

### Vertraulichkeit – Integrität – Verfügbarkeit

Die Digitalisierung schreitet in verschiedenen Ausprägungen in jedem Bereich unaufhaltsam voran. Was bei all den verschiedenen Ausprägungen des Begriffes Digitalisierung den Konsens bildet, ist die Tatsache, dass eine zuvor nie gekannte Quantität und Qualität der Informationsverarbeitung existiert. Es stellt sich also die Frage, wie mit den veränderten Rahmenbedingungen, im Kern also der enormen Informationsflut, die sich aus der Digitalisierung ergibt, umzugehen ist. Dabei hat Informationssicherheit eine besondere Bedeutung.

Ein **Informationssicherheits-Managementsystem** bietet Ihrem Unternehmen die Möglichkeit eines systematischen Überblicks über die vorhandenen **Unternehmenswerte**, wie z.B. Hardware oder Software und veranschaulicht die **Chancen und Risiken**, die mit den Unternehmenswerten (sogenannten Assets) verbunden sind. Dabei spielen Kryptographie und die Verschlüsselung von Informationen ebenso eine Rolle, wie physische und umgebungsbezogene Sicherheit in Gebäuden und Räumen. Um vor potentiellen **Informationssicherheitsvorfällen** gewappnet zu sein, wird ein Notfallmanagement implementiert, aber auch die zweckmäßige Auswahl von Dienstleistern ist Bestandteil eines ISMS. Als wichtiger Teil der Informationssicherheit wird im **Datenschutz** ein besonderes Augenmerk auf **personenbezogene Daten** gelegt. Um Handlungssicherheit auch bei Ihren Mitarbeitern sicherzustellen, werden umfangreiche **Schulungen** angeboten. Durch regelmäßige **Audits** ist sichergestellt, dass sich das ISMS kontinuierlich verbessert.

Durch eine gelungene Umsetzung der verschiedenen Anforderungen bekannter Normen, wie die der **ISO 27001** oder **TISAX** präsentieren Sie gleichzeitig Vertrauenswürdigkeit nach außen zu Ihren Kunden.

## Informationen rund um das Thema

### Veranstaltungen & Schulungen der VIA Consult

finden Sie unter

[www.via-consult.de](http://www.via-consult.de)



### VIA Consult GmbH & Co. KG

Martinstraße 25  
57462 Olpe

Telefon: +49 2761-83668-0  
Telefax: +49 2761-83668-24  
info@via-consult.de

[www.via-consult.de](http://www.via-consult.de)

# Informationssicherheitsmanagement

TISAX



## Allgemeines

- TISAX (Trustes Information Security Assessment Exchange) wurde 2016 vom VDA Arbeitskreis Informationssicherheit gemeinsam mit der ENX Association entwickelt
- Basis sind internationale Managementsystemstandards, wie die ISO 27001
- Ganzheitlicher Ansatz – umfasst Aspekte der
  - Physischen Sicherheit
  - Organisatorischen Sicherheit
  - Technischen Sicherheit
- Ziele von TISAX sind
  - Wettbewerb zwischen Prüfdienstleistern schaffen
  - Ein gemeinsames Sicherheitsniveau in der Automobilindustrie etablieren
  - Allgemein anerkannte Prüfergebnisse schaffen
  - Kosten, Aufwände und Komplexität reduzieren



## Warum TISAX?

- Warum ein separater Standard für die Automobilindustrie?
- Der TISAX Standard Scope stellt sicher, dass alle für den Kunden relevanten Prozesse geprüft werden.
  - Transparente, vergleichbare und einfach interpretierbare Ergebnisse
  - Umgang mit Kundeninformationen ist im Mittelpunkt der Prüfung
  - Maßgeschneidert auf die Aufgaben, die am relevanten Standort durchgeführt werden
- Austausch von Prüfergebnissen durch standardisierte und zentrale Austauschprozesse
  - Einfach durch den Geprüften durch das ENX Portal zu steuern
  - Einfach auszuwerten – über Ergebnislisten oder über automatisierten Abgleich mit Lieferantenmanagementsystemen

## Aktuelle Zahlen

**1.800**  
TISAX Teilnehmer

**11**  
TISAX Prüfdienstleister

**61%**  
der registrierten Standorte haben weniger als 100 Mitarbeiter

**4.000**  
zu prüfende Standorte

**1.500**  
geprüfte Standorte

**33%**  
der registrierten Standorte sind ausserhalb Deutschlands

Information Security Assessment - Fragen		VDA	Verband der Automobilindustrie
based on ISO 27001:2013			
Firma:	0		
Ort:	0		
Datum:	00.01.1900		
Reifegrad Level 0-5:	na	Trifft eine Frage nicht zu, so ist na (not applicable) einzutragen.	
<b>1 General Aspects</b>			
<input type="checkbox"/>	1.1	Inwieweit ist ein Information Security Management System durch die Organisationsleitung freigegeben und sein Umfang dokumentiert? (Referenz zu ISO 27001: 4 und 5.1)	
Beschreibung d. Umsetzung:			
Referenz Dokumentation:			
Feststellungen:			
Maßnahmen:			
Ziel: Durch den Aufbau, Betrieb und die Weiterentwicklung eines Information Security Management Systems (ISMS) sowie der Benennung von Verantwortlichkeiten erfolgt eine systematische Steuerung und Kontrolle der Informationssicherheit innerhalb des festgelegten Anwendungsbereiches. Das ISMS definiert Prozesse und Verfahren, damit die Informationssicherheitsziele hinsichtlich einer angemessenen Vertraulichkeit, Verfügbarkeit und Integrität der Unternehmenswerte auf Basis der Sicherheitspolitik erreicht werden.			
Anforderungen: <u>Hierzu muss gehören:</u> <ul style="list-style-type: none"><li>+ Die Anforderungen der Organisation an ein ISMS sind ermittelt.</li><li>+ Ein durch die Organisationsleitung freigegebenes ISMS ist etabliert.</li><li>+ Der Geltungsbereich (Scope) des ISMS ist festgelegt (z. B. gesamte Organisation, Teilbereiche).</li><li>+ Eine Anwendbarkeitsklärung (Statement of Applicability, SoA) ist vorhanden (z. B. ausgefüllter VDA ISA Katalog).</li></ul> <u>Hierzu sollte gehören:</u> Keine. <u>Hierzu kann gehören:</u> <ul style="list-style-type: none"><li>+ Zertifizierung nach ISO 27001:2013 (inklusive Scope Statement und SoA).</li></ul> <u>Zusätzlich bei hohem Schutzbedarf:</u> Keine. <u>Zusätzlich bei sehr hohem Schutzbedarf:</u> Keine.			
<input type="checkbox"/>	1.2	Inwieweit ist ein Prozess zur Identifikation, Bewertung und Behandlung von Informationssicherheits-Risiken definiert, dokumentiert und umgesetzt? (Referenz zu ISO 27001: 8.2 und 6.1.2)	