TISAX Einführung -

Pragmatisch umsetzen

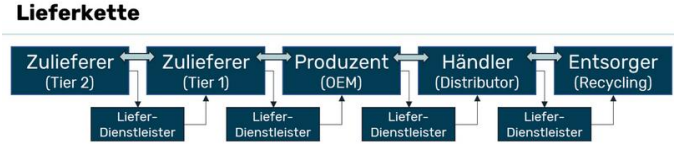
CONSUVATION
Beratung mit Kompetenz / Experts in Advice

TISAX Einführung –
pragmatisch umsetzen

01 Was ist TISAX?

02 Welche Anforderungen sind bei TISAX zu erfüllen?

03 Wie sieht unser Lösungsansatz aus, um TISAX pragmatisch umzusetzen?



Fokus ist der Schutz der Informationen über Prototypen in der Automobilbranche.

WAS IST TISAX?

TISAX heißt „**T**rusted **I**nformation **S**ecurity **A**ssessment **E**xchange“ und ist ein Standard im Bereich der Informationssicherheit in der Automobilbranche.

Der Standard wurde von dem Verband der Automobilindustrie (VDA) und seinen Mitgliedern entwickelt, um den Nachweis von vorhandener Informationssicherheit in der Lieferantenkette der Automobilhersteller (OEM) und deren Partnern zu optimieren.

Bisher wurden die Zulieferer von verschiedenen Auftraggebern oftmals mehrfach „auditiert“. Das war sehr aufwendig für beide Seiten. Aus diesem Grunde wurde TISAX als Prüfungsstandard und Austauschplattform für den positiven Nachweis der Informationssicherheit entwickelt.

Der Ansatz ist ganz einfach. Der Partner registriert sich auf der TISAX-Plattform und beauftragt eine zugelassene Prüfungsorganisation, sein TISAX System mittels eines Assessment zu prüfen. Bei Erfolg wird das Ergebnis als sogenannte „Labels“ auf der Plattform hinterlegt und die auditierte Unternehmung entscheidet, wer die Ergebnisse einsehen darf.

Es gibt verschiedene „Labels“, je nach dem geforderten Bereich und Sicherheitsanforderung.

Damit ist Transparenz für den OEM und den Partner geschaffen worden und es muss nur einmal ein Assessment durchgeführt werden.

Für die Zulieferer ist die Erfüllung von TISAX sehr wichtig, da es zukünftig eine Voraussetzung für die Zulassung für den Lieferantenstatus ist. Der Einkauf der OEM wird zukünftig nur noch Lieferanten mit TISAX Labels listen.

TISAX ist somit eine Prüfungsgrundlage und ein Verfahren zur Kommunikation der Assessmentergebnisse. Das Assessment wird auf Grundlage des VDA ISA Prüfungsvorlage durchgeführt.

WELCHE ANFORDERUNGEN SIND FÜR TISAX ZU ERFÜLLEN?

Die verwendete VDA ISA Prüfungsgrundlage umfasst folgende Teile:

- Informationssicherheitssystem
- Anbindung Dritter
- Datenschutz
- Prototypenschutz

Es müssen nicht alle Prüfungsteile erfüllt werden. Dabei kommt es an, was der OEM von seinem Partner für die eingekaufte Leistung fordert. Es kann sein, dass dann alle Prüfungsteile notwendig sind oder nur eine Auswahl davon. Je nachdem, welche Sicherheitsanforderungen formuliert wurden, kann sich auch der Umfang der geforderten Maßnahmen erhöhen.

INFORMATIONSSICHERHEITSSYSTEM

Der Prüfungsteil „Informationssicherheitssystem [ISMS]“ basiert auf dem internationalen Standard der ISO27001, ISO 27002 für Informationssicherheit und der ISO 27017 für die Anforderungen von Informationssicherheit in der Cloud.

Hier geht es darum ein Managementsystem für Informationssicherheit – ein ISMS - aufzubauen.

TISAX wird in der Zukunft die Grundlage für eine Lieferantenbeziehung in der Automobilbranche sein.

Bei dem Assessment der Prüfungsgesellschaft wird der Assessor prüfen, ob ein ISMS entwickelt, aufgebaut, installiert und kontinuierlich verbessert wird.

Was versteht man unter einem Managementsystem?

Ein Managementsystem ist die Art und Weise wie ein Unternehmen seine Strukturen und Prozesse organisiert, um systematisch ein geplantes Ziel zu erreichen. Hierfür werden Rollen und Verantwortlichkeiten benötigt – die Aufbauorganisation. Und für die Erreichung der Ziele der Informationssicherheit benötigt das Unternehmen Prozesse, die wiederum Dokumentationen erzeugen.

Die zugrundeliegenden ISO Normen formulieren hierfür Anforderungen an das Managementsystem bzw. deren Strukturen und Prozesse und auch Anforderungen an Maßnahmen für die Umsetzung der Informationssicherheit auf organisatorischer als auch technischer Ebene.

Zusammengefasst benötigt das Unternehmen ein ISMS mit definierter Aufbauorganisation (Organigramme, Politik und Regelungen) sowie der notwendigen Prozesse und Maßnahmen.

ANBINDUNG DRITTER

Bei dem Prüfungsbereich „Anbindung Dritter“ geht es darum, mit welchen Sicherheitsmaßnahmen gearbeitet wird, wenn der Partner z.B. im Netzwerk des OEM arbeite oder welche Regelungen und Maßnahmen er für seine internen und externen Mitarbeiter getroffen hat. Schwerpunkt hier sind:

- Verpflichtungen
- Zugangskontrolle
- Physische Sicherheit und
- Sicherheit der Kommunikation

Umgesetzt wird diese mit einer Teilmenge aus Maßnahmen aus dem ISMS.

DATENSCHUTZ

Der Datenschutz rückt dann in den Fokus, wenn der Partner Dienstleistungen erbringt, wo er personenbezogene Daten verarbeitet, zum Beispiel führt er Schulungen über Produkte des OEM durch und verarbeitet Teilnehmerdaten.

PROTOTYPENSCHUTZ

Bei dem Prüfungsgebiet des Prototypenschutzes geht es um den Schutz der Informationen der neuen Produkte des OEM. Dabei kann es sich darum drehen, dass Felgen eines neuen Fahrzeugs nicht vor dessen Markteinführung bekannt werden.

Schwerpunkte des Prototypenschutzes sind dabei:

- Organisatorische Regelungen
- Physischer Sicherheit
- Umgang mit Prototypen

Dieser Bereich ist für Unternehmen unterschiedlicher Branchen in der Partnerrolle zutreffend.

Es können Unternehmen sein, die den Prototypen bei sich auf dem Betriebsgelände haben oder auch Agenturen, die Medien über neue Fahrzeugmodelle erstellen oder Events dafür vorbereiten und durchführen.

Wie man erkennen kann, gehen die Anforderungen der OEM über die der klassischen ISO27001 Norm für Informationssicherheit hinaus. Deshalb wurde das Verfahren TISAX mit Nutzung des VDA ISA Prüfungsbogen entwickelt und jetzt eingesetzt.

Ist das Label erreicht, gilt es 3 Jahre lang. Dann muss das TISAX Verfahren neu gestartet werden.

WAS HABEN WIR ENTWICKELT, UM TISAX PRAGMATISCH UMZUSETZEN?

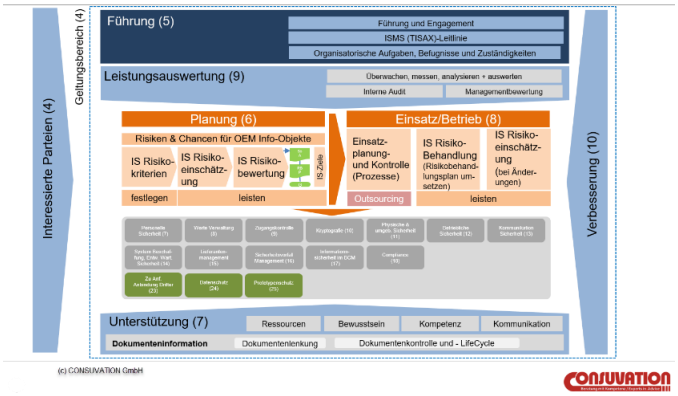
Unsere TISAX LÖSUNG besteht aus drei Säulen

Für das Assessment **muss** ein Unternehmen darlegen können, wie es systematisch die Anforderungen für TISAX bzw. die VDA ISA Prüfungsanforderungen erfüllt.

Dazu gehört auf **JEDEN FALL** ein nachgewiesenes **ISMS**.

Hierfür hat CONSUVATION ein Managementmodell für TISAX entwickelt.

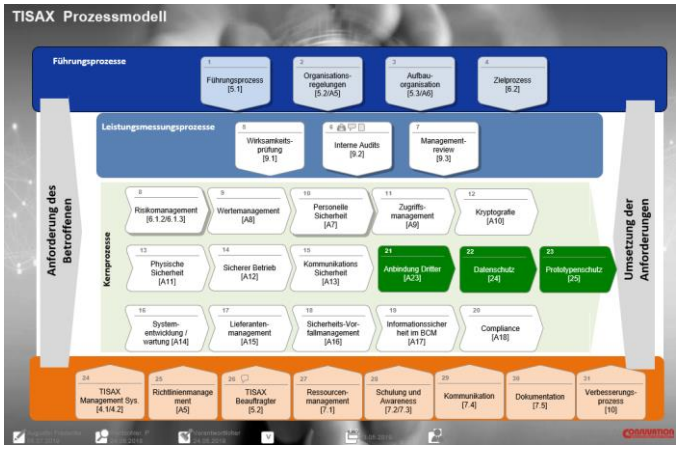
TISAX-Modell nach VDA ISA
(auf Basis der ISO 27001 und ISO 27017)



Dieses TISAX-Modell benötigt die Umsetzung der Aufbau- und Ablauforganisation und weiteren Anforderungen.

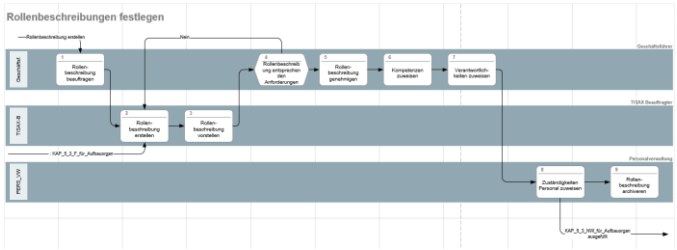
PROZESSMODELL [1]

Hierfür haben wir ein Prozessmodell entwickelt, welches ein ISMS auf Basis der Anforderungen von TISAX [VDA ISA] abbildet



Damit werden alle Prozesse, Verantwortlichkeiten, Regelungen etc. dargestellt.

Das Prozessmodell bildet in der ersten Ebene die Hauptprozesse ab. In den darunterliegenden Prozessebenen werden die konkreten Prozesse für das ISMS abgebildet



Damit werden alle Prozesse, Verantwortlichkeiten, Regelungen etc. dargestellt.

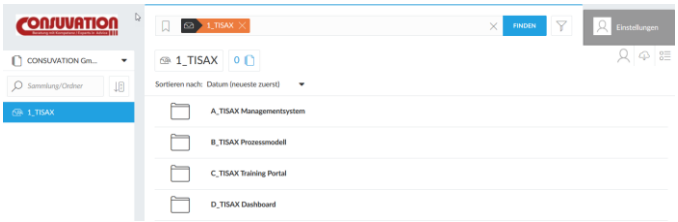
An die Dokumente werden im ISMS Anforderungen gestellt, man nennt diese Dokumentenlenkung. Es geht z.B. darum,

- Wer ist für welches Dokument zuständig?
- Wer hat welche Dokumente erstellt, geprüft und freigegeben?
- Welche Dokumente gelten im Augenblick?
- Welche Regelungen sind in Kraft gesetzt worden und von wem?

TISAX Portal [2]

Um all diese Anforderungen zu erfüllen, haben wir ein TISAX Portal entwickelt, in welchem das ISMS beschrieben ist und alle dazugehörigen Dokumente nachweislich gelenkt sind.

Damit wird die Zuständigkeit für Dokumente und die Dokumentenverwaltung abgebildet.



TISAX Schulungsportal [3]

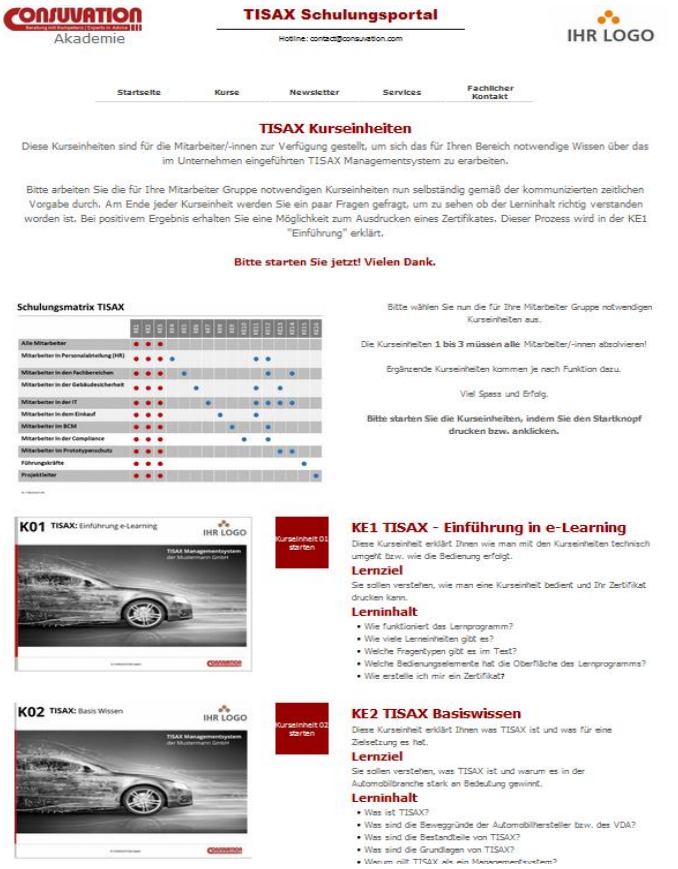
Unsere **dritte Säule** ist die Schulung und Bewusstseinsbildung für Informationssicherheit für Mitarbeiter.

In verschiedenen Stellen des VDA ISA Prüfkatalog wird die Schulung für Mitarbeiter des Unternehmens in unterschiedlichen Themengebieten gefordert. Sei es eine

Schulung über allgemeine Bedrohungen im Umgang mit Informationen, über das ISMS oder über die Anweisungen im Prototypenschutz. Dabei genügt es nicht, nur Schulungen durchzuführen, sondern es muss auch die Wirksamkeit und die Durchführung nachgewiesen werden.

Hierfür haben wir ein Schulungsprotal für TISAX entwickelt.

Darin werden alle notwendigen Kurse als e-Learning Einheiten zur Verfügung gestellt. Bearbeitet ein Mitarbeiter einen Kurs, dann muss er am Ende ein paar Fragen zum Inhalt beantworten.



Bei Erfolg erhält er ein Zertifikat, das in seiner Personalakte abgelegt wird. Mit diesen Werkzeugen kann man TISAX pragmatisch und schneller umsetzen.

Natürlich kann man die Lösung nicht 1:1 auf das eigene Unternehmen übertragen, denn man hat eine eigene Aufbauorganisation und Prozesse. Dies muss natürlich angepasst werden.

Aber es existiert auf jeden Fall eine „Blaupause“ mit der man sofort starten kann.

Wie gehen wir vor?

Zu aller erst ist es wichtig, was der Kunde für eine Größe und Wünsche zur Umsetzung hat.

Lösungspaket 1: Kleine TISAX Lösung

Bei kleinen Unternehmen bieten wir eine kleine Lösung an, indem wir unser Portal mit den notwendigen Dokumenten zur Verfügung stellen und der Geschäftsführer die Dokumente selbst füllen kann. Wir übernehmen hier nur noch eine Funktion der „Qualitätskontrolle“ und „Coach“. Das Portal nimmt dem Kunden die Entwicklung, Erstellung und Verwaltung der Dokumente ab. Er lädt die Dokumente herunter und nach erfolgter Bearbeitung schiebt er das gültige Dokument zurück ins Portal.

Lösungspaket 2: Mittlere TISAX Lösung

Ist das Unternehmen größer und komplexer, empfehlen wir die Durchführung mittels eines Projektes. Am besten startet man mit einer GAP-Analyse. Dann weiß man wo das Unternehmen steht und wie hoch die Aufwände sein werden.

Im Projekt bringen wir unseren Werkzeugkoffer mit und stellen unser „Know How“ zur Verfügung.

Dazu gehört auch ein entsprechendes Muster eines Projektplanes mit den notwendigen Aktivitäten. In der Projektarbeit passen wir zusammen

- das Prozessmodell
- die Dokumente
- die Kurse

an den Kunden an und schulen alles mittels dem Schulungsportal.

Somit hat unser Kunde zu Beginn einen roten Faden, was zu tun ist und danach ein fertiges System.

Das passiert pragmatisch und schneller, als wenn man alles selbst entwickeln muss.

Lösungspaket 3: Große TISAX Lösung

Bei großen und sehr komplexen Kunden, welche ihre eigene Systemlandschaft haben, bauen wir mit unserem „Know How“ zusammen eine Lösung auf Basis unserer Produkte in deren Welt auf.

Dabei unterstützen wir das Projektmanagement, arbeiten als Berater und operative Umsetzer.

Lösungspaket 4: Übernahme Beauftragter

Verfügt das Unternehmen nicht über das „Know How“ oder die Kapazitäten für die Pflege und Weiterentwicklung des TISAX Modells, übernehmen wir dies für unseren Kunden – ebenso, wie die IS-Beauftragen Rolle.

Lösungspaket 5: Teil-Übernahme von Prozessen

Es ist auch möglich, einzelne Prozesse zur Durchführung an uns zu übergeben, wie z. B. das notwendige interne Audit etc.

Lösungspaket 6: Unser 3 Säulen TISAX Portal

Unser Portal bieten wir unseren Kunden gegen eine monatliche Nutzungsgebühr an. Diese variiert je nach Größe und Mitarbeiterzahl des Kunden. Gerne unterbreiten wir hierfür ein Angebot für Sie.

Haben wir Ihr Interesse geweckt?

Wollen Sie einen schnelleren und sicheren Weg zu TISAX gehen, dann nehmen Sie Kontakt mit uns auf. Wir freuen uns über Ihre Email oder Anruf.

CONSUVATION GmbH beschäftigt sich seit **über 20 Jahren** mit Managementsystemen. ITIL, COBIT, ISO27001, ISMS, Risikomanagement, BCM und Datenschutz gehören zu unseren Kernkompetenzen.

Wir verfügen neben dem TISAX-Modell auch über ähnliche Modelle für:

- den Datenschutz
- das klassische ISMS nach ISO 27001
- Risikomanagement
- Business Continuity Management
- Compliance Management
- IT Governance Management

Wir sind für Sie da – sprechen sie uns bitte an.

CONSUVATION
Beratung mit Kompetenz / Experts in Advice