

Die Compliance-Bewertung deckt insgesamt 23 Anforderungen ab:

CRA Anhang I — Teil I: 14 Produkthanforderungen

- (1) Secure by Design
- (2a) Ohne bekannte ausnutzbare Schwachstellen
- (2b) Sichere Standardkonfiguration, Rücksetzmöglichkeit
- (2c) Sicherheitsupdates bereitstellen
- (2d) Zugangssteuerung — Authentifizierung, Identitätsmanagement
- (2e) Vertraulichkeit — Verschlüsselung
- (2f) Datenintegrität — Schutz vor Manipulation
- (2g) Datenminimierung
- (2h) Verfügbarkeit wesentlicher Funktionen, DoS-Abwehr
- (2i) Minimierung negativer Auswirkungen auf andere Geräte/Netzwerke
- (2j) Angriffsfläche minimieren
- (2k) Auswirkungen von Sicherheitsvorfällen minimieren
- (2l) Logging und Monitoring sicherheitsrelevanter Aktivitäten
- (2m) Sichere Datenlöschung ermöglichen

CRA Anhang I — Teil II: 5 Schwachstellenmanagement-Anforderungen

- (II-1) Schwachstellen identifizieren, dokumentieren, beheben
- (II-2) SBOM erstellen und pflegen
- (II-3) Coordinated Vulnerability Disclosure (CVD) — VDP veröffentlichen
- (II-4) Sicherheitsupdates unverzüglich und kostenlos bereitstellen
- (II-5) Informationen über behobene Schwachstellen veröffentlichen

Maschinenverordnung — Anhang III: 4 Anforderungen

- 1.1.2 — Sicherheitsintegration
- 1.1.9 — Schutz gegen Korrumpierung
- 1.2.1 — Sicherheit und Zuverlässigkeit von Steuerungssystemen
- 1.7.4 — Betriebsanleitung — Cybersecurity-Hinweise für den Nutzer

Das Dashboard im Asset Inventory Tool zeigt automatisch den aggregierten Erfüllungsgrad pro Asset und über alle Assets hinweg. Dies gibt Ihnen jederzeit einen Überblick, wo Sie stehen und wo Handlungsbedarf besteht.

Praxistipp

Arbeiten Sie sich Asset für Asset durch die Anforderungsliste. Nutzen Sie die Referenzspalte konsequent, um auf TARA-Threats und Test Cases zu verweisen — so entsteht eine durchgängige Nachweiskette vom Risiko zur Massnahme zur Compliance-Erfüllung.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.

Schritt 10 — Dokumentation zusammenführen

Ziel: Alle Ergebnisse der Schritte 1–9 in einer zentralen, konsistenten technischen Dokumentation zusammenführen.

Werkzeug: Alle bisherigen Werkzeuge — TARA-Vorlage, Asset Inventory, externe Diagramme

Output: Vollständige technische Dokumentation (Cybersecurity-Teil)

Am Ende des Prozesses verfügen Sie über alle Bausteine, die zusammen den Cybersecurity-Teil der technischen Dokumentation nach CRA Anhang VII bilden. In diesem Schritt führen Sie alles zusammen und prüfen die Konsistenz.

Ihre Dokumentationsbausteine:

#	Dokument	CRA-Referenz	MV-Referenz	Quelle
1	Produktprofil mit Security Context	Art. 13 Abs. 2; Anh. VII Nr. 1	Anh. IV Nr. 1	TARA-Vorlage
2	Architekturdiagramm mit Security Zones	Anh. VII Nr. 2a	Anh. IV Nr. 1	Extern (draw.io etc.)
3	Vollständige TARA (Ist + Soll + Massnahmen)	Anh. VII Nr. 3	Anh. IV Nr. 2	TARA-Vorlage
4	Compliance-Matrix pro Asset	Anh. VII Nr. 3	—	Asset Inventory
5	Asset-Register mit SBOM-Referenzen	Anh. VII Nr. 2	—	Asset Inventory
6	Lifecycle-Prozessdokumentation	Art. 13; Art. 14	—	Organisatorisch

Konsistenzprüfung — Checkliste:

- Stimmen die Asset-IDs im Asset-Register, im TARA-Sheet und in den Compliance-Blättern überein?
- Ist jedes Asset aus dem Register auch im TARA-Sheet mit mindestens einer Bedrohung erfasst?
- Verweisen die Compliance-Blätter korrekt auf TARA-Threats und Test Cases?
- Sind alle Risiken mit Klasse «High» oder «Critical» behandelt (Massnahme, Akzeptanz oder Transfer)?



- Sind Restrisiken, die in der Betriebsanleitung kommuniziert werden müssen, identifiziert?
- Sind die Dashboards in beiden Tools aktuell und konsistent?

Zusätzlich empfehlen wir, folgende Lifecycle-Prozesse zu etablieren und zu dokumentieren:

- **Schwachstellenmanagement:** SBOM pflegen, CVE-Feeds überwachen, Triage-Prozess definieren
- **Meldeprozess:** Wer meldet innerhalb 24h an ENISA/CSIRT? Interner Eskalationsweg definiert?
- **Vulnerability Disclosure Policy (VDP):** Veröffentlicht? security@-Adresse eingerichtet?
- **Security Updates:** Prozess für Erstellung, Test, Freigabe und Auslieferung von Patches
- **Periodische Neubewertung:** TARA mindestens jährlich aktualisieren (CRA Art. 13 Abs. 7)

Wichtig: Fristen beachten

Der Meldeprozess und die VDP müssen bis September 2026 stehen — die CRA-Meldepflicht (Art. 14) gilt für ALLE Produkte am Markt, unabhängig vom Alter. Die vollständigen CRA-Anforderungen gelten ab Dezember 2027.

✓ **Review-Checkpoint:** Lassen Sie die Ergebnisse dieses Schritts von einer internen oder externen Person prüfen, bevor Sie zum nächsten Schritt übergehen.



Zusammenfassung

Dieser Prozessleitfaden führt Sie in zehn Schritten von der Scope-Definition bis zur vollständigen, auditfähigen technischen Dokumentation. Die Methodik kombiniert den bewährten IEC-62443-3-2-Ansatz mit den spezifischen Anforderungen des Cyber Resilience Act und der Maschinenverordnung.

Die wichtigsten Erfolgsfaktoren:

- Beginnen Sie mit dem Security Context und dem Zonenplan — ohne diese Grundlagen ist alles Weitere Stochern im Nebel.
- Trennen Sie Bedrohungsidentifikation (Schritt 5) sauber von der Bewertung (Schritt 6) — erst sammeln, dann bewerten.
- Dokumentieren Sie jede Entscheidung nachvollziehbar — auch und gerade die Entscheidung, ein Risiko zu akzeptieren.
- Nutzen Sie die Review-Checkpoints konsequent — ein zweites Augenpaar findet, was Ihnen entgeht.
- Planen Sie Test Cases früh ein — sie dokumentieren die Wirksamkeit Ihrer Massnahmen.
- Schliessen Sie den Kreis: Von der Bedrohung zur Massnahme zur Compliance-Erfüllung — die Nachweiskette muss lückenlos sein.

Alpina Connect GmbH — www.alpinaconnect.com

Für Fragen, Workshop-Anfragen oder Unterstützung bei der Durchführung: info@alpinaconnect.com

Haftungsausschluss

Dieses Dokument wurde von Alpina Connect GmbH nach bestem Wissen und Gewissen erstellt. Es dient ausschliesslich der allgemeinen Information und der strukturierten Herangehensweise für Cybersecurity-Risikoanalysen. Die Inhalte können Fehler oder Unvollständigkeiten enthalten.

Dieses Dokument stellt keine Rechtsberatung dar. Massgeblich sind ausschliesslich die amtlich veröffentlichten Verordnungstexte. Alpina Connect GmbH übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der Inhalte. Für konkrete rechtliche Fragestellungen empfehlen wir die Konsultation einer spezialisierten Rechtsberatung.

© 2026 Alpina Connect GmbH. Alle Rechte vorbehalten. — Stand: März 2026