# DIE WICHTIGSTEN FAKTEN ZUR „TISAX“ ZERTIFIZIERUNG

Die „TISAX“ (**T**rusted **I**nformation **S**ecurity **A**ssessment E**x**change) Zertifizierung ist eine Informationssicherheits-zertifizierung, welche einen Großteil der Zulieferer und Dienstleister der deutschen Automobilhersteller und deren Tochterunternehmen betrifft.

Nicht nur die klassischen produzierenden Unternehmen sind seit 2017 von „TISAX“ betroffen, sondern auch eine Vielzahl von Dienstleistern wie z.B. Marketing Unternehmen, Schulungsanbieter oder sogar Fotostudios.

Nach ungefähr 3 Jahren kann man „TISAX“ definitiv als etabliert und bewährt bezeichnen. Die Anforderungen sind transparent und lassen sich auch klar in die Praxis übertragen, so dass bei guter Vorbereitung einer erfolgreichen Zertifizierung nichts im Wege stehen sollte.

Daher stellt dieser Artikel kurz die wichtigsten Fakten um „TISAX“ dar und was die wichtigen Schritte auf dem Weg zur Zertifizierung sind.

**Woraus besteht „TISAX“?**

„TISAX“ basiert auf dem Prüfkatalog **VDA ISA**, welcher von dem Arbeitskreis Informationssicherheit des **Verbands der Automobilindustrie (VDA)** verabschiedet wurde. Grundlegend orientiert sich der Standard an der internationalen Norm ISO/IEC 27001.

Der **Prüfkatalog** besteht insgesamt aus 4 Modulen, einem Hauptmodul und 3 Sondermodulen.

| Informationssicherheit | | |
|---|---|---|
| Anbindung Dritter | Datenschutz | Prototypenschutz |

Eine Zertifizierung erfolgt in der Regel mindestens immer gegen das **Hauptmodul Informationssicherheit** und bei Bedarf gegen eines oder mehrere der Sondermodule.

**Wie funktioniert die Zertifizierung?**

Grundsätzlich kann ein Unternehmen sich auch proaktiv zertifizieren lassen, d.h. ohne das eine Aufforderung durch einen der Automobilhersteller vorliegt. In der Praxis wird der Vergabeprozess genutzt, um die Anforderungen zu platzieren und entsprechend durchzusetzen. Wenn Ihr Unternehmen auf einen Vertrag bietet oder dieser erneuert wird, wird der Einkauf in Abstimmung mit der jeweiligen Fachabteilung des Automobilherstellers festlegen, ob eine TISAX-Zertifizierung notwendig ist und welche Module relevant sind. Abgesehen von der Festlegung der Module, wird auch bestimmt nach welchem **Level** die Prüfung des Hauptmoduls Informationssicherheit erfolgt:

| Level | Prüfungsgegenstand |
|---|---|
| 2 | Modul Informationssicherheit nach hohem Schutzbedarf |
| 3 | Modul Informationssicherheit nach sehr hohem Schutzbedarf |

**Für wen ist „TISAX“ relevant, wer muss sich zertifizieren?**

Jedes Unternehmen, welches Informationen mit einem **hohen Schutzbedarf (Level 2)** oder **sehr hohem Schutzbedarf (Level 3)** von VW, BMW, Porsche, Audi, Daimler oder deren Tochterunternehmen erhält, muss sich in der Praxis nach „TISAX“ zertifizieren lassen. Jedoch sehen wir, dass auch immer mehr der großen Zulieferer auf den Standard aufspringen und auch von Ihren Partnerunternehmen und Zuliefern erwarten, dass diese über eine TISAX-Zertifizierung verfügen. „TISAX“ ist ganz klar zu einem relevanten Wettbewerbsfaktor geworden. In diesem Zusammenhang kann es absolut Sinn machen sich proaktiv zu zertifizieren.

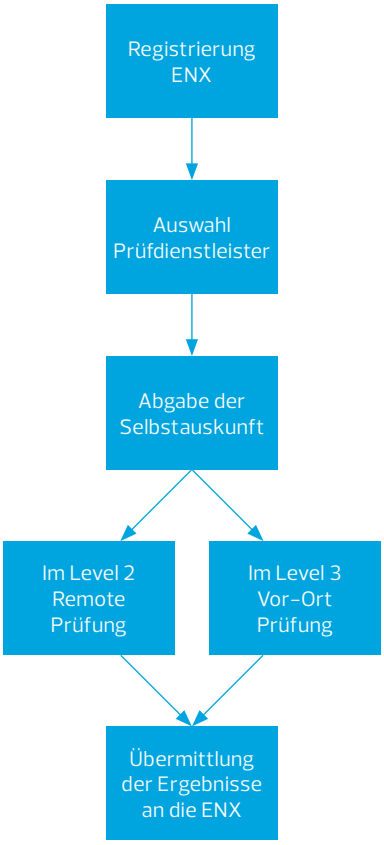
**Wie läuft eine Zertifizierung ab?**

Unternehmen, die Sich zertifizieren lassen wollen, müssen sich bei der **Governance Organisation ENX** registrieren. Die ENX verwaltet die Registrierung und die Ergebnisse der durchgeführten Prüfungen.

Anschließend folgt „TISAX" einem sehr praxisorientierten Zertifizierungsansatz, so dass sich, sofern man sich gut vorbereitet hat und den nötigen Reifegrad in der Informationssicherheit besitzt, auch in relativ kurzer Zeit eine Zertifizierung erlangen lässt.

Im Groben folgt die Zertifizierung den folgenden Schritten:

1. Registrierung bei der ENX
2. Auswahl eines Prüfdienstleisters
3. Ausfüllen der Selbstauskunft – der VDA ISA Fragebogen wird von dem Auditee eigenständig befüllt
4. Prüfung durch den Auditor, im Level 2 **remote** und im Level 3 durch eine **Vor-Ort**-Prüfung
5. Abschluss der Prüfung und Übermittlung der Ergebnisse an die ENX




**Wie kann man sich auf eine „TISAX" Zertifizierung vorbereiten?**

Sofern schon eine Aufforderung zur Zertifizierung erfolgt ist, sollte detailliert bestimmt werden, welche Module und welcher Level für die Zertifizierung relevant sind. Dies sollte final immer mit dem anfordernden Automobilkonzern oder Zulieferer abgestimmt werden.

Anschließend sollte der Scope identifiziert werden, d.h. welche Informationen sind im Fokus der Zertifizierung und wo werden diese genutzt bzw. verarbeitet. Dies kann sich auf Lokationen, Abteilungen, Prozesse und natürlich Systeme beziehen.

Ist dies erfolgt, ist es im Rahmen einer guten Vorbereitung wichtig einmal realistisch den aktuellen Reifegrad der Informationssicherheit zu ermitteln. Hierzu sollte die **Selbstauskunft** einmal vollumfänglich mit Prozess-, Dokumenten- und Umsetzungsreferenzen ausgefüllt werden. Wichtig im Rahmen der TISAX-Prüfung ist es zu allen Controls die **zwei elementaren Elemente** aufzuzeigen. Erstens, wie und wo ist die Vorgabe formal dokumentiert; hierbei wird es sich in der Regel um eine **Richtlinie** handeln. Zweitens, wie ist die Vorgabe in der Praxis umgesetzt.

Durch diesen Schritt können **eventuelle Gaps** identifiziert und strukturiert in eine **Roadmap** einfließen, um diese zu schließen.

**Wie kann RSM Sie in diesen Schritten unterstützen?**

**Unsere erfahrenen TISAX-Auditoren können Sie bei jedem dieser Schritte begleiten und Sie optimal auf die Prüfung vorbereiten:**

- Schulung zu den wichtigsten Aspekten von „TISAX". Wir machen Ihre Cybersecurity-Experten fit in „TISAX" und erklären alles rund um die Anforderungen und die Zertifizierung.
- Identifizierung der Informationen, die Gegenstand der Prüfung sind und deren komplementären Prozesse, Systeme und Anwendungen. Konsolidierung dieser, um den „Compliance Footprint" zu reduzieren.
- Durchführen eines **„readiness-assessments"**. Gemeinsam mit unseren Experten simulieren Sie die Prüfung und identifizieren relevante Gaps.
- Entwickeln einer Roadmap, um die Lücken strukturiert zu schließen.
- Implementierung eines Frameworks (Information Security Management System), um den TISAX-Anforderungen gerecht zu werden.

Unsere Cybersecurity-Experten unterstützen Sie gerne:

**Kontakt**

**RSM Competence Team „Risk Advisory Services"**
Gregor Strobl – Co-Head RAS
Jonathan Schlaeger – Manager Cyber Security

Kontakt über:
+49 40 35006-225
RAS@rsm.de