TISAX® Assessment in der Automobilindustrie

White Paper TISAX®

Die Automobilindustrie hat eine der komplexesten Lieferketten der Welt. Hersteller und Kunden fordern daher bei der Übertragung oder dem Austausch von Daten eine robuste, belastbare und konsistente Informationssicherheit entlang der gesamten Wertschöpfungskette - nicht nur während der Entwicklung von Prototypen. Der zuverlässige Nachweis der Datensicherheit ist Voraussetzung in der Automobilindustrie, um ein zuverlässiger Teil der Zulieferkette zu sein. TISAX® Assessments ermöglichen es Unternehmen, die Einhaltung der relevanten Anforderungen an die Informationssicherheit glaubwürdig zu dokumentieren.

Hintergrund

Der Test- und Austauschstandard TISAX® (Trusted Information Security Assessment Exchange) basiert auf dem VDA ISA-Fragebogen, der wiederum vom ISO 27001 Standard abgeleitet wurde. Dieser Fragebogen dient der Selbstbewertung und wurde in den letzten Jahren von den Mitgliedsunternehmen für interne Zwecke sowie für Lieferanten- und Dienstleister-Audits verwendet. In der Praxis hat dies oft dazu geführt, dass ein Dienstleister oder Lieferant, der sensible Informationen verarbeitet, mehrfach, manchmal sogar in kurzen Abständen, auditiert wird. Das TISAX®-Modell wurde daher entwickelt, um solche Mehrfachaudits zu verhindern und Prozesse zu rationalisieren, indem es die gegenseitige Anerkennung von Informationssicherheitsbewertungen zwischen den verschiedenen Zulieferern in der Automobilindustrie ermöglicht. Das bedeutet, dass der Prüfstandard nicht nur unternehmensübergreifend, sondern auch branchenübergreifend eingesetzt werden kann, ohne dass zusätzliche firmenspezifische Fragebögen benötigt werden.

Ihre Vorteile

Automobilunternehmen profitieren bei einem TISAX® Assessment von verschiedenen Vorteilen:

- In der Automobilindustrie haben der ENX-Verband und der VDA Anfang 2017 die TISAX® Bewertung eingeführt, um den unternehmensübergreifenden Austausch von Nachweisen der Informationssicherheit zwischen Herstellern, Zulieferern und Dienstleistern zu erleichtern.
- Die TISAX®-Plattform spart sowohl Zeit als auch Geld. Dadurch werden doppelte und mehrfache Prüfungen der Informationssicherheit vermieden.
- Das geprüfte Unternehmen entscheidet selbst, mit wem es seine Ergebnisse teilt.
- Die TISAX®-Registrierung führt zu einem erhöhten Sicherheitsbewusstsein der Mitarbeiter und fördert die Unternehmenswerte.
- Registrierte Unternehmen können die Plattform nutzen, um sicherzustellen, dass auch ihre Lieferanten und Dienstleister das erforderliche Maß an Informationssicherheit erfüllen.

Wer ist betroffen?

Hersteller, Zulieferer und Dienstleister der gesamten Zulieferkette der Automobilindustrie, die sensible Informationen verarbeiten, haben ein Interesse an der aktiven Nutzung von TISAX®. Zulieferer der Automobilindustrie müssen beispielsweise die Einhaltung der Vorschriften und der strengen Anforderungen an die Informationssicherheit regelmäßig nachweisen. In den meisten Fällen basiert die Einhaltung auf dem Anforderungskatalog der VDA ISA (Information Security Assessment). Ein gegenseitig akzeptiertes und solides Maß an Informationssicherheit in der Branche schützt auch die von den Lieferanten intern bereitgestellten Informationen. Zudem wird den Kunden bestätigt, dass mit ihren sensiblen Informationen sorgfältig umgegangen wird. Die ENX Association wurde vom VDA als neutrale Instanz mit dem Betrieb der Austauschplattform TISAX® betraut.

TISAX® ist mehr als nur eine technische Checkliste

Der Test- und Austauschmechanismus basiert auf dem ISA Anforderungskatalog des VDA. Durch TISAX® entfällt die Notwendigkeit anderer umfangreicher Kataloge, die von großen Automobilherstellern herausgegeben werden. Da alle ISO-Normen in den ersten Abschnitten die gleiche übergeordnete Struktur aufweisen, enthält auch der TISAX® ISA-Katalog mit seinen Verweisen auf ISO 27001 wesentliche Anforderungen an das Qualitätsmanagement nach ISO 9001:2015. Ein robustes IT-Sicherheitsmanagementsystem basiert immer auf dem Qualitätsmanagement und vor allem auf den dafür erforderlichen organisatorischen Maßnahmen. Damit legen die an TISAX® teilnehmenden Unternehmen auch den Grundstein für eine mögliche spätere Zertifizierung nach ISO 27001.

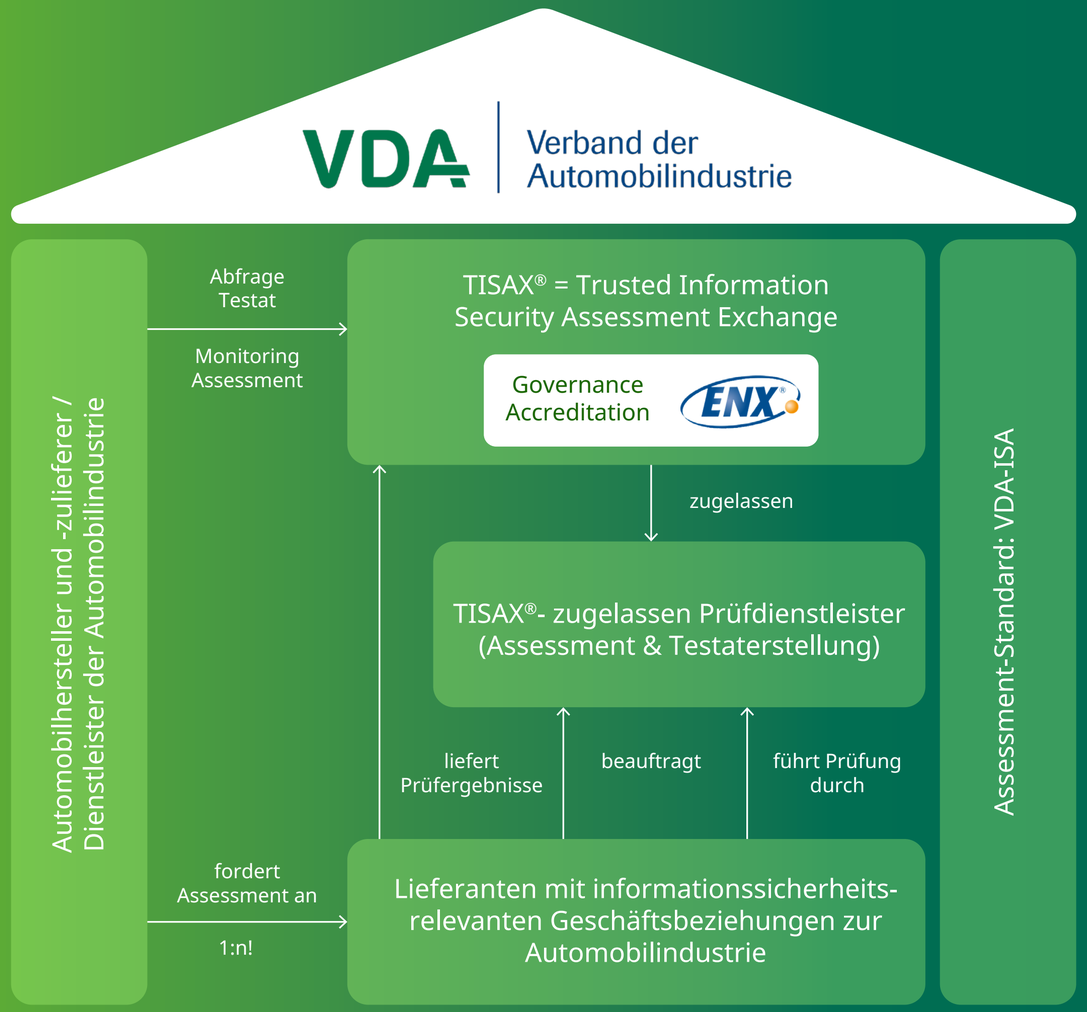

Abbildung 1: VDA TISAX®-Modell. Quelle: Eigene Darstellung nach VDA (2017, https://www.vda.de/de/Search-Results.html?q=tisax+modell)

Teilnahme an TISAX®
in vier Schritten

1 Registrierung des Unternehmens als Teilnehmer auf der TISAX®-Plattform

2 Wahl eines Testdienstleisters

3 Überprüfung anhand von Dokumenten oder Besichtigungen vor Ort

4 Austausch von Testergebnissen mit ausgewählten Lieferanten und Dienstleistern

DEKRA

Der Umfang der Prüfung

Die Grundprüfung zielt auf „Informationssicherheit“ ab und kann um die optionalen Module „Anbindung an Dritte“, „Datenschutz“ und „Prototypenschutz“ erweitert werden. Der ISA-Anforderungskatalog verwendet ein umfassendes Arbeitsblatt mit verschiedenen Testkategorien, um den Prozess zu beschreiben, mit dem Unternehmen ihren Reifegrad der Informationssicherheit (Grundprüfung) bestimmen.

Beginnen Sie mit einer Bewertung der Informationssicherheit

Der VDA empfiehlt, die Selbsteinschätzung mit dem Tabellenblatt „Informationssicherheit“ zu beginnen. Dieser Fragebogen listet 52 Sicherheitsthemen (Controls) auf, mit denen sich das Unternehmen einen umfassenden Überblick über den eigenen Informationssicherheitsstatus verschaffen muss. Jedes dieser Themen muss mit einem Zielerreichungsgrad (von Stufe 0 bis 5) bewertet werden, um eine Gesamtbeurteilung zu erhalten.

Der Anforderungskatalog erfordert einen hohen Umsetzungs- und Reifegrad im Unternehmen, insbesondere für die folgenden Sicherheitsthemen:

- **Sensibilisierung und Schulung der Mitarbeiter**
  Sensibilisierungsmaßnahmen sollten Erkenntnisse aus Vorfällen in der Informationssicherheit enthalten.
- **Benutzer-Registrierung**
  Sammelkonten sollten nur in Ausnahmefällen verwendet werden, da sie die eindeutige Zuordnung von Benutzeraktivitäten erschweren.
- **Change Management**
  Ein effektiver Änderungsmanagementprozess führt zu einer geringeren Fehlerquote bei den durchgeführten Änderungen und trägt somit zu einem sichereren Betrieb bei.
- **Schutz gegen Malware**
  Aktuelle Virensignaturen sind eine Voraussetzung für effektive Endgerätesicherheit.

- **Informationssicherheit (Backup)**
  Die Datensicherheit muss durch eine doppelte Kontrolle der Sicherungen mittels Maßnahmen, wie z.B. Systemwiederherstellungen, gewährleistet werden.
- **Schwachstellenverfolgung (Patch-Management)**
  Die rechtzeitige Installation von Patches stärkt die Systeme und Anwendungen und reduziert so Sicherheitslücken in der Betriebssoftware.
- **Verarbeitung von Informationssicherheitsvorfällen**
  Vorfälle der Informationssicherheit müssen entsprechend ihrer Schwere priorisiert und angemessen behandelt werden.4. Warum sollte ich mein Unternehmen nach

Andere Sicherheitsthemen/„Controls“ sind:

- Informationssicherheitpolitik
- Informationssicherheit in Projekten
- Mobile Geräte
- Sicherheitszonen
- Schutzmaßnahmen im Liefer- und Versandbereich
- Ereignisprotokollierung
- Netzwerkdienste
- Geheimhaltungsvereinbarungen
- Voraussetzungen für Informationsbeschaffungs-Systeme
- Sicherheit im Software-Entwicklungsprozess
- Prüfung der Wirksamkeit

Welchen Grad haben Sie erreicht?

Die Umsetzung der VDA ISA-Anforderungen wird durch die Zuordnung von Reifegraden bewertet. Je nach Bedeutung der Prüfungen variieren die angestrebten Reifegrade zwischen Stufe 2 und Stufe 4. Besonders wichtige Anforderungen erfordern jedoch Reifegrade von 3 und 4.

- **Level 0**
  Die Umsetzung der Anforderungen ist unvollständig. Es existiert kein Prozess oder der Prozess erreicht nicht die erforderlichen Ergebnisse.
- **Level 1**
  Die notwendigen Anforderungen wurden entsprechend den Bedürfnissen an die Informationssicherheit erfüllt. Ein Prozess existiert und hat sich bewährt, ist aber nicht vollständig dokumentiert. Seine Zuverlässigkeit kann daher nicht vollständig gewährleistet werden.
- **Level 2**
  Der Prozess zur Zielerreichung wird kontrolliert und dokumentiert, zudem liegen Nachweise (z.B. Dokumentation) vor.
- **Level 3**
  Der Prozess zur Zielerreichung ist etabliert und die Prozesse sind verknüpft, um bestehende Abhängigkeiten abzubilden. Die Dokumentation ist aktuell und gepflegt.
- **Level 4**
  Die Anforderungen aus Stufe 3 sind erfüllt. Darüber hinaus werden Messungen der Ergebnisse (z.B. KPI) durchgeführt und machen den Prozess vorhersehbar.
- **Level 5**
  Die Anforderungen aus Stufe 4 werden erfüllt und zusätzliche Ressourcen (z.B. Personal und Geld) werden zur Optimierung des Prozesses eingesetzt. Es findet eine kontinuierliche Verbesserung des Prozesses statt.

Das Ergebnis der Bewertung

Die Ergebnisse der Prüfkataloge werden in einer Übersicht zusammengefasst und für den späteren Druck vorformatiert. Der VDA hat für den Basistest „Informationssicherheit“ ein übersichtliches Spinnennetzdiagramm für die 52 Sicherheitsthemen entwickelt. Dadurch soll auf einen Blick der ermittelte Reifegrad der 52 Themen beziehungsweise deren Abweichungen von den Ziel-Controls dargestellt werden. Besonders kritische Abweichungen vom Ziel-Reifegrad werden in einem speziellen Ampel-System in Rot dargestellt. „Bei der Berechnung des Gesamtergebnisses werden die Ergebnisse von Controls, die den Ziel-Reifegrad übererfüllen, gekürzt und der Durchschnitt ermittelt. Dies stellt sicher, dass die Anforderungen themenübergreifend erfüllt werden und kein Ausgleich von über- und untererfüllten Controls stattfindet“, heißt es in der Erklärung des VDA zu den Prüfkatalogen.

Fallbeispiel

Ein Zulieferer der Automobilindustrie für einfache mechanische Komponenten hat den VDA ISA-Prüfkatalog für den Basistest „Informationssicherheit“ durchgearbeitet. Der Lieferant hat den erreichten Reifegrad für jedes der 52 Sicherheitsthemen (18 übergeordnete Themen) durch die Analyse von Dokumenten und die Durchführung von Interviews und internen Audits ermittelt. Das Spinnennetzdiagramm auf der rechten Seite zeigt das Gesamtergebnis, den Grad der Zielerreichung sowie die Abweichungen vom Zielreifegrad.

Die Bewertung ergab unter anderem, dass der Reifegrad an verschiedenen zentralen Prüfpunkten zu gering war. Diese niedrigen Reifegrade spiegeln sich in dem Spinnennetzdiagramm für die Kategorien ISMS (1), Organization of Information Security (6) und Information Security Aspects of Business Continuity Management (17) wider.

DEKRA

Gesamtergebnis: 2,62

Maximal erreichbar: 3.00

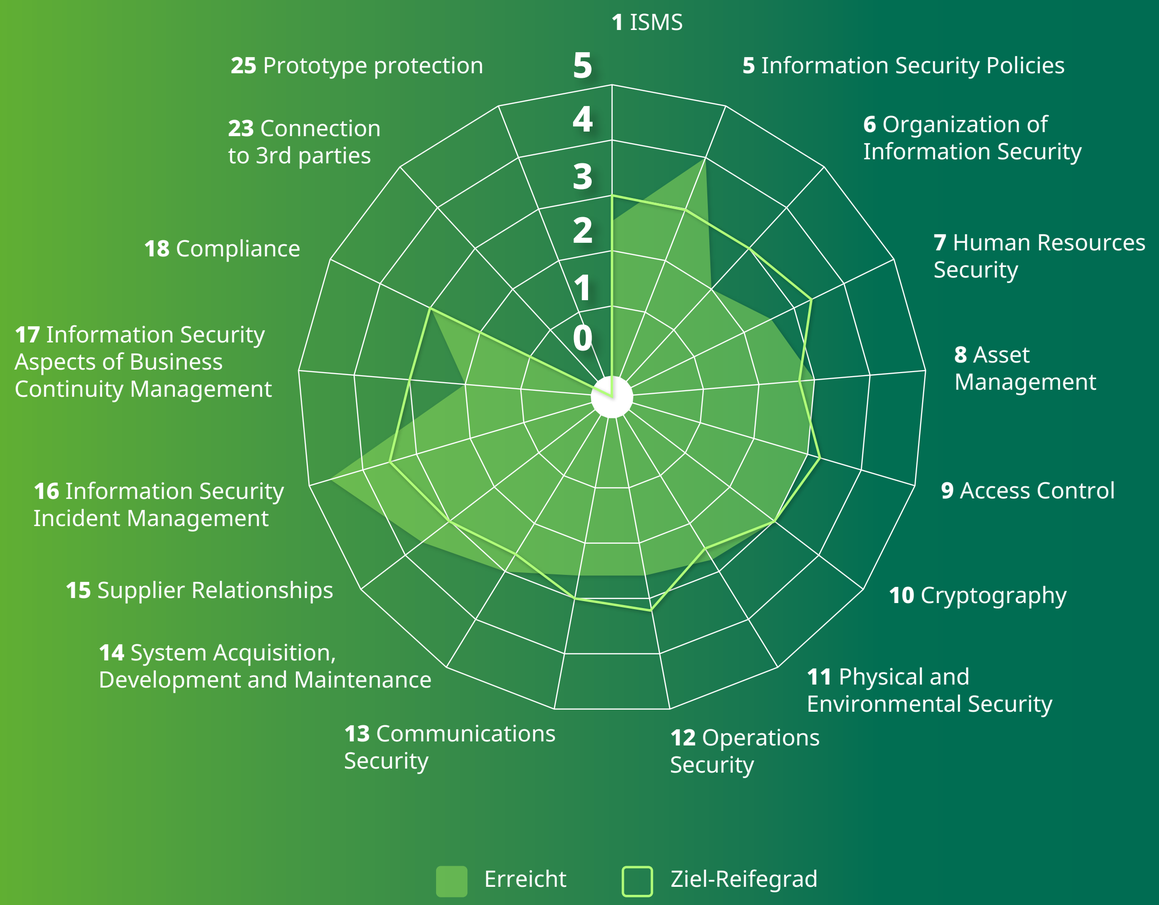

Abbildung 2: Bewertung der Informationssicherheit.
Quelle: Eigene Illustration basierend auf einem fiktiven Kunden

Ihr Partner

Wir sind berechtigt, Unternehmen, die sensible Informationen für die Automobilindustrie verarbeiten, nach dem TISAX®-Standard zu prüfen. Die Prüfung ist drei Jahre gültig. Durch die Teilnahme an TISAX® und die Bewertung durch unsere Experten eröffnen sich für Unternehmen neue Möglichkeiten, Aufträge zu gewinnen.

Sind Sie an einem TISAX® Assessment interessiert, um die Zuverlässigkeit Ihrer Informationssicherheit in der Automobilindustrie nachzuweisen? Dann fordern Sie jetzt ein Angebot an!

Kontaktieren Sie uns!

Ausgezeichnet – das DEKRA Siegel

Setzen Sie ein Ausrufezeichen für höchste Qualität und Zuverlässigkeit – branchenübergreifend und international. Das DEKRA Siegel leistet beste Dienste als Imageträger, Marketinginstrument und um sich vom Wettbewerb abzuheben. So zeigen Sie Ihren Kunden und Geschäftspartnern, dass Leistung bei Ihnen ihr Geld wert ist. Wir unterstützen Sie gerne dabei.

Wünschen Sie weitere Informationen?
Besuchen Sie unsere Website:

dekra-certification.de