CADIS - Cybersecurity Assessment for Defence Industry Suppliers

Whitepaper CADIS

Die Verteidigungs- und Rüstungsindustrie ist heute stärker denn je auf belastbare, sichere und widerstandsfähige Lieferketten angewiesen. Geopolitische Spannungen, neue regulatorische Anforderungen wie NIS2, BSIG und der Cyber Resilience Act sowie eine zunehmend digitalisierte Wertschöpfung stellen Hersteller und Zulieferer vor eine gemeinsame Aufgabe: Cybersicherheit nachweisbar zu machen – über alle Stufen der Lieferkette hinweg.

Hintergrund

Bestehende Standards wie ISO/IEC 27001 oder TISAX adressieren wichtige Teilaspekte, decken aber die spezifischen Anforderungen der Verteidigungs- und Rüstungsindustrie nicht ganzheitlich ab. CADIS geht gezielt darüber hinaus: ein eigenständiges Modul für Operational Technology für die Absicherung von Produktions- und Steuerungssystemen nach IEC 62443; abgestufte Sonderanforderungen für Lieferanten mit erhöhter Kritikalität; geopolitische Risiken und geografische Lage als verbindliche Eingangskriterien der Lieferantenbewertung; ein Modul speziell zum verantwortungsvollen Einsatz von Künstlicher Intelligenz auf Basis der ISO/IEC 42001; und ein eigenes Modul für Transport und Umschlag sicherheitsrelevanter Güter. So entsteht ein Prüfrahmen, der die Realität sicherheitsrelevanter Lieferketten abbildet – statt sie auf einen branchenneutralen Standard zu zwingen.

Als erstes europäisches Prüfverfahren speziell für Zulieferer der Verteidigungs- und Rüstungsindustrie schafft CADIS eine einheitliche, transparente und messbare Grundlage für Cybersicherheit in der Lieferkette und schließt diese Lücke. Entwickelt und exklusiv durchgeführt von DEKRA, bündelt das Verfahren 14 modulare Prüfbausteine – von physischer Sicherheit über IT- und OT-Security bis hin zu Datenschutz, Compliance und KI-Governance – und verbindet sie mit den Anforderungen aus ISO/IEC 27001:2022, IEC 62443, NIST CSF v2.0, BSI IT-Grundschutz, NIS2, BSIG, DSGVO und Cyber Resilience Act.

Ihre Vorteile

- **Marktzugang:** Sie werden als zuverlässiger Partner in der Verteidigungs- und Rüstungsindustrie wahrgenommen und qualifizieren sich für sicherheitsrelevante Aufträge.
- **Wettbewerbsvorteil:** Nachweisbare Cybersicherheit schafft Vertrauen bei Systemherstellern, Behörden und Versicherern – und stärkt Ihre Marktposition gegenüber Wettbewerbern.
- **Effizienz:** Ein Audit, viele Anspruchsteller. Über den standardisierten CADIS-Result-Exchange teilen Sie Ihr Prüfergebnis kontrolliert mit anfragenden Auftraggebern – und vermeiden Mehrfachprüfungen.
- **Regulatorische Sicherheit:** NIS2, BSIG und Cyber Resilience Act systematisch abgedeckt – mit klarer Verbindung zu ISO/IEC 27001, IEC 62443 und NIST CSF.
- **Verhältnismäßige Prüftiefe:** Drei Level of Examination (LoE 1–3) und Sonderanforderungen in drei Stufen passen die Prüfung an Ihr Risikoprofil an – nicht umgekehrt.
- **Messbares Ergebnis:** Der Security Score (0,00–3,00) entsteht aus der gewichteten Summe aller Prüfmodule und macht Cybersicherheitsreife vergleichbar – innerhalb Ihres Unternehmens, im Zeitverlauf und gegenüber Auftraggebern. Klare Schwellen (≥2,75 konform, 1,01–2,74 nicht kritisch abweichend, ≤1,00 kritisch abweichend) ordnen das Ergebnis einer der drei Ergebnisstufen zu.

Wer ist betroffen?

Wenn Sie als Zulieferer oder Dienstleister Konstruktionsdaten, Komponenten oder Services in die Verteidigungs- und Rüstungsindustrie liefern, sind Sie zunehmend gefordert, Ihre Cybersicherheit nachweisbar zu machen – gegenüber OEMs, Behörden und Versicherern. CADIS richtet sich an Unternehmen entlang der gesamten Lieferkette, unabhängig von Größe und Tätigkeitsfeld:

- Direkte Lieferanten von Systemherstellern
- Sub-Lieferanten in mehrstufigen Wertschöpfungsketten
- Cloud- und Managed-Service-Anbieter mit Zugang zu Engineering-Daten
- Dienstleister mit Bezug zu Konstruktions- und Prototypendaten
- Logistikpartner, die eingestufte oder sicherheitsrelevante Güter umschlagen
- Betreiber kritischer OT-Umgebungen in Produktion und Fertigung

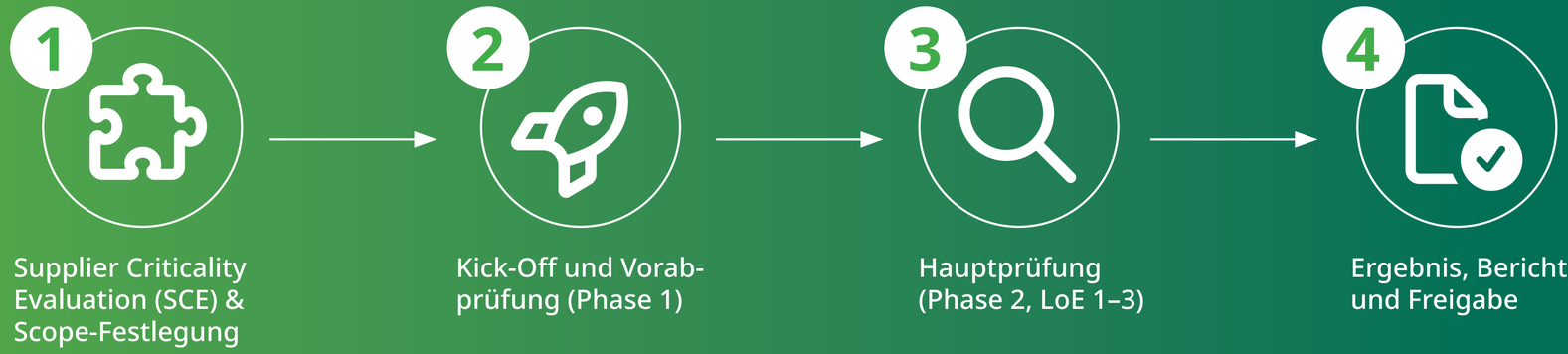
CADIS ist mehr als eine Checkliste

Bewertet wird nicht nur, ob eine Maßnahme existiert, sondern wie reif, wirksam und nachvollziehbar sie umgesetzt ist. Auf einer Bewertungsskala von 0 bis 3 prüfen DEKRA-Auditoren, ob Maßnahmen dokumentiert, eingeführt, gelebt und kontinuierlich verbessert werden.

Der Angemessenheitsgrundsatz berücksichtigt Größe, Branche und Risikoprofil – das Bewertungsniveau bleibt dennoch einheitlich und vergleichbar.

Das CADIS-Modell: 14 modulare Prüfbausteine

1. Physische Sicherheit am Standort
2. Organisation der Informationssicherheit
3. Einsatz cloudbasierter und externer Serviceleistungen
4. Sicherheit in der Softwareentwicklung
5. Informationssicherheit in Projektmanagement, Personalwesen und Einkauf
6. Incident- und Krisenmanagement
7. Kontinuitätsmanagement (BCM)
8. Identitäts- und Zugriffsmanagement (IAM)
9. IT-Security
10. Operational Technology (OT)
11. Compliance Management
12. Datenschutz
13. Einsatz künstlicher Intelligenz
14. Transport und Umschlag



Teilnahme in 4 Schritten

Schritt 1: Umfang der Prüfung (SCE & Scope-Festlegung)
Der Prüfumfang wird vom Auftraggeber individuell auf Basis der Supplier Criticality Evaluation (SCE) festgelegt. In die SCE fließen Sicherheitsrelevanz, technologische Abhängigkeiten, regulatorische Anforderungen sowie das geopolitische Risikoprofil des Lieferanten ein.

Aus der SCE leiten sich das anzuwendende Level of Examination (LoE 1–3) sowie die Sonderanforderungen (Stufen 1–3) ab. Der Prüfscope umfasst Standorte, Prüfmodule und die jeweilige Prüftiefe.

Schritt 2: Kick-Off und Vorabprüfung (Phase 1)
Nach einem Kick-Off-Termin, in dem Ablauf, Scope und Ansprechpartner abgestimmt werden, reicht das Unternehmen in Phase 1 den ausgefüllten CADIS-Prüfkatalog ein. Geprüft wird, ob für alle Prüffragen ein Reifegrad (0–3) gesetzt, eine Umsetzungsbeschreibung hinterlegt und mindestens ein Nachweis referenziert wurde. Dem Unternehmen stehen bis zu drei Einreichungsversuche zur Verfügung.

Schritt 3: Hauptprüfung (Phase 2, LoE 1–3)
Ist die Vorabprüfung erfolgreich abgeschlossen, beginnt die Hauptprüfung. DEKRA-Auditoren bewerten die Prüfmodule vor Ort und remote auf dem in der SCE festgelegten Level of Examination (LoE 1–3). Grundlage sind Dokumentenprüfung, Interviews mit Verantwortlichen und stichprobenartige Wirksamkeitsprüfungen – ergänzt um die folgenden, exemplarisch ausgewählten Prüfthemen:

Ausgewählte Prüfthemen
Auf organisatorischer Ebene wird geprüft, ob Informationssicherheit verankert und gelebt wird – von Awareness und Zugriffskontrolle bis zu strukturierten Change- und Patch-Prozessen.

Auf technischer Ebene werden die Wirksamkeit von Schutzmaßnahmen, Backup- und Wiederanlaufkonzepten sowie das Incident- und Krisenmanagement bewertet.

Für industrielle Umgebungen kommen Prüfungen zur sicheren Trennung von IT und OT sowie zur IEC-62443-konformen Absicherung der Steuerungssysteme hinzu.

Reifegrade: Die Bewertungssystematik von CADIS
Reifegrad statt Häkchen: CADIS bewertet nicht, ob eine Maßnahme existiert, sondern wie vollständig, wirksam und nachvollziehbar sie umgesetzt ist. Auf einer Skala von 0 bis 3 prüft der Auditor jeden Prüfpunkt auf Basis nachvollziehbarer Evidenzen und unter Berücksichtigung des Angemessenheitsgrundsatzes (Größe, Branche, Risikoprofil der Organisation). Das Ergebnis ist ein realistisches Bild der tatsächlichen Sicherheitsreife – nicht nur eine Compliance-Bestätigung.

Schritt 4: Ergebnis, Bericht und Freigabe
Im letzten Schritt werden die Prüfungsergebnisse in einem Bericht zusammengeführt, dem Unternehmen übergeben und nach Freigabe über den CADIS-Result-Exchange für berechtigte Auftraggeber zugänglich gemacht. Der Bericht weist Reifegrade je Prüfmodul, den aggregierten Security Score sowie eine der drei folgenden Ergebnisstufen aus:

- Konform (Score 2,75–3,00, keine Abweichungen): Freigabe für bis zu zwei Jahre; im Folgejahr risikobasierte Überwachungsprüfung.
- Nicht kritisch abweichend (Score 1,01–2,74 oder mindestens eine nicht kritische Abweichung): temporäre Freigabe unter Auflagen, sofern ein Maßnahmenplan vorliegt; Heraufstufung auf konform nach vollständiger Abstellung der Abweichungen möglich.
- Kritisch abweichend (Score 0,00–1,00 oder mindestens eine kritische Abweichung): keine Freigabe; Abstellung innerhalb von drei Monaten erforderlich, anschließend Follow-Up-Prüfung.

Ihr Partner für CADIS

CADIS ist ein DEKRA-eigenes Produkt – von DEKRA entwickelt und ausschließlich durch DEKRA durchgeführt. Damit liegen Methodik, Auditorenqualifikation und Result-Exchange in einer Hand: bei einem der führenden Prüf-, Inspektions- und Zertifizierungshäuser mit jahrzehntelanger Erfahrung in der unabhängigen Begutachtung sicherheitskritischer Systeme.

Als Träger des CADIS-Programms verantwortet DEKRA die Methodik, qualifiziert die Auditoren und betreibt die zentrale CADIS-Result-Exchange-Datenbank. Alle Prüfenden verfügen über einschlägige Qualifikationen, darunter CISA, CISM und ISO/IEC 27001 Lead Auditor sowie modulspezifische Nachweise für OT (IEC 62443), Datenschutz und KI (ISO/IEC 42001).

Warum DEKRA?

- **Exklusiv:** CADIS wurde von DEKRA in Zusammenarbeit mit der Verteidigungs- und Rüstungsindustrie entwickelt und wird ausschließlich von DEKRA durchgeführt.
- **Unabhängig:** Großes Netzwerk qualifizierter Auditoren, organisatorisch getrennt von Beratungsleistungen.
- **Branchenexpertise**: jahrzehntelange Erfahrung in Cybersicherheit, industriellen Prüfungen und sicherheitskritischen Systemen.
- **Ganzheitlich:** Informationssicherheit, Datenschutz, OT, KI und physische Sicherheit aus einer Hand.
- **Effizient:** ein Audit, viele Anspruchsteller – über den standardisierten CADIS-Result-Exchange.
- **Planbar:** zweijähriger Prüfzyklus mit klaren Übergangsregelungen und definierten Maßnahmenfristen.

Ihr nächster Schritt

Vereinbaren Sie ein unverbindliches Erstgespräch mit unseren Expertinnen und Experten. Gemeinsam klären wir Ihren individuellen Prüfumfang, das passende Level of Examination und den Zeitplan für Ihre erste Prüfung.

Kontaktieren Sie uns! **Mehr erfahren!**

Wünschen Sie weitere Informationen?
Besuchen Sie unsere Website:

dekra-certification.de