Technischer Leitfaden
TISAX® - Trusted Information Security Assessment Exchange

DEKRA
Alles im grünen Bereich.

In der heutigen digitalisierten Geschäftswelt ist die Informationssicherheit zu einer immer wichtigeren Voraussetzung für die Zusammenarbeit von Herstellern, Zulieferern und Dienstleistern über die gesamte Wertschöpfungskette der Automobilindustrie geworden. Der Trusted Information Security Assessment Exchange (TISAX®) bietet den Mitgliedern einen standardisierten Informationssicherheitsstatus, der von Partnern aus der gesamten Automobilindustrie genutzt werden kann.

Inhalt

1. TISAX® Übersicht und Vorteile

Ziele

TISAX® wurde speziell für die Automobilindustrie entwickelt und zielt darauf ab, die Integrität Ihres Informationssicherheitssystems zu gewährleisten. Die TISAX®-Plattform bietet Mitgliedern eine standardisierte Bewertung des Status ihrer Informationssicherheit, den sie mit ihren Partnern, entlang der gesamten Wertschöpfungskette teilen können. Ihre erreichte Schutzklasse wird auf einer speziell dafür vorgesehenen digitalen Plattform registriert und ausgewählten Mitgliedern, die Ihren TISAX®-Status beantragen, zur Verfügung gestellt. Zu den Partnern des TISAX® Assessments gehören:

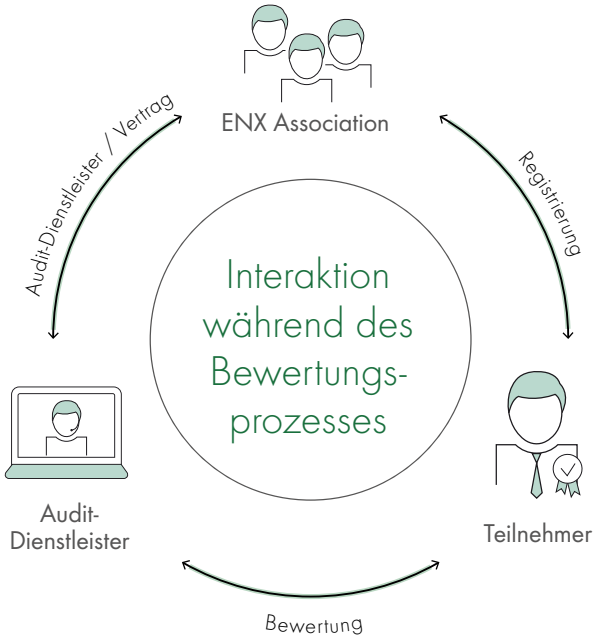
- die ENX Association
- ein autorisierter Audit-Dienstleister
- ein teilnehmendes Unternehmen, das die Zertifizierung beantragt

Die TISAX®-Zertifizierung ist für einen Zeitraum von drei Jahren gültig. Registrierte Partner geben vertrauliche Informationen weiter und können sich absolut sicher zu sein, dass andere mit diesen Informationen nach den etablierten TISAX®-Standards umgehen. Basierend auf den Bewertungsergebnissen wird der Status der Informationssicherheit jedes registrierten Teilnehmers auf der Online-Plattform zur Verfügung gestellt. Kein TISAX®-Mitglied hat automatisch Zugriff auf die Bewertungsergebnisse und den Status der anderen. Ausgewählte Partner mit denen Informationen geteilt werden, werden von jedem TISAX®-Teilnehmer auf Einzelfallbasis festgelegt.

TISAX®, VDA und ENX

Der Anfang 2017 eingerichtete Test- und Austauschmechanismus TISAX® basiert auf dem ISA (Information Security Assessment)-Anforderungskatalog des Verbandes der Automobilindustrie (VDA).

Im Jahr 2000 wurde die ENX Association gegründet und agiert als rechtlich unabhängiger Zusammenschluss von Unternehmen und nationalen Verbänden wie Audi, BMW, Bosch, Continental, Daimler, DGA, Ford, Magna, PSA Peugeot Citroën, Renault, Volkswagen ANFAC (Spanien), GALIA (Frankreich), SMMT (Großbritannien) und VDA



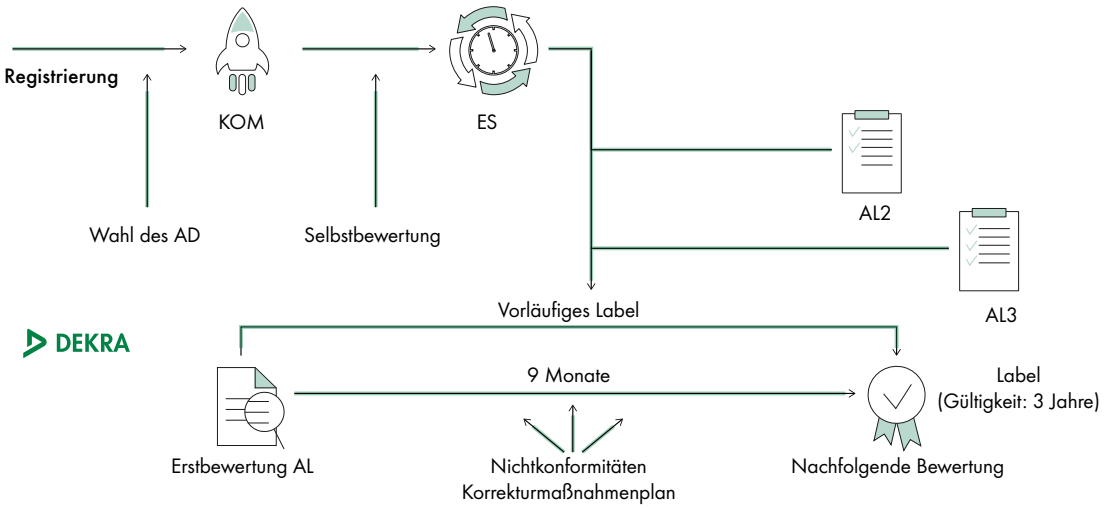
(Deutschland). Der VDA überwacht die Leistung der zertifizierten Dienstleister, betreibt zentrale ENX-Netzwerkdienste und unterstützt Anbieter mit effizienten Lösungen.

Im Kern zielt TISAX® auf die Etablierung einer standardisierten Kennzeichnung ab, die auf Kriterien der Automobilindustrie basiert. TISAX® wurde entwickelt, um eine Gemeinschaftsumgebung zu schaffen, in der die Leistung und Sicherheit von IT- und IS-Systemen geteilt werden kann.

Phasen der TISAX®-Zertifizierung

1. Registrierung auf der TISAX®-Plattform
2. Auswahl eines Audit-Dienstleisters
3. Vorläufige Verifizierung der Bewertung von Label/Umfang und Informationsschutzklasse und vereinfachte Gruppenbewertung (wenn möglich)
4. Ausführung und Unterzeichnung des Vertrags
5. Selbsteinschätzung (Assessment Level 1)
6. Off-Site-Audit (Überprüfung des Assessment Level 1 entsprechend der Dokumentation und Bestätigung von Label/Umfang oder Assessment Level 2) optional
7. Vor-Ort-Audit (Assessment Level 3)
8. Label-Validierung
9. Austausch von Audit-Informationen mit exklusiven TISAX®-Partnern, die von dem geprüften Mitgliedsunternehmen benannt wurden

Ablaufplan des TISAX® Assessments



KOM = Kick-off-meeting ES = Eröffnungssitzung AL = Assessment level AD = Audit-Dienstleister

Vorteile der TISAX®-Zertifizierung

Zusätzlich zum Mehrwert Ihres anerkannten Status der Informationssicherheit bietet Ihnen die TISAX®-Zertifizierung folgende Vorteile:

- Erhöhte Glaubwürdigkeit dank Ihres zertifizierten Informationssicherheitssystem
- Unternehmensübergreifende Anerkennung unter den TISAX®-Mitgliedern
- Gute Strategien für ein effektives Risikomanagement
- Transparenz durch den einheitlichen VDA-ISA-Katalog
- Stärkere Konzentration auf die Bedürfnisse und Erwartungen der Kunden
- International anerkannte Auflistung in der TISAX® Online-Plattform
- Vollständige Kontrolle darüber, wer auf Ihre Bewertungsergebnisse zugreifen kann
- TISAX® Assessment alle drei Jahre, wodurch Zeit und Geld für mehrfache Kontrollen entfallen

2. Rollen der Beteiligung

Mitgliedsorganisationen, die am Austauschmodell teilnehmen, können, je nach den besonderen Umständen, entweder eine passive oder eine aktive Rolle übernehmen:

Passiver Teilnehmer (z.B. OEM, Automobilhersteller): Er fordert, dass sich ein anderes Unternehmen, z.B. ein Lieferant, einer Bewertung unterzieht und bittet um Zugang zu den Bewertungsergebnissen.

Aktiver Teilnehmer (z.B. Lieferant): Er beauftragt entweder eine Bewertung oder wird von einem OEM oder Kunden zur Bewertung aufgefordert. Der aktive Teilnehmer gewährt dann ausgewählten Partnern Zugang zu den Bewertungsergebnissen.

Die drei Schritte der Teilnahme:

1. Anmeldung

Ihr ausgewählter TISAX®-Dienstleister sammelt Informationen über Ihr Unternehmen und legt den Umfang Ihrer Bewertung fest.

2. Bewertung

Die Bewertung wird von einem akkreditierten TISAX®-Auditanbieter durchgeführt.

3. Austausch

Die Bewertungsergebnisse und Zertifizierung(en) werden ausschließlich mit den benannten Partnern geteilt.

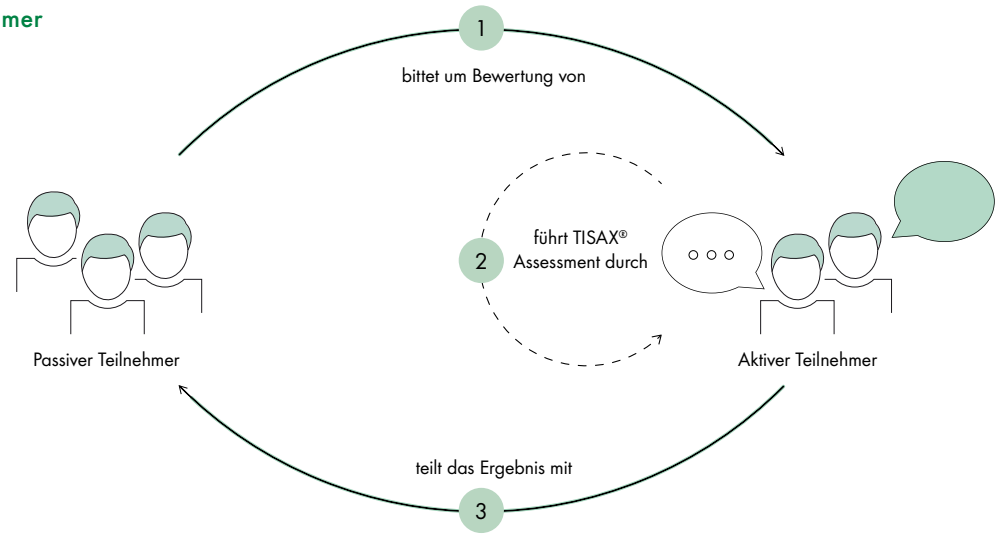
Schritt 1

Kunden können sich auf der TISAX®-Plattform registrieren und müssen einen bestimmten Prozess befolgen, um eine „Teilnehmernummer“ zu erhalten.

Während des Online-Registrierungsprozesses von TISAX® müssen die Kandidaten:

- Kontaktdaten und Rechnungsinformationen angeben,
- die TISAX®-Bedingungen akzeptieren und
- den Umfang der Informationssicherheitsbewertung definieren.

Rollen der Teilnehmer



Der Prüfungsumfang basiert auf dem VDA ISA-Katalog. Die Auditdauer wird entsprechend dem festgelegten Umfang berechnet und kann nicht allein aufgrund der Struktur der Organisation vorausberechnet werden.

Schritt 2

Die Bewertung ist in vier Teilschritte unterteilt:

- **Vorbereitung der Beurteilung**
  Der Umfang der Vorbereitung hängt vom aktuellen Reifegrad des Informationssicherheits-Managementsystems ab und muss sich an den Anforderungen des VDA ISA-Katalogs orientieren.
- **Auswahl des Audit-Dienstleisters**
  Die Teilnehmer wählen ihren bevorzugten Partner aus der Liste der akkreditierten TISAX®-Auditoren aus.
- **Bewertung(en) der Informationssicherheit**
  Der Audit-Dienstleister führt die Bewertung auf der Grundlage des Umfangs durch, der durch die Anforderungen des anfragenden Partners bestimmt wird. Jeder Beurteilungsprozess besteht mindestens aus einem ersten Audit, wobei für diejenigen, die nicht sofort bestehen, zusätzliche Maßnahmen erforderlich sind.
- **Gemeinsame Nutzung der Bewertungsergebnisse**
  Nach Abschluss eines erfolgreichen Audits werden der Bericht und die Ergebnisse mit Zustimmung des aktiven Teilnehmers weitergegeben.

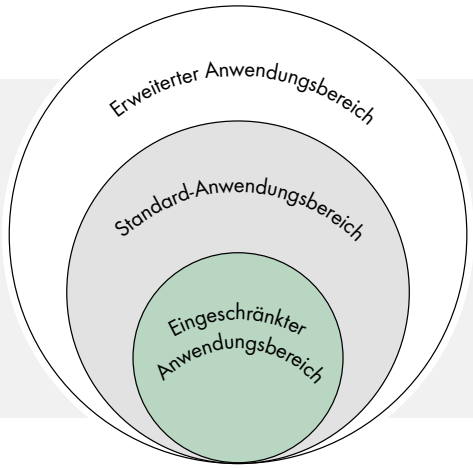
Schritt 3

Die Ergebnisse werden auf der TISAX®-Plattform eingegeben, um diese, je nach Bedarf, ausschließlich mit den benannten Partnern zu teilen. Der Inhalt Ihres TISAX®-Berichts ist in verschiedene Ebenen strukturiert. Nur Sie sind befugt, die Ebene zu bestimmen, auf die Ihr Partner Zugriff hat. Die Veröffentlichung der Ergebnisse und des Bewertungslabels auf der digitalen TISAX®-Plattform durch TISAX® und ENX macht Ihre Zertifizierung offiziell.

3. TISAX®-Bewertungsbereiche

Es stehen folgende Bewertungsbereiche zur Verfügung:

- **Standard-Umfang**
  In den meisten Fällen ist der Standardumfang so vordefiniert, dass er alle Ressourcen und Prozesse umfasst, die bei der Sammlung, Speicherung und Verwaltung digitaler Informationen verwendet werden.
- **Angepasster, erweiterter Umfang**
  Maßgeschneidert auf Ihre Bedürfnisse, über den Standardumfang hinaus.
- **Angepasster, eingeschränkter Umfang**
  Maßgeschneidert, um lediglich die spezifischen Bedürfnisse zu erfüllen (es kann kein Label ausgestellt werden).



VDA ISA Kriterienkatalog	Protection Level (PL)	TISAX® Bewertungsziel	Assessment Level
Informationssicherheit	hoch	Informationen mit hohem Schutzniveau	AL 2
	sehr hoch	Informationen mit sehr hohem Schutzniveau	AL 3
Verbindung zu Dritten	hoch	Verbindung zu Dritten mit hohem Schutzniveau	AL 2
	sehr hoch	Verbindung zu Dritten mit sehr hohem Schutzniveau	AL 3
Schutz von Prototypen		Handhabung von Prototypen mit hohem Schutzniveau (weitere Informationen siehe Kapitel 9)	AL 3
Datenschutz	hoch	Datenschutz nach §11 BDSG („Auftragsdatenverarbeitung")	AL 2
	sehr hoch	Datenschutz bei besonderen Arten von personenbezogenen Daten, Datenschutz nach §11 BDSG („Auftragsdatenverarbeitung"), besondere Arten nach §3 Abs. (9) BDSG („Besondere Arten")	AL 3

Die TISAX®-Zertifizierung endet mit einem erreichten Bewertungslabel, das das Bewertungsergebnis widerspiegelt. Es gibt vier verschiedene Label-Kategorien, die von verschiedenen Partnern verlangt werden können. Die zu Beginn des Prozesses definierten Bewertungsziele werden geprüft und nach erfolgreichem Abschluss des Audits dem entsprechenden Bewertungsniveau zugeordnet. Die Grade „hoch" oder „sehr hoch" definieren das erreichte Schutzniveau in jeder Kategorie.

Umfang und Dauer des TISAX® Assessments werden von Fall zu Fall entsprechend der Liste der zu erfüllenden Kriterien, der definierten Schutzziele, der Komplexität des ISMS und der Anzahl der betroffenen Standorte festgelegt.

4. Etablierte VDA ISA-Anforderungen

Die VDA ISA-Bewertung umfasst einen allgemeinen Fragebogen zur Informationssicherheit sowie drei zusätzliche spezifische Themenmodule:

- **Schutz von Prototypen:** Ursprünglich vom VDA PTS abgedeckt, wurde das Modul überarbeitet und folgt nun der gleichen Struktur wie der Hauptkatalog.
- **Verbindungen zu Dritten:** Das Modul beschreibt die spezifischen Anforderungen, die Anbieter und Dienstleister bei der Anmietung von Räumlichkeiten für den Betrieb von Partnernetzwerkverbindungen vor Ort berücksichtigen sollten.
- **Datenschutz:** Dieses Modul wird bei Dienstleistern angewendet, die gemäß Artikel 28 der Europäischen Allgemeinen Datenschutzverordnung (DSGVO) mit der Verarbeitung von Informationen beauftragt sind.

5. Registrierter TISAX®-Teilnehmer

Der Zugang zu TISAX® ist für registrierte Teilnehmer über das TISAX® Online-Portal möglich. Die Registrierung ist die Voraussetzung für die Auswahl eines akkreditierten TISAX®-Auditors aus der Liste der autorisierten Dienstleister. Eine einzelne Organisation kann mehrere Standorte registrieren und bei Bedarf eine Gruppenbewertung durchführen lassen. Nach einer Bewertung auf der Grundlage der VDA ISA-Anforderungen können aktive Teilnehmer Informationen zur Verfügung stellen, die sie mit ihren designierten TISAX®-Partnern teilen können.

TISAX® verwendet den vom Verband der Automobilindustrie (VDA) erstellten VDA-ISA-Fragebogen, der sich auf wesentliche Aspekte des international anerkannten Standards ISO/IEC 27001 für Informationssicherheitsmanagementsysteme (ISMS) stützt.

ENX überwacht die Einhaltung des TISAX®-Verfahrens, das spezifische Anforderungen an ENX TISAX®-Audit-Dienstleister enthält, um die Qualität der Implementierung und

der Bewertungsergebnisse zu gewährleisten. ENX schließt daher Verträge mit allen autorisierten Audit-Dienstleistern und registrierten Teilnehmern ab. Die TISAX®-Standardisierung und Qualitätskontrolle stellt sicher, dass Ihre Zertifizierung von den TISAX®-Mitgliedern in der gesamten Wertschöpfungskette der Automobilindustrie anerkannt wird.

6. ISO 27001 vs. TISAX®

Das TISAX® Assessment basiert auf dem Prüfkatalog des VDA Information Security Assessment (VDA ISA). Dieser basiert wiederum auf den Anforderungen der ISO/IEC 27001 bzw. der ISO/IEC 27002, die um automobilspezifische Anforderungen, wie z.B. den Prototypenschutz oder die Integration von Dritten oder den Datenschutz, erweitert wurden.

Ein Unternehmen, das das TISAX®-Verfahren erfolgreich durchlaufen hat, wird nicht automatisch nach ISO 27001 zertifiziert. Die Zertifizierung nach ISO 27001 muss separat durchgeführt werden.
Hier sind die wichtigsten Unterschiede:

7. Definierte TISAX® Schutz- und Bewertungsstufen

Als Betreiber des TISAX®-Programms hat die ENX Association klar definierte Schutz- und Bewertungsstufen. TISAX® unterscheidet dabei zwischen zwei Schutzstufen, mit deren Hilfe die angemessene Sicherheit für die Art der zu prüfenden Informationen definiert werden kann. Die Sicherheitsebenen umfassen:

- **Hoch:** Der potenzielle Schaden wäre erheblich, mittelfristig und nicht auf eine einzige Einheit beschränkt.
- **Sehr hoch:** Der potenzielle Schaden wäre existenzbedrohend, langfristig und nicht auf ein einzelnes Unternehmen beschränkt.

TISAX® unterscheidet auch zwischen drei Bewertungsstufen (Assessment Level, AL), die sowohl die Bewertungstiefe als auch die Methode für die drei Informationskategorien definieren:

- **Informationen mit normalem Schutzniveau:**
  Assessment Level 1 Selbstbewertung. Die Ergebnisse des Assessment Level 1 werden in TISAX® normalerweise nicht referenziert, können aber zur allgemeinen Verwendung angefordert werden.
- **Informationen mit hohem Schutzniveau:**
  Assessment Level 2 Audit, das von einem unabhängigen akkreditierten Dienstleister auf Grundlage der Selbstbewertung zusammen mit verschiedenen Dokumenten und einem Telefoninterview durchgeführt wird (ggf. ist eine Überprüfung vor Ort erforderlich).
- **Informationen mit sehr hohem Schutzniveau:**
  Assessment Level 3 Audit, das von einem unabhängigen akkreditierten Dienstleister auf der Grundlage der Dokumentation und einer Vor-Ort-Überprüfung durchgeführt wird.

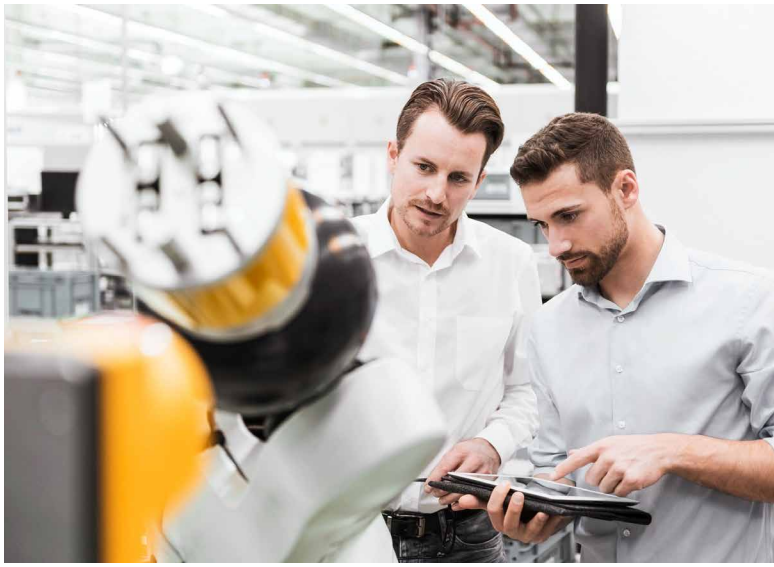
	ISO 27001:2013	TISAX®
Häufigkeit der Prüfung	Jährlich	Alle drei Jahre
Nachweis	Zertifikat	Elektronisches Label (nur in der ENX-Datenbank verfügbar)
Internationale Anerkennung	Ja	Zurzeit nur in der Automobilindustrie
Umgang mit Abweichungen	Größere Abweichungen müssen behoben werden, bevor das Zertifikat ausgestellt wird	Alle größeren und kleineren Abweichungen müssen vor der Ausgabe des Labels behoben werden

8. Prüfzeichen und Label

Eine angemessene Kennzeichnung entsprechend der Schutz- und Beurteilungsklassifikationsebene ist Voraussetzung für den richtigen Umgang mit Informationen. Neben dem Ersteller müssen sowohl die Empfänger als auch die Verarbeiter von Informationen die damit verbundenen Anforderungen an die Klassifizierungsstufe kennen, verstehen und bei der Handhabung anwenden.

Die Kennzeichnung ist besonders kritisch, wenn vertrauliche und streng vertrauliche Informationen über Unternehmensgrenzen hinweg übertragen werden.

Die Arbeitsgruppe Informationssicherheit fordert neben einer einheitlichen Informationsklassifizierung und einer entsprechenden Kennzeichnung der Dokumente auch eine einheitliche Kennzeichnung der IT-Anwendungen. Beim Öffnen digitaler Informationen wie E-Mails oder einer angehängten Datei kann ein farbiger Hinweis eine wichtige



Anzeigefunktion darstellen, um den Klassifizierungsgrad einer digitalen Information visuell zu signalisieren. Ein klarer Hinweis wie ein farbiger Balken kann das universelle Verständnis der Klassifizierungsebene unabhängig von sprachlichen Unterschieden unterstützen.

9. Bewertungsziele für den TISAX®-Prototypenschutz

Bewertungsziel	Informationen
Schutz von Prototypteilen und Komponenten	Gilt für Unternehmen, die als gefährdet eingestufte Fahrzeuge oder Komponenten in ihren eigenen Räumlichkeiten herstellen, lagern oder bereitstellen.
Schutz von Prototyp-Fahrzeugen	Gilt für Unternehmen, die Fahrzeuge, die von Kunden zur Verfügung gestellt werden und als schutzbedürftig eingestuft sind, in ihren eigenen Räumlichkeiten herstellen und lagern.
Handhabung von Testfahrzeugen und Komponenten	Gilt für Unternehmen, die Tests und Testfahrten mit vom Kunden zur Verfügung gestellten, als schutzbedürftig eingestuften Fahrzeugen durchführen.
Schutz von Prototypen während Veranstaltungen und Film- oder Fotoaufnahmen	Gilt für Unternehmen, die Präsentationen oder Veranstaltungen sowie Film- und Fotoaufnahmen mit vom Kunden zur Verfügung gestellten Fahrzeugen, Komponenten oder Teilen durchführen, die als schutzbedürftig eingestuft werden.

Benötigen Sie ein TISAX® Assessment für Ihr Unternehmen? Kontaktieren Sie jetzt unsere Experten!

Über DEKRA

Seit unserer Gründung vor über 90 Jahren bietet DEKRA Dienstleistungen zur Gewährleistung höchster Sicherheitsstandards an. Mit Leidenschaft, Fachwissen und 45.000 Mitarbeitern weltweit denken wir voraus, um die zukünftigen Herausforderungen im Bereich Sicherheit zu bewältigen. Wir fördern den Umgang des Menschen mit den Themen Technik und Umwelt und bemühen uns, den heutigen Sicherheitsanforderungen im Hinblick auf die Digitalisierung gerecht zu werden. Auf der Straße, am Arbeitsplatz und zu Hause - unsere kompetenten DEKRA Experten arbeiten für mehr Sicherheit in allen wichtigen Lebensbereichen.

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.de/de/audits/