VANTARION

TISAX für Automotive-Zulieferer

Strukturiert und effizient zur Auditfähigkeit

Ein Praxisleitfaden für
Geschäftsführung, QM, ISB & IT-Leitung

MANAGEMENT SUMMARY

Für viele Automotive-Zulieferer ist TISAX heute keine Option, sondern Voraussetzung für Geschäftsbeziehungen mit OEMs und Tier-n-Unternehmen. Die Anforderung kommt meist direkt aus Kundenverträgen oder Lieferantenportalen, verbunden mit klaren Fristen und definierten Prüfanforderungen.

Die zentrale Herausforderung lautet daher nicht:

„Ob wir TISAX machen“,
sondern:
„Wie setzen wir TISAX strukturiert, wirtschaftlich und auditfähig um?“

Dieses Whitepaper zeigt, wie Unternehmen TISAX systematisch angehen, mit klarer Scope-Definition, realistischer Einordnung der Schutzbedarfe und sauberer Nachweisführung.

Der Fokus liegt auf:

1. **Praktischer Einordnung der VDA-ISA-Logik**
2. **Realistischer Bewertung der Prüfziele (Vertraulichkeit, Verfügbarkeit, Datenschutz, Prototypenschutz)**
3. **Klarer Auditstruktur**

Wenn Struktur, Schutzbedarf und Verantwortlichkeiten sauber definiert sind, wird TISAX planbar.

Tobias Frank,
Gründer und CEO

Als **Head of IT und Verantwortlicher für Informationssicherheit** in Handelsunternehmen und Fertigungsindustrie und habe ich in allen Facetten erlebt, wie aufwändig Informationssicherheit für CxO und Teams im Alltag ist. 20 Jahre lang.

Aus diesem persönlichen Antrieb heraus entwickelten wir VantarIS und gründeten Vantarion.

VantarIS nimmt die Bürokratie aus Normen wie NIS2 und bringt kompetente Sicherheit.

VANTARIS

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

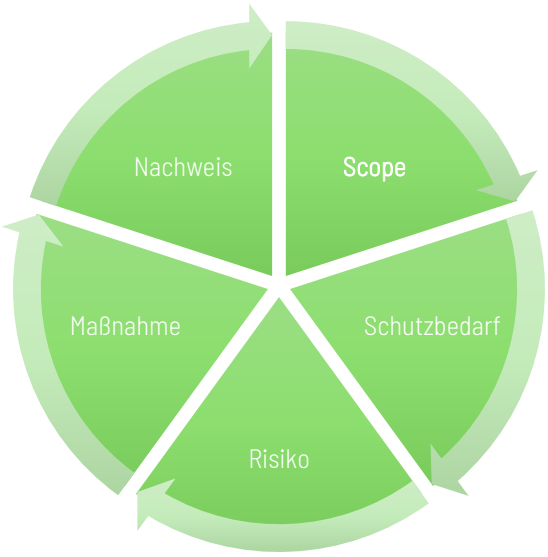
WAS TISAX PRAKTISCH FORDERT

TISAX ist kein eigenständiger Sicherheitsstandard, sondern ein branchenspezifischer Prüf- und Austauschmechanismus auf Basis des VDA ISA-Katalogs (Verband der Automobilindustrie Information Security Assessment). Inhaltlich baut TISAX stark auf ISO 27001 auf, erweitert diese jedoch um Automotive spezifische Anforderungen.

Im Kern bewertet TISAX:

- ☑ **Informationssicherheit**
- ☑ **Vertraulichkeit von OEM-Daten**
- ☑ **Verfügbarkeit kritischer Prozesse**
- ☑ **Datenschutz gemäß DSGVO (Art. 28 / Art. 9 bei besonderen Daten)**
- ☑ **Prototypenschutz (sofern relevant)**

TISAX prüft dabei nicht isolierte Maßnahmen, sondern die Systematik dahinter:



Entscheidend ist die nachvollziehbare Herleitung von Schutzmaßnahmen, insbesondere im Umgang mit sensiblen Entwicklungs- und Produktionsdaten.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

DIE VDA ISA-LOGIK UND PRÜFZIELSTRUKTUR

Der VDA ISA-Katalog bildet die inhaltliche Grundlage für TISAX-Prüfungen. Er strukturiert die Anforderungen nicht nach „Technikthemen", sondern nach klar definierten Prüfzielbereichen und Assessment-Leveln.

Zentral ist die Unterscheidung zwischen:

- ☑ **Informationssicherheit**
- ☑ **Datenschutz**
- ☑ **Prototypenschutz**

Jeder dieser Bereiche folgt einer eigenen Logik – sowohl inhaltlich als auch in der Prüfungstiefe.

Informationssicherheit – Schutzbedarfsstufen

Im Bereich Informationssicherheit erfolgt eine Differenzierung nach:

- ☑ **hoher Schutzbedarf**
- ☑ **sehr hoher Schutzbedarf**

Diese Schutzbedarfsstufen beziehen sich insbesondere auf die Schutzziele:

- ☑ **Vertraulichkeit**
- ☑ **Verfügbarkeit**

Je höher der Schutzbedarf, desto höher sind die Anforderungen an:

- ☑ **Zugriffsbeschränkungen**
- ☑ **Protokollierung**
- ☑ **Netzwerksegmentierung**
- ☑ **physische Sicherheitsmaßnahmen**
- ☑ **organisatorische Disziplin**
- ☑ **Nachweisführung im Audit**

Die Schutzbedarfsfeststellung ist damit kein formaler Schritt, sondern das zentrale Steuerungsinstrument. Sie definiert die Intensität der erforderlichen Maßnahmen.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

Unternehmen müssen nachvollziehbar darstellen:

- ☑ **Welche Informationen verarbeitet werden**
- ☑ **Welcher Schutzbedarf gilt**
- ☑ **Wie die Maßnahmen angemessen umgesetzt wurden**

Datenschutz – eigenständiger Prüfbereich

Datenschutz wird im VDA ISA als eigenständiger Prüfbereich betrachtet.

Hier erfolgt keine Einteilung in „hoher" oder „sehr hoher Schutzbedarf" im Sinne der Informationssicherheit. Stattdessen richten sich die Anforderungen nach:

- ☑ **Auftragsverarbeitung gemäß Art. 28 DSGVO**
- ☑ **Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO**

Geprüft werden insbesondere:

- ☑ **Auftragsverarbeitungsverträge**
- ☑ **Technische und organisatorische Maßnahmen (TOMs)**
- ☑ **Verzeichnis von Verarbeitungstätigkeiten**
- ☑ **Zugriffsbeschränkungen**
- ☑ **Schulungs- und Awareness-Nachweise**

Datenschutz ist somit kein Annex zur Informationssicherheit, sondern ein eigenständiger Prüfbereich mit klarer Dokumentationslogik.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

Prototypenschutz – Schutz klassifizierter Fahrzeuge und Komponenten

Der Prototypenschutz betrifft den Umgang mit durch den Kunden als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Entwicklungsinformationen. Die Anforderungen ergeben sich aus den vertraglich definierten Schutzvorgaben.

Geprüft werden insbesondere:

- ☑ **Physische Zutrittskontrollen**
- ☑ **Trennung sensibler Bereiche**
- ☑ **Besucher- und Fremdfirmenmanagement**
- ☑ **Regelungen zu mobilen Geräten und Kameras**
- ☑ **Dokumentierte Vertraulichkeitsvereinbarungen**
- ☑ **Schutz während Transport, Lagerung oder Testbetrieb**

Im Unterschied zur Informationssicherheit wird hier nicht zwischen „hohem" oder „sehr hohem" Schutzbedarf unterschieden. Maßgeblich ist die Klassifizierung durch den Auftraggeber und die daraus resultierende organisatorische und physische Absicherung.

Assessment-Level – Prüfungstiefe statt Schutzbedarfsstufe

Neben den Prüfzielbereichen definiert TISAX die Prüfungstiefe über Assessment-Level.

Die Assessment-Level bestimmen:

- ☑ **ob eine Plausibilitätsprüfung ausreicht**
- ☑ **ob Interviews durchgeführt werden**
- ☑ **ob ein Vor-Ort-Audit stattfindet**
- ☑ **wie intensiv Nachweise geprüft werden**

Die Prüfungstiefe ist somit eine Frage der Auditintensität – nicht der Schutzbedarfsdefinition.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

PRAKTISCHE KONSEQUENZ FÜR ZULIEFERER

Für Unternehmen in der Lieferkette bedeutet die ISA-Logik:

1. **Scope klar definieren**
2. **Relevante Prüfziele bestimmen**
3. **Schutzbedarf im Bereich Informationssicherheit dokumentieren**
4. **Datenschutzpflichten sauber abgrenzen (sofern relevant)**
5. **Prototypenschutz strukturiert absichern (sofern relevant)**

Erst wenn diese Bereiche sauber getrennt und dokumentiert sind, entsteht eine konsistente TISAX-Struktur.

TISAX verlangt keine pauschale Maximalsicherheit. Es verlangt eine nachvollziehbare, systematische Ableitung der Maßnahmen aus den tatsächlichen Anforderungen innerhalb der Lieferkette.

WELCHE NACHWEISE AUDITOREN TATSÄCHLICH PRÜFEN

TISAX-Audits sind keine rein dokumentengetriebenen Prüfungen. Auditoren bewerten die Konsistenz zwischen:

- ☑ **Scope**
- ☑ **Schutzbedarfsfeststellung**
- ☑ **Risikologik**
- ☑ **Maßnahmenumsetzung**
- ☑ **tatsächlicher organisatorischer Praxis**

In der Praxis konzentrieren sich Auditoren insbesondere auf folgende Kernnachweise:

1. Scope & Prüfzieldefinition

- ☑ **Dokumentierter Geltungsbereich**
- ☑ **Abgrenzung von Standorten und Prozessen**
- ☑ **Klar definierte Prüfziele (Informationssicherheit, Datenschutz, ggf. Prototypenschutz)**

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

2. Schutzbedarfsfeststellung (Informationssicherheit)

- ☑ Dokumentierte Einordnung in „hoher" oder „sehr hoher" Schutzbedarf
- ☑ Begründung der Einstufung
- ☑ Konsistente Ableitung von Maßnahmen

3. Risikomanagement

- ☑ Strukturierte Risikoübersicht
- ☑ Priorisierung
- ☑ Dokumentierte Maßnahmenplanung
- ☑ Nachweis der Umsetzung

4. Zugriffskontrolle

- ☑ Rollen- und Berechtigungskonzept
- ☑ Dokumentierte Vergabeprozesse
- ☑ Regelmäßige Überprüfung

5. Incident-Management

- ☑ Dokumentierter Prozess
- ☑ Eskalationswege
- ☑ Nachweise zu Vorfällen oder Tests

6. Lieferantensteuerung

- ☑ Bewertungslogik
- ☑ Vertragliche Sicherheitsanforderungen
- ☑ Dokumentierte Überprüfung

7. Datenschutz (sofern im Scope)

- ☑ AV-Verträge
- ☑ TOM-Dokumentation
- ☑ Awareness-Nachweise

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

8. Prototypenschutz (sofern relevant)

- ☑ Physische Sicherheitsmaßnahmen
- ☑ Besucherregelungen
- ☑ Dokumentierte organisatorische Maßnahmen

Auditfähigkeit bedeutet:
Dokumentation, Umsetzung und Nachweis bilden eine geschlossene Logik.

STRUKTURIERTER PROJEKTSTART

Ein professioneller Einstieg in TISAX folgt einer klaren Reihenfolge:

1. Scope festlegen

- ☑ Welche Standorte sind relevant?
- ☑ Welche Prozesse betreffen Kundendaten?
- ☑ Welche Prüfziele gelten?

2. Schutzbedarfe einordnen

- ☑ Informationssicherheit: hoher oder sehr hoher Schutzbedarf?
- ☑ Datenschutz erforderlich?
- ☑ Prototypenschutz Bestandteil des Scopes?

3. Projektstruktur definieren

- ☑ Geschäftsführung
- ☑ Informationssicherheitsbeauftragter
- ☑ QM / Compliance
- ☑ IT-Leitung

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

4. Maßnahmensteuerung etablieren

- ☑ Zentrale Maßnahmenliste
- ☑ Priorisierung
- ☑ Verantwortlichkeiten
- ☑ Fristen

5. Auditvorbereitung strukturieren

- ☑ Nachweisablage
- ☑ Dokumentationsstruktur
- ☑ interne Vorprüfung

Ein klar strukturierter Projektstart reduziert spätere Korrekturschleifen erheblich.

KONKRETE UMSETZUNGSBAUSTEINE

Eine erfolgreiche TISAX-Vorbereitung entsteht nicht durch abstrakte Konzepte, sondern durch klar definierte Arbeitsergebnisse. Entscheidend ist, dass Anforderungen in strukturierte, prüfbare und steuerbare Elemente übersetzt werden.

Unternehmen benötigen keine überdimensionierte Dokumentationslandschaft, sondern klar priorisierte Nachweise, eindeutige Verantwortlichkeiten und eine saubere Maßnahmensteuerung. Genau hier setzen die folgenden Umsetzungsbausteine an: Sie schaffen Transparenz über den aktuellen Reifegrad und ermöglichen eine systematische Vorbereitung auf das Audit

TISAX-Readiness-Checkliste

- ☑ Scope-Dokument
- ☑ Prüfzieldefinition
- ☑ Schutzbedarfsfeststellung
- ☑ Risikoübersicht
- ☑ Maßnahmenliste
- ☑ Berechtigungskonzept
- ☑ Incident-Prozess
- ☑ Lieferantenbewertung

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

- ☑ **Datenschutzdokumentation**
- ☑ **Management-Review**
- ☑ **Nachweise zu physischer Sicherheit (bei Prototypenschutz)**

Die Checkliste ermöglicht eine strukturierte Selbstbewertung vor dem offiziellen Audit.

FAZIT

TISAX ist kein Sonderprojekt, sondern ein strukturierter Nachweis von Informationssicherheit innerhalb der Lieferkette. Für viele Zulieferer ist das Label heute Voraussetzung für Geschäftsbeziehungen und damit nicht Kür, sondern Pflicht.

Erfolgreiche TISAX-Umsetzungen beginnen mit Klarheit:

- ☑ **ein sauber definierter Scope,**
- ☑ **korrekt eingeordnete Prüfziele,**
- ☑ **nachvollziehbar dokumentierte Schutzanforderungen**
- ☑ **klar geregelte Verantwortlichkeiten**

Erst wenn diese Struktur steht, lassen sich Maßnahmen effizient priorisieren und auditfähig nachweisen.

TISAX verlangt keine pauschale Maximalsicherheit, sondern eine konsistente Systematik. Schutzbedarf, Risiko, Maßnahme und Nachweis müssen logisch zusammenpassen. Ist diese Logik hergestellt, wird das Audit zur formalen Bestätigung eines funktionierenden Systems – nicht zum Risiko.

Der entscheidende nächste Schritt ist daher eindeutig:
Scope festlegen. Schutzanforderungen einordnen. Struktur aufbauen.

Mit einer klaren Projektlogik wird TISAX planbar – organisatorisch beherrschbar und strategisch nutzbar.