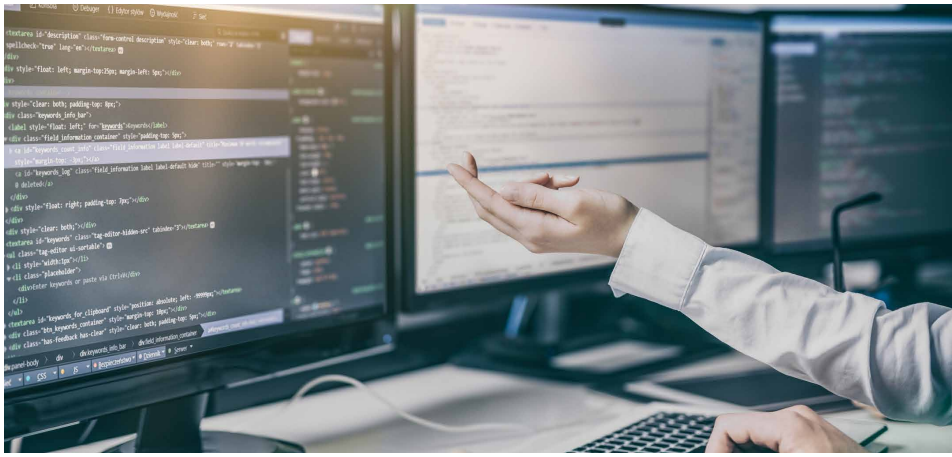
DEKRA
Alles im grünen Bereich.

TISAX®
Informationssicherheit in der Automobilindustrie



Das Assessment Label:
Nachweis für den sicheren Informationsaustausch in der Automobil-Lieferkette.

Die Automobilindustrie verfügt weltweit über eine der am meist verzweigten Lieferketten. Hersteller und Auftraggeber verlangen, dass der Schutz der überlassenen oder ausgetauschten Daten sichergestellt wird. Nicht nur bei der Mitarbeit an Prototypen muss garantiert sein, dass über die gesamte Wertschöpfungskette ein robustes / belastbares und vergleichbares Informationssicherheitsniveau besteht. Hierfür den verlässlichen Nachweis zu bringen, wird zur entscheidenden Voraussetzung, um weiterhin Teil der Lieferkette zu bleiben oder zu werden.

- Um in der Automobilindustrie den Nachweis der Informationssicherheit unternehmensübergreifend zwischen Herstellern, Zulieferern und Dienstleistern zu erleichtern, hat die ENX Assiciation gemeinsam mit dem VDA Anfang 2017 das TISAX®-Modell auf den Markt gebracht. TISAX® steht für Trusted Information Security Assessment Exchange.
- Die TISAX®-Plattform spart Zeit und Geld. Doppel- und Mehrfachüberprüfungen der Informationssicherheit im Unternehmen werden vermieden.
- Das auditierte Unternehmen entscheidet selbst, mit wem sie die Resultate teilt.
- Eine TISAX®-Registrierung führt zu einem gesteigerten Sicherheitsbewusstsein der Mitarbeiter und zum Schutz der eigenen Unternehmenswerte.
- Registrierte Unternehmen können die Plattform nutzen um sicherzustellen, dass auch ihre Lieferanten und Dienstleister wiederum die Informationssicherheit im notwendigem Maß (Level) erfüllen.

(1) Hintergrund

Der Prüf- und Austauschstandard TISAX® basiert auf dem VDA ISA-Fragenkatalog auf Grundlage der Norm ISO 27001. Dieser Fragenkatalog dient als Selbst-Assessment und wurde von den Mitgliedsunternehmen in den vergangenen Jahren für interne Zwecke und für Prüfungen bei Lieferanten und Dienstleistern verwendet. Allerdings hatte dies in der Praxis häufig die Folge, dass ein Dienstleister bzw. Lieferant, der sensible Informationen verarbeitet, in mitunter kurzen Abständen mehrfach geprüft wurde. Vor diesem Hintergrund ist das TISAX®-Modell zur gegenseitigen Anerkennung von Assessments der Informationssicherheit zwischen den unterschiedlichen Anbietern in der Automobilindustrie entwickelt worden. Somit ist der Prüfstandard nicht nur unternehmens-, sondern auch branchenübergreifend einsetzbar. Es entfallen zusätzliche unternehmensspezifische Fragebögen.

(2) Wer ist betroffen?

Hersteller, Zulieferer und Dienstleister aller Stufen der Lieferketten, die für die Geschäftsbeziehungen in der Automobilindustrie sensible Informationen verarbeiten, sollten ein Interesse an einer aktiven Nutzung von TISAX® haben. So müssen Zulieferer der Automobilindustrie in regelmäßigen Abständen nachweisen, ob die hohen Anforderungen in punkto Informationssicherheit eingehalten werden. Grundlage ist in den meisten Fällen der Anforderungskatalog VDA ISA (ISA – Information Security Assessment).

Ein gegenseitig in der Branche akzeptiertes und geprüftes Niveau der Informationssicherheit schützt auch die Informationen der Zulieferer im eigenen Hause und bestätigt den Auftraggebern den sorgfältigen Umgang mit sensiblen Informationen. Mit der Markteinführung im Januar 2017 haben sich bislang bereits 1.000 Unternehmen mit über 1.500 Standorten in 32 Ländern bei TISAX® registriert, und über 500 Prüfungen wurden bereits durchgeführt.

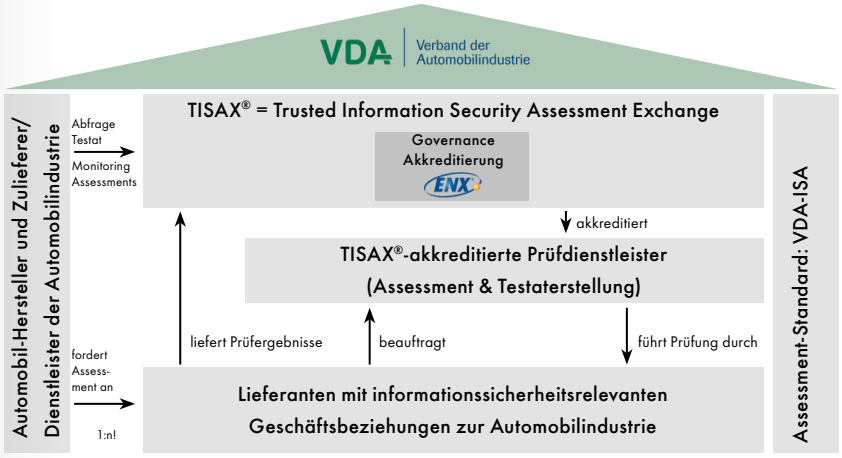


Abbildung 1: VDA TISAX-Modell. Quelle: eigene Darstellung nach VDA (2017, https://www.vda.de/de/Search-Results.html?q=tisax+modell)

Der Betreiber der Austauschplattform TISAX® ist die ENX Association. Sie ist vom VDA als neutrale Instanz mit dem Betrieb betraut worden.

(3) TISAX® ist mehr als eine technische Checkliste

Weil alle ISO-Normen in den ersten Abschnitten denselben Aufbau (High Level Struktur) haben, enthält auch der ISA-Katalog von TISAX® mit den Bezügen zur ISO 27001 wesentliche Anforderungen aus dem klassischen Qualitätsmanagement nach ISO 9001:2015. Ein robustes Managementsystem zur IT-Sicherheit beruht immer auf dem Qualitätsmanagement, und vor allem auf den dort geforderten organisatorischen Maßnahmen. Damit legen an TISAX® teilnehmende Unternehmen auch wichtige Grundlagen für eine etwaige spätere Zertifizierung nach ISO 27001.

(4) Die Teilnahme an TISAX® in vier Schritten

1. Definition des Scopes und des Assessment-Levels sowie Registrierung des Unternehmens als Teilnehmer auf der TISAX® Plattform
2. Wahl eines Prüfdienstleisters
3. Assessment anhand des VDA ISA-Fragenkatalog, über den Stand der Informationssicherheit im Unternehmen mit Dokumentenanalysen, Interviews, interne Audits
4. Die Prüfergebnisse werden an die TISAX® Plattform gemeldet. Austausch des Assessment-Berichts mit den Prüfergebnissen nach Freigabe durch das auditierte Unternehmen: http://enx.com/tisax/

(5) Der Prüfungsumfang

Grundlage des Prüf- und Austauschmechanismus ist der Anforderungskatalog ISA (Information Security Assessment) vom VDA. Dadurch entfallen die Sonderanforderungen mit teils umfangreichen Spezialkatalogen der großen Automobilhersteller.
Das Assessment baut auf dem Themenbereich „Informationssicherheit“ als Grundprüfung auf und ist erweiterbar um die optionalen Module „Anbindung an Dritte“, „Datenschutz“ sowie den „Prototypenschutz“. Der Anforderungskatalog ISA beschreibt über eine umfassende Excel-Tabelle mit verschiedenen Prüfkategorien den Prozess, den Unternehmen durchlaufen müssen, um den eigenen Reifegrad z. B. hinsichtlich der „Informationssicherheit“ (Grundprüfung) zu bestimmen.

Mit einem Assessment zur Informationssicherheit starten

Der VDA empfiehlt, das Selbst-Assessment mit dem Tabellenblatt „Informationssicherheit“ zu starten. In diesem Fragekatalog sind 52 Sicherheitsthemen (Controls) genannt, anhand derer sich das Unternehmen einen umfassenden Überblick über den Stand der eigenen Informationssicherheit verschaffen muss. Jedes dieser Themen muss mit einem Grad der Zielerreichung (von Level 0 bis 5) bewertet werden, um eine Gesamtbeurteilung zu erhalten.

Der Anforderungskatalog verlangt insbesondere bei folgenden Sicherheitsthemen einen hohen Umsetzungs- bzw. Reifegrad im Unternehmen:

- **Sensibilisierung und Schulung der Mitarbeiter**
  Die Inhalte von Awareness-Maßnahmen sollten Erkenntnisse aus Informationssicherheits-vorfällen berücksichtigen.
- **Benutzerregistrierung**
  Sammelaccounts sollten grundsätzlich nicht bzw. nur in Ausnahmefällen genutzt werden, da eine eindeutige Zuordnung von Benutzeraktivitäten erschwert wird.
- **Änderungsmanagement (Change Management)**
  Eine hohe Qualität des Change Management Prozesses führt zu einer geringen Fehlerquote von durchgeführten Änderungen und trägt so zu einem sicheren Betrieb bei.
- **Schutz vor Schadsoftware**
  Aktuelle Virensignaturen sind die Voraussetzung für eine effektive Endpoint Security.
- **Informationssicherung (Back-Up)**
  Die Qualität einer Datensicherung muss durch Kontrolle der Backups sichergestellt werden. Maßnahmen sind z. B. Datenrücksicherungen, System-Wiederherstellungen.
- **Verfolgung von Schwachstellen (Patch Management)**
  Die zeitnahe Installation von Patches härtet Systeme und Anwendungen und reduziert so Sicherheitslücken in der Betriebssoftware.
- **Bearbeitung von Informationssicherheitsvorfällen**
  Informationssicherheitsvorfälle müssen nach Ihrer Kritikalität angemessen priorisiert und behandelt werden.

Weitere zentrale Controls sind:

- **Informationssicherheitsrichtlinie**
- **Informationssicherheit in Projekten**
- **Mobile Endgeräte**
- **Sicherheitszonen**
- **Schutzmaßnahmen im Anlieferungs- und Versandbereich**
- **Event-Logging**
- **Netzwerkdienste**
- **Geheimhaltungsvereinbarungen**
- **Anforderungen an die Beschaffung von Informationssystemen**
- **Sicherheit im Software-Entwicklungsprozess**
- **Wirksamkeitsprüfung**

(6) Auf welchem Level sind Sie?

Die Umsetzung der jeweiligen Anforderungen nach VDA ISA wird mit unterschiedlichen Reifegraden beurteilt. Je nach Bedeutung der Controls variieren die Ziel-Reifegrade zwischen dem Level 2 und Level 4. Allerdings sind bei besonders wichtigen Anforderungen Reifegrade von 3 und 4 erforderlich.

- Level 0: Die Umsetzung der Anforderungen ist unvollständig. Es existiert kein Prozess bzw. der Prozess erreicht nicht die erforderlichen Ergebnisse.
- Level 1: Die je nach Schutzbedarf der Informationen notwendigen Anforderungen sind durchgeführt. Ein Prozess existiert und lässt erkennen, dass er funktioniert. Er ist jedoch nicht vollständig dokumentiert. Es kann daher nicht sichergestellt werden, dass er immer funktioniert.
- Level 2: Der Prozess zur Erreichung des Ziels ist gesteuert. Er ist dokumentiert und Nachweise (z.B. Dokumentationen) sind vorhanden.
- Level 3: Der Prozess zur Erreichung des Ziels ist etabliert, die Prozesse sind verknüpft, um existierende Abhängigkeiten abzubilden. Die Dokumentation ist aktuell und wird gepflegt.
- Level 4: Anforderungen aus Level 3, darüber hinaus finden Messungen der Ergebnisse (z.B. KPI) statt und machen den Prozess somit vorhersagbar.
- Level 5: Anforderungen aus Level 4, darüber hinaus werden zusätzliche Ressourcen (z.B. Personal und Geld) optimierend eingesetzt. Es findet eine kontinuierliche Verbesserung des Prozesses statt.

(7) Das Assessment-Ergebnis

Die Ergebnisse der Prüfkataloge werden in einem Überblick zusammengefasst und sind für den Ausdruck vorformatiert. Für die 52 Sicherheitsthemen der Grundprüfung zur Informationssicherheit hat der VDA ein übersichtliches Spinnennetz-Diagramm erarbeitet, um den ermittelten Reifegrad zu den jeweiligen 52 Sicherheitsthemen bzw. deren Abweichungen von Ziel-Controls auf einem Blick darzustellen.

Besonders kritische Abweichungen vom Ziel-Reifegrad werden in einem Ampelsystem 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 den Erläuterungen des VDA zu den Prüfkatalogen.

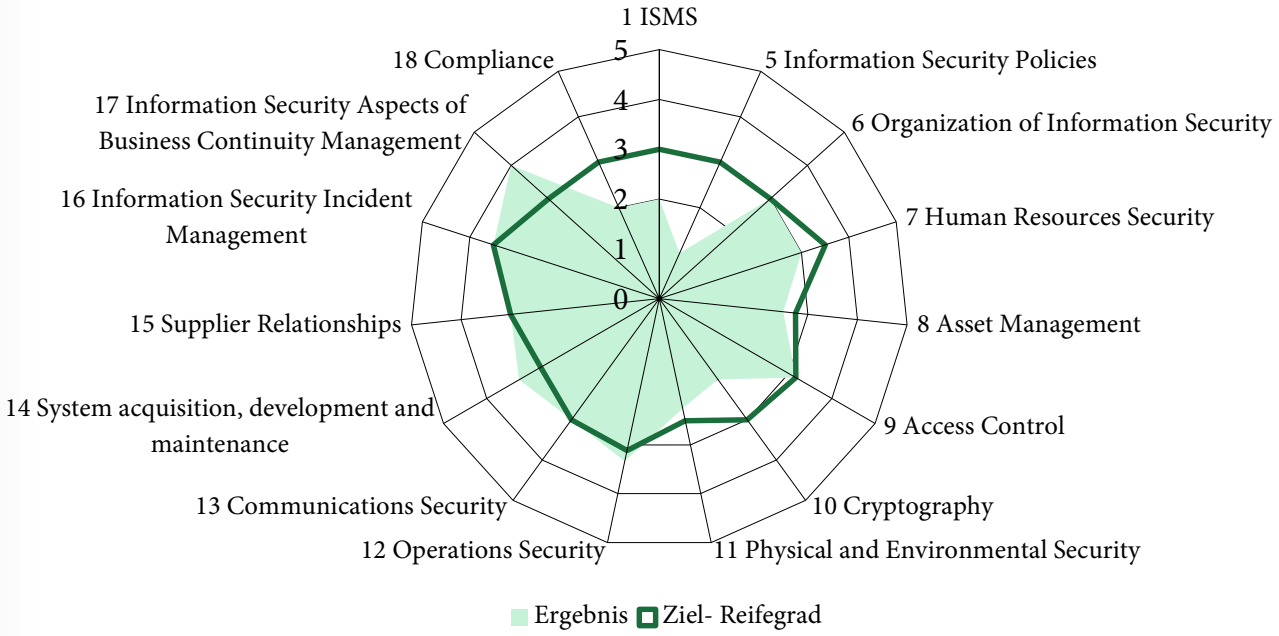
(8) Fallbeispiel

Ein Zulieferer von einfachen mechanischen Bauteilen für die Automobilindustrie hat den Prüfkatalog VDA ISA für die Grundprüfung „Informationssicherheit“ durchgearbeitet. Der Lieferant hat zu jedem der 52 Sicherheitsthemen (18 übergeordnete Themen) den jeweils erreichten Reifegrad anhand der Analyse von Dokumenten, Interviews und internen Audits ermittelt.

Das folgende Spinnendiagramm zeigt als Gesamtergebnis den Grad der Ziel-Erreichung und die Abweichungen vom Ziel-Reifegrad.

Gesamtergebnis: 2,49 Maximal erreichbar: 3,00

Abbildung 2: Information Security Assessment. Quelle: eigene Darstellung nach VDA (2017, https://www.vda.de/de/services/Publikationen/information-security-assessment.html)



Alles im grünen Bereich.

Das Assessment hatte u. a. bei folgenden zentralen Prüfpunkten (siehe Seite 7) einen zu niedrigen Reifegrad (in Rot das erreichte Level) aufgedeckt. Diese niedrigen Erfüllungsgrade spiegeln sich auch in dem Spinnendiagramm bei den Punkten Kategorien ISMS (1), Organization of Information Security Policies (6) und Access Control (9) wider.

Ihr Partner

DEKRA Certification ist befugt, Unternehmen, die für die Automobilindustrie sensible Informationen verarbeiten, nach dem TISAX®-Standard zu prüfen. Die Prüfung hat eine Gültigkeit von drei Jahren. Mit der Teilnahme an TISAX® und einer Bewertung durch DEKRA Certification erschließen Unternehmen neue Chancen für eine Auftragsvergabe.

- Unterstützung von der TISAX®-Planung bis zum - Prüfbericht
- Zentrale Ansprechpartner und schnelle Reaktionszeiten
- Mit einer zusätzlichen ISO 27001-Zertifizierungen positionieren Sie sich als ein sicherer Partner für Ihre Kunden.

Informationssicherheitsrichtlinie	3	1
Eine Organisation muss eine Richtlinie definieren, welche die Wichtigkeit und Bedeutung von Informationssicherheit für die Organisation widerspiegelt. Diese muss auf die Geschäftsstrategie, Vorschriften, Gesetze und potenzielle Bedrohungslagen der Informationssicherheit angepasst sein.		
Mobile Endgeräte	3	0
Der Umgang mit mobilen Endgeräten - insbesondere in ungeschützten Umgebungen - ist mit erhöhten Risiken verbunden (z. B. Verlust, Diebstahl, Infektion mit Malware). Damit die auf dem Gerät abgelegten Informationen geschützt sind, müssen technische Schutzmaßnahmen umgesetzt werden. Weiterhin sollten die Mitarbeiter auf die Gefahren im Umgang mit mobilen Endgeräten sensibilisiert werden.		
Benutzerregistrierung	4	2
Durch die Verwendung eindeutiger und personalisierter Benutzerkennungen (Benutzerkonten) wird gewährleistet, dass Handlungen eindeutig nachvollziehbar sind. Die Anmeldeinformationen (z. B. Passwörter) dürfen nur dem berechtigten Benutzer bekannt sein. Für den Lifecycle von Benutzerkonten sind definierte Prozesse vorhanden. Es erfolgt eine regelmäßige Überprüfung der vorhandenen Benutzerkonten auf ihre Notwendigkeit.		

Sie sind an einem TISAX Assessment zum Nachweis der belastbaren Informationssicherheit in der Automobilindustrie interessiert? Dann fordern Sie jetzt ein Angebot an!

IHR KONTAKT FÜR WEITERE FRAGEN
Karsten Fischer
Key Account Manager Cyber Security
Telefon +49.2394.242058
E-Mail karsten.fischer@dekra.com

DEKRA Certification GmbH
Handwerkstraße 15
70565 Stuttgart
Telefon +49.711.7861-2566
Telefax +49.711.7861-2615
Mail certification.de@dekra.com
Web www.dekra-certification.de