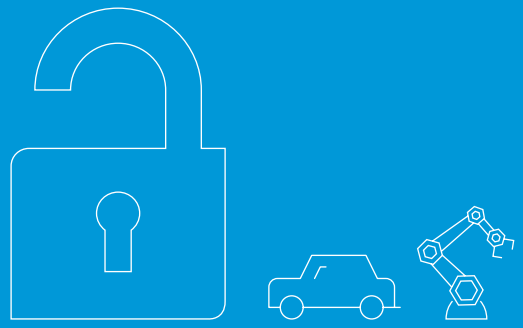
Informationssicherheit

TISAX-ZERTIFIZIERUNG? WIR MACHEN'S EINFACH.

DAS EINHEITLICHE NIVEAU FÜR IHRE INFORMATIONSSICHERHEIT

In Deutschland setzt die Automobilindustrie mit TISAX auf ein gemeinsames Prüf- und Austauschverfahren. Ziel ist es, ein einheitliches Niveau an Informationssicherheit zu schaffen. Um eine TISAX-Zertifizierung zu erhalten, müssen Unternehmen in den Bereichen Informationssicherheit, Prototypenschutz und Datenschutz mindestens den Reifegrad 3 erreichen. Wir unterstützen Unternehmen dabei, die Anforderungen des VDA Information Security Assessments (VDA ISA) zu verstehen, die notwendigen Maßnahmen erfolgreich umzusetzen und den Nachweis über die Sicherheit von Informationen zu erbringen.



Das gemeinsame Prüf- und Austauschverfahren für die Automobilindustrie TISAX (Trusted Information Security Assessment eXchange) basiert auf einem vom VDA (Verband Deutscher Automobilindustrie e.V.) entwickelten Fragebogen zur Informationssicherheit (ISA – Information Security Assessment).

Der Industriestandard richtet sich insbesondere an Unternehmen, die für eine Zusammenarbeit mit einem Automobilhersteller in Deutschland ein bestimmtes Sicherheitsniveau nachweisen wollen und müssen. Der nicht unerhebliche Aufwand zahlt sich jedoch aus: Die Bewertungsergebnisse sind bei allen TISAX-Teilnehmern unternehmensübergreifend anerkannt und unterstützen eine vertrauensvolle Partnerschaft.

Sie stehen ebenfalls vor der Herausforderung, die Zertifizierung erfüllen oder erneuern zu müssen? Wir stehen Ihnen gern zur Seite und unterstützen mit einem strukturierten Vorgehen.

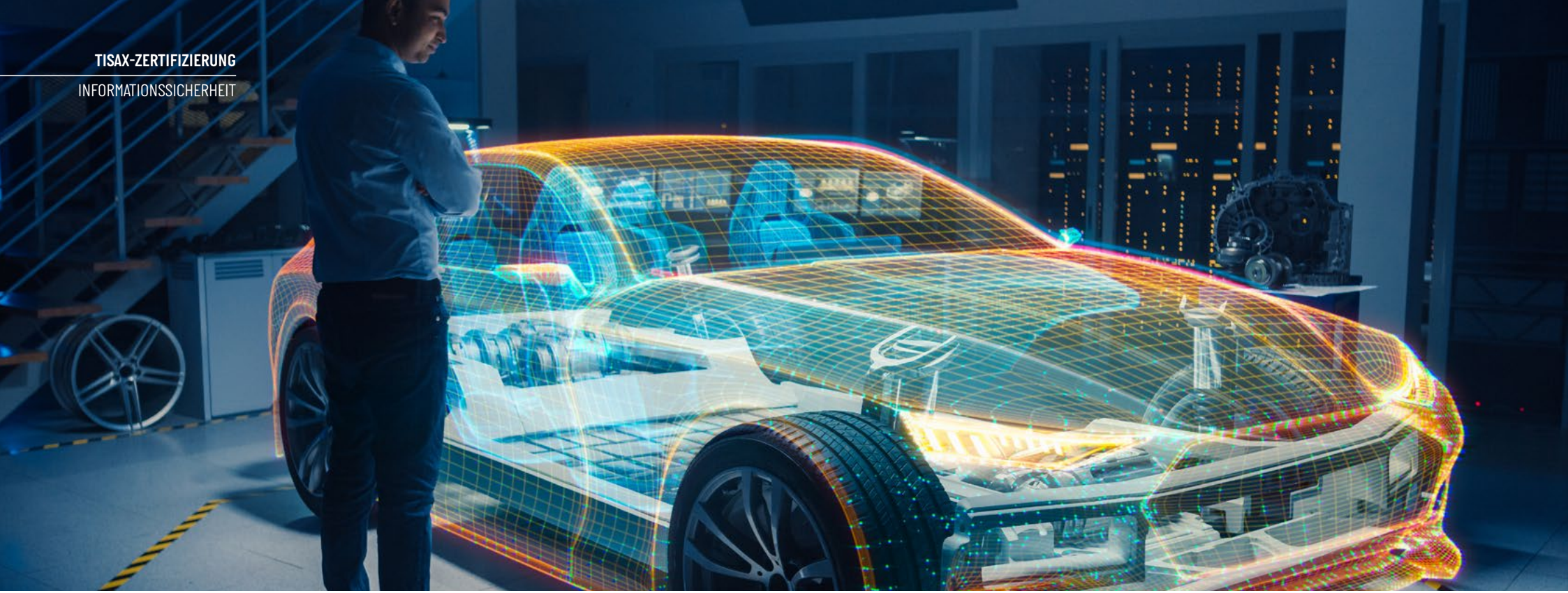
UMFASSENDER ALS ISO 27001

TISAX orientiert sich im Wesentlichen an der internationalen Norm für Informationssicherheit ISO 27001. Diese definiert Anforderungen, Regeln und Methoden, um die Sicherheit von Informationen zu gewährleisten. Der Prüfkatalog greift auf die in ISO 27001 festgelegten „Controls" (Maßnahmen) zurück. Sie beschreiben, wie sich die jeweiligen Anforderungen (muss, sollte) umsetzen lassen, wie Prozesse sicherzustellen sind und welche Hilfsmittel eingesetzt werden können.

Falls Sie bereits eine ISO-27001-Zerfizierung haben, ist dies jedoch keine Voraussetzung für das TISAX-Assessment. Dennoch: Sie ist immer von Vorteil, weil damit bereits belegt ist, dass bestimmte Sicherheitslevel eingehalten werden. Ist ISO 27001 umgesetzt, ist in der Regel bereits mindestens Reifegrad 1 oder 2 erfüllt. Ist bereits ein Information Security Management System (ISMS) implementiert, das alle Leitlinien sowie Richtlinien erfüllt und Verantwortlichkeiten klar zuordnet, bewegt sich der Reifegrad wahrscheinlich bereits in Richtung der Zielnorm 3.

TISAX ist speziell an die automobilspezifischen Belange angepasst und berücksichtigt auch den Prototypenschutz und den Datenschutz.

Der Prototypenschutz umfasst als schutzbedürftig klassifizierte Fahrzeuge, Komponenten und Bauteile, die der OEM noch nicht der Öffentlichkeit vorgestellt hat. Der Datenschutz basiert auf den Anforderungen der Datenschutz-Grundverordnung (DSGVO). Mit der Durchführung und Überwachung des TISAX-Verfahrens ist die ENX-Association betraut.



ISA – EIN SELF-ASSESSMENT

Basis für die TISAX-Zertifizierung ist das Information Security Assessment (ISA) Version 5.0, das kostenfrei auf der VDA-Webseite zum Download zur Verfügung steht. Das Excel-Dokument ist als Self-Assessment ausgelegt und besteht aus mehreren Tabellen. Dabei gibt es in den Modulen Informationssicherheit, Datenschutz und Prototypenschutz genaue Vorgaben, welche Anforderungen ein Unternehmen jeweils erreichen muss.

Die Umsetzung wird mittels eines 5-stufigen Reifegradmodells bewertet. Die Reifegrade (0 bis 5) gehen dabei von 0 = unvollständig über 1 = durchgeführt und 3 = etabliert bis hin zu 5 = optimierend. Der Zielreifegrad für alle Kontrollfragen liegt immer beim Reifegrad 3, also etabliert. Nur, wenn ein Unternehmen in allen Bereichen mindestens diesen Reifegrad erreicht, erhält es eine TISAX-Zertifizierung.

TISAX unterscheidet dabei drei Assessment-Level (Schutzbedarfe): normal (Level 1), hoch (Level 2) und sehr hoch (Level 3). Davon sind sowohl die Prüfmethode als auch der Prüfaufwand abhängig. Während Level 1 auf einer Selbsteinschätzung ohne Plausibilitätsprüfung beruht, wird die Selbsteinschätzung bei Level 2 durch einen Prüfdienstleister im Rahmen einer Plausibilitätsprüfung kontrolliert. Das erfolgt in der Regel durch eine Telefonkonferenz. Bei Level 3 findet eine Plausibilitätsprüfung der Selbsteinschätzung durch einen Prüfdienstleister vor Ort statt. Für die TISAX-Zertifizierung gilt immer Level 2 oder 3.

ZU WENIG RESSOURCEN UND ZU VIELE FRAGEZEICHEN?

Bis es soweit ist, müssen Unternehmen zunächst das gesamte Information Security Assessment durchlaufen und die dort gestellten Anforderungen erfüllen. Dazu sind eine Menge Ressourcen notwendig, die in vielen Unternehmen intern oftmals nicht verfügbar sind. Denn zum einen mangelt es an der Zeit, zum anderen an der Expertise, um die gestellten Anforderungen zu verstehen und diese auch entsprechend umzusetzen.

ZIELREIFEGRAD 3 = TISAX-ZERTIFIZIERUNG

INFORMATIONSSICHERHEIT
DATENSCHUTZ
PROTOTYPENSCHUTZ

ZIEL: Die geordnete Verarbeitung von Informationssicherheitsereignissen hat das Ziel, möglichen Schaden zu begrenzen und ein wiederholtes Eintreten zu verhindern.

REIFEGRAD 0

UNVOLLSTÄNDIG

Es gibt keinen Prozess oder der Prozess ist nicht geeignet.

REIFEGRAD 1

DURCHGEFÜHRT

Es gibt einen nicht oder unvollständig dokumentierten Prozess.

REIFEGRAD 2

GESTEUERT

Es gibt einen Prozess mit Prozessdokumentation und Prozessdurchführungsnachweisen.

REIFEGRAD 3

ETABLIERT

Es gibt einen integrierten Standardprozess. Es gibt Nachweise der Nutzung über einen längeren Zeitraum.

REIFEGRAD 4

VORHERSAGBAR

Es wird einem etablierten Prozess gefolgt. Kennzahlen werden kontinuierlich überwacht. Grenzwerte sind definiert.

REIFEGRAD 5

OPTIMIEREND

Es wird einem vorhersagbaren Prozess gefolgt. Kontinuierliche Verbesserung ist ein wesentliches Ziel.

DREI ASSESSMENT-LEVEL (SCHUTZBEDARFE):

normal (Level 1) = Selbsteinschätzung ohne Plausibilitätsprüfung
hoch (Level 2) = Plausibilitätsprüfung der Selbsteinschätzung durch einen Prüfdienstleister/Auditor in einer Telefonkonferenz
sehr hoch (Level 3) = Plausibilitätsprüfung der Selbsteinschätzung durch einen Prüfdienstleister/Auditor vor Ort

ANFORDERUNG TISAX-ZERTIFIZIERUNG

MIT PROFIS SCHRITT FÜR SCHRITT ZUR ZERTIFIZIERUNG

Computacenter unterstützt Unternehmen auf dem Weg zur TISAX-Zertifizierung. Denn wir sind in der Lage, ISA zu interpretieren und in die Sprache Ihres Unternehmens zu übersetzen. Darüber hinaus steuern wir den gesamten Prozess und führen alle Prozessschritte zusammen.

1. Zunächst werden Verantwortliche für die einzelnen Themen wie beispielsweise die Personalabteilung für das Thema Personal, die Rechtsabteilung für Compliance oder das Notfallmanagement für die Notfallvorsorge definiert. Darüber hinaus ist ein:e Informationssicherheitsbeauftragte:r oder ein Security Officer notwendig, der die übergreifende Steuerung übernimmt. Auch Abteilungsleiter:innen für IT-Betrieb, Service Management, Prozess-Change-Management oder Incident Management etc. müssen entsprechend ins Boot geholt werden.

2. Im nächsten Schritt gilt es, die Verantwortlichen abzuholen und ihnen genau zu erklären, was von ihnen erwartet wird. Hierbei unterstützen wir auch als „Übersetzer" und zeigen auf, was hinter einzelnen Anforderungen steckt.

3. Dann findet zunächst ein Ist-Abgleich statt. Dabei steht die Frage im Vordergrund, welche Sicherheitsmechanismen bereits vorhanden sind und ob dafür schon Nachweise existieren.

4. Anschließend wird ein Soll-Ist-Abgleich durchgeführt, der prüft, welche Diskrepanzen zwischen dem Ist und dem Soll sind. In diesem Schritt erfolgt die Reifegradanalyse, die als Soll den Reifegrad 3 vorgibt. Dabei ist der Schritt von einem Reifegrad zum nächsten von der kompletten Erfüllung des vorherigen Reifegrads abhängig. Erst wenn Reifegrad 1 vollständig abgedeckt ist, kann Reifegrad 2 angegangen werden. Es wird zudem festgelegt, welche Anforderungen noch zu erfüllen sind. Computacenter gibt hier Empfehlungen für Maßnahmen ab und belegt diese mit oder ohne Zeitangaben.

5. Danach ermitteln wir, welcher Aufwand und welche Kosten erforderlich sind, um die Anforderungen zu erfüllen. Sie können anschließend entscheiden, ob Sie diesen Weg für Ihr Unternehmen gehen möchten bzw. die Anforderungen erfüllen können.

6. Werden die empfohlenen Maßnahmen erfolgreich umgesetzt, haben Sie den notwendigen Reifegrad 3 erfüllt. Dabei ist es nicht nur notwendig, Maßnahmen umzusetzen, sondern diese auch aussagekräftig zu dokumentieren. Wir prüfen stets, ob der Nachweis ausreicht oder ob noch einmal nachgearbeitet werden muss.

Im letzten Schritt erfolgt die TISAX-Zertifizierung durch einen Auditor. Sie ist für zwei Jahre gültig, dann muss sie erneuert werden. TISAX ist in Unternehmen ein lebender Prozess, der kontinuierlich von einer Expertin oder einem Experten begleitet und weiterentwickelt wird.

Computacenter steht auch nach der Zertifizierung bei Fragestellungen als Berater weiterhin zur Verfügung.

1

STAKEHOLDER-ANALYSE UND VERANTWORTLICHKEITEN DEFINIEREN

Beispielsweise:

- Informationssicherheitsbeauftragte:r/ Security Officer
- Personalabteilung
- Rechtsabteilung
- Notfallmanager
- IT-Betrieb
- Service-Management
- Prozess-Change-Management
- Incident-Management

2

STAKEHOLDER AUF DEN PROZESS VORBEREITEN

Dienstleister kann als Übersetzer der Anforderungen in die verschiedenen Bereiche agieren.

3

IST-ANALYSE

- Welche Sicherheitsmechanismen sind bereits vorhanden?
- Existieren schon Nachweise?

4

SOLL-IST-ABGLEICH

- Lücken aufdecken
- Reifegradanalyse
- Maßnahmen zur Soll-Erfüllung für mindestens Reifegrad 3 festlegen

5

KOSTEN- & AUFWANDERMITTLUNG

- Entscheidung, ob Zertifizierung angestrebt werden soll

6

VORBEREITUNGEN ZUM AUDIT

- Notwendige Maßnahmen erfolgreich umsetzen
- Diese dokumentieren
- Dienstleister kann vorab Checks zur Validierung vornehmen

7

AUDIT UND ZERTIFIZIERUNG

LANGJÄHRIGE SECURITY-EXPERTISE

Computacenter hat als eines der ersten Unternehmen in Deutschland bereits im Februar 2006 die ISO-27001-Zertifizierung erlangt und besitzt langjährige Erfahrung in der Umsetzung und Beratung von ISO 27001. Darüber hinaus sind wir als Partner vieler Automobilhersteller selbst TISAX-zertifiziert und haben hier bereits Projekte erfolgreich umgesetzt und Unternehmen bei ihrem Zertifizierungsprozess unterstützt.

Wir setzen auf ein umfangreiches Information-Security-Portfolio und integrierte und ganzheitliche Lösungen. Das Angebot reicht dabei von der Beratung und Implementierung bis hin zur Beschaffung und dem Betrieb von Sicherheitslösungen. Über 20 Jahre Erfahrung und mehr als 160 Security-Spezialist:innen sowie zertifizierte Partnerschaften mit allen führenden Herstellern sind die Basis für eine erfolgreiche TISAX-Zertifizierung. Damit legen Unternehmen den Grundstein für eine vertrauensvolle Zusammenarbeit innerhalb der Automobilindustrie und ihrer Partner.

Sie möchten mehr erfahren? Sprechen Sie gern Ihr Account Management an oder kontaktieren Sie uns über www.computacenter.com/de

---

Unternehmensprofil

Computacenter ist der führende, unabhängige Anbieter von IT-Infrastrukturservices und -lösungen für Großunternehmen und große Organisationen des öffentlichen Sektors. Wir unterstützen unsere Kunden bei der Beschaffung, Transformation und Verwaltung ihrer IT-Infrastruktur und bei der Umsetzung ihrer digitalen Transformation.

Computacenter ist eine Aktiengesellschaft, die im Londoner FTSE 250 Index notiert ist und weltweit rund 17.000 Mitarbeiter:innen beschäftigt.

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen

computacenter.de
+49 (0)2273 5970