TISAX – Informationssicherheitsstandard in der Automobilindustrie

Die Automobilindustrie ist stark vernetzt und arbeitet mit zahlreichen Zulieferern und Partnern zusammen. Um den Schutz sensibler Daten – wie Fahrzeugsoftware, Konstruktionspläne oder personenbezogene Informationen – zu gewährleisten, wurde der Sicherheitsstandard **TISAX (Trusted Information Security Assessment Exchange)** entwickelt.
TISAX ist ein branchenspezifischer Standard, der vom VDA-QMC (Qualitätsmanagement-Center des Verbands der Automobilindustrie) eingeführt wurde. Er stellt sicher, dass Unternehmen der Zuliefererbranche einheitliche Sicherheitsanforderungen erfüllen und so das Vertrauen in die Lieferkette gestärkt wird.

Die Umsetzung von TISAX erfolgt in mehreren Schritten: Zunächst werden die relevanten Systeme identifiziert und bestehende Sicherheitsmaßnahmen analysiert. Anschließend werden notwendige Verbesserungen priorisiert und umgesetzt. Ein kontinuierlicher Prüf- und Verbesserungsprozess sorgt dafür, dass die Sicherheitsstandards dauerhaft eingehalten werden.

Hauptfunktionen von TISAX

- **Informationssicherheitsmanagementsystem (ISMS)**: Etablierung von Prozessen, Richtlinien und Verantwortlichkeiten.
- **Risikomanagement**: Regelmäßige Analyse und Bewertung von Bedrohungen.
- **Zugriffs- und Authentifizierungsmethoden**: Rollenbasierte Rechte, Passwortrichtlinien und Multi-Faktor-Authentifizierung.
- **Datenverarbeitung und Datenschutz**: Klare Regeln zum Umgang mit personenbezogenen Daten und Backups.
- **Netzwerk- und Systemabsicherung**: Firewalls, Penetrationstests und Richtlinien für Updates.
- **Incident Management**: Geregelte Prozesse zur Meldung und Bearbeitung von Sicherheitsvorfällen.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

Vorteile von TISAX

- **Standardisierte Sicherheit** entlang der gesamten Lieferkette in der Automobilindustrie.
- **Verbesserter Datenschutz** für personenbezogene und unternehmenskritische Daten.
- **Nachweisbare Compliance** gegenüber Automobilherstellern und Partnern.
- **Reduzierung von Cyberrisiken** durch systematisches Sicherheitsmanagement.
- **Stärkung des Vertrauens** zwischen Herstellern und Zulieferern.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

TISAX-Checkliste für Unternehmen

Ziel: Herausfinden, ob Ihr Unternehmen die Anforderungen von TISAX erfüllt.

1. Sicherheitsmanagement

Fragen:	Ja	Nein
Ist ein Informationssicherheitsmanagementsystem (ISMS) etabliert?	☐	☐
Wird regelmäßig ein Risikomanagement durchgeführt?	☐	☐
Gibt es einen benannten Sicherheitsbeauftragten?	☐	☐
Werden aktuelle Sicherheitshinweise an Mitarbeitende weitergegeben?	☐	☐
Sind klare IT-Sicherheitsrichtlinien vorhanden?	☐	☐

---

2. Zugriffs- und Authentifizierungsmethoden

Fragen:	Ja	Nein
Existieren Benutzerrollen zur Regelung von Zugriffsrechten?	☐	☐
Wird Multi-Faktor-Authentifizierung (MFA) genutzt?	☐	☐
Werden Passwörter und Benutzerkennungen regelmäßig geändert?	☐	☐
Gibt es verbindliche Richtlinien zur Passwort- und Authentifizierungssicherheit?	☐	☐

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

3. Datenverarbeitung und Datenschutz

Fragen:	Ja	Nein
Werden alle erhobenen Daten vertraulich behandelt?	☐	☐
Werden Mitarbeitende regelmäßig zur Vertraulichkeit geschult?	☐	☐
Existieren klare Regeln für die Löschung personenbezogener Daten?	☐	☐
Werden Dateisysteme und Datenbanken regelmäßig gesichert?	☐	☐
Werden Mitarbeitende aktiv über Sicherheitsrisiken informiert (z. B. Intranet)?	☐	☐

---

4. Netzwerk- und Systemabsicherung

Fragen:	Ja	Nein
Sind Netzwerke so konfiguriert, dass Angriffe abgewehrt werden (z. B. Firewalls)?	☐	☐
Werden Server und Systeme regelmäßig auf Sicherheit geprüft (z. B. Penetrationstests)?	☐	☐
Gibt es klare Richtlinien für Updates und Patches?	☐	☐
Werden Systeme regelmäßig auf Sicherheitslücken überprüft?	☐	☐
Sind kryptografische Sicherheitsregeln für den Betrieb definiert?	☐	☐

---

5. Meldungen von Sicherheitsvorfällen

Fragen:	Ja	Nein
Wissen Mitarbeitende, wie sie bei einem Cyberangriff reagieren müssen?	☐	☐
Existiert eine Anleitung zur Meldung von Sicherheitsvorfällen?	☐	☐
Werden Vorfälle automatisch erkannt und gemeldet?	☐	☐
Werden Sicherheitsvorfälle in einem Protokoll dokumentiert?	☐	☐
Werden Mitarbeitende im Incident Management regelmäßig geschult?	☐	☐

Auswertung der Checkliste

Anzahl „Ja“ Antworten	Einschätzung
0–2	Wahrscheinlich nicht TISAX-relevant, alternative Standards prüfen.
3–5	Möglicherweise betroffen – eingehendere Prüfung empfohlen.
6 oder mehr	Sehr wahrscheinlich betroffen – Vorbereitung auf TISAX dringend empfohlen.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg