T.I.S.P./T.P.S.S.E. Community Meeting 2025

Berlin, 04. - 05.11.2025

TISAX® - Informationssicherheit in der Automobilindustrie

Bernd Schart, operational services GmbH & Co. KG

operational services GmbH & Co. KG

ICT „Made in Germany“

Full Service ICT Provider
10 Standorte in Deutschland
Zentrale in Frankfurt am Main

Kompetenzen für den Mittelstand

Infrastructure & Cloud
Digitization & Data
Transformation & Change Management
Security
Special Solutions

Partnernetz & Zertifizierungen

Microsoft Solution Partner
ServiceNow Worldwide Partner
Atlassian Gold Partner
SAP Advanced, IBM etc.
ISO 9001/27001
TISAX®

Hochsichere Data Center FFM & MUC

24/7 Operations Center (OPC)
Network Operations Center (NOC)
Service Desk
Private Cloud Automation
SDDC

Organisation

100% Tochter der T-Systems

Fachteam Audit-Services

Zugelassener TISAX® Prüfdienstleister
20 Auditoren mit spezifischem Automotive-Fachwissen
Mehr als 15 Jahre Auditerfahrung mit VDA ISA
Über 3.000 TISAX® Assessments weltweit
Ca. 450 Assessments jährlich

Inhalt

1 Sicherer Datenaustausch in der Automobilbranche durch TISAX®

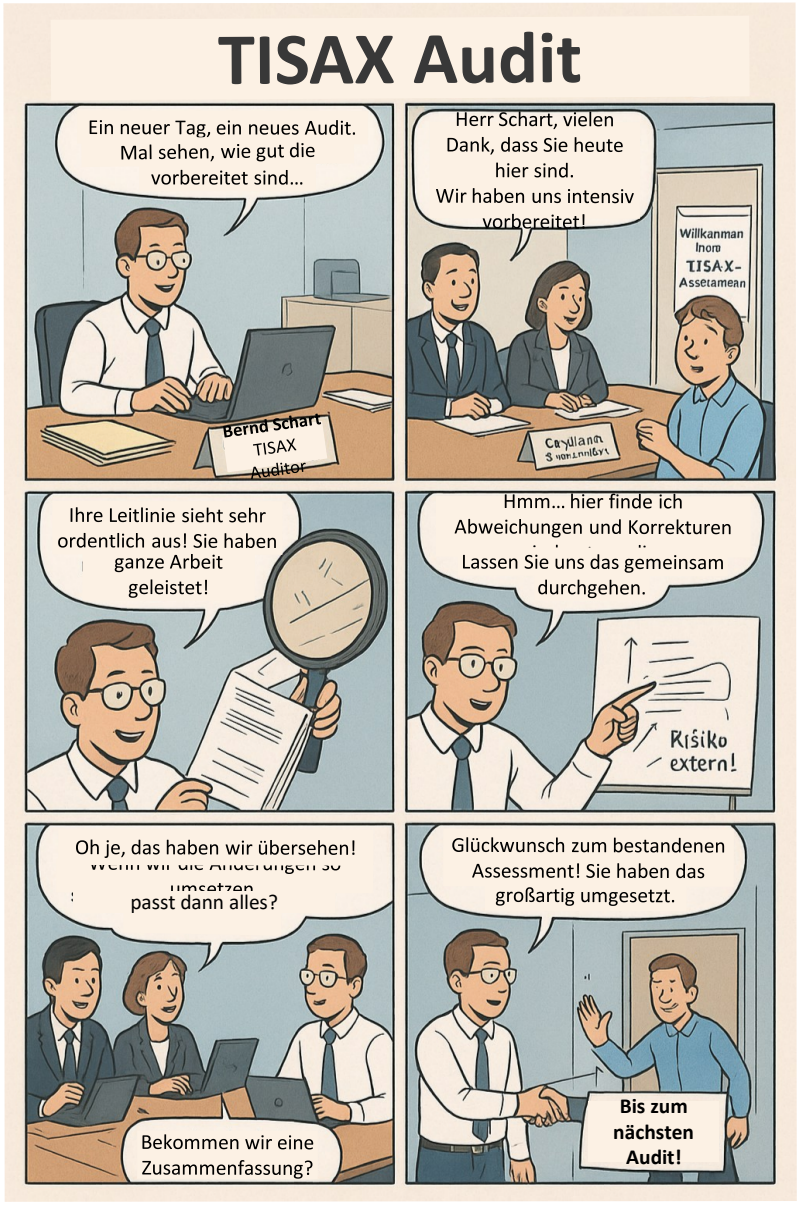
2 Zahlen – Daten - Fakten

3 TISAX® vs. ISO 27001

4 Herausforderungen für Auditee und Auditoren

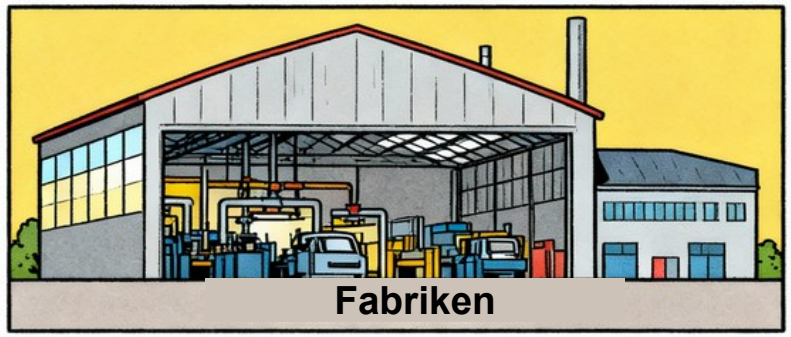
5 Sicherheit in der Praxis

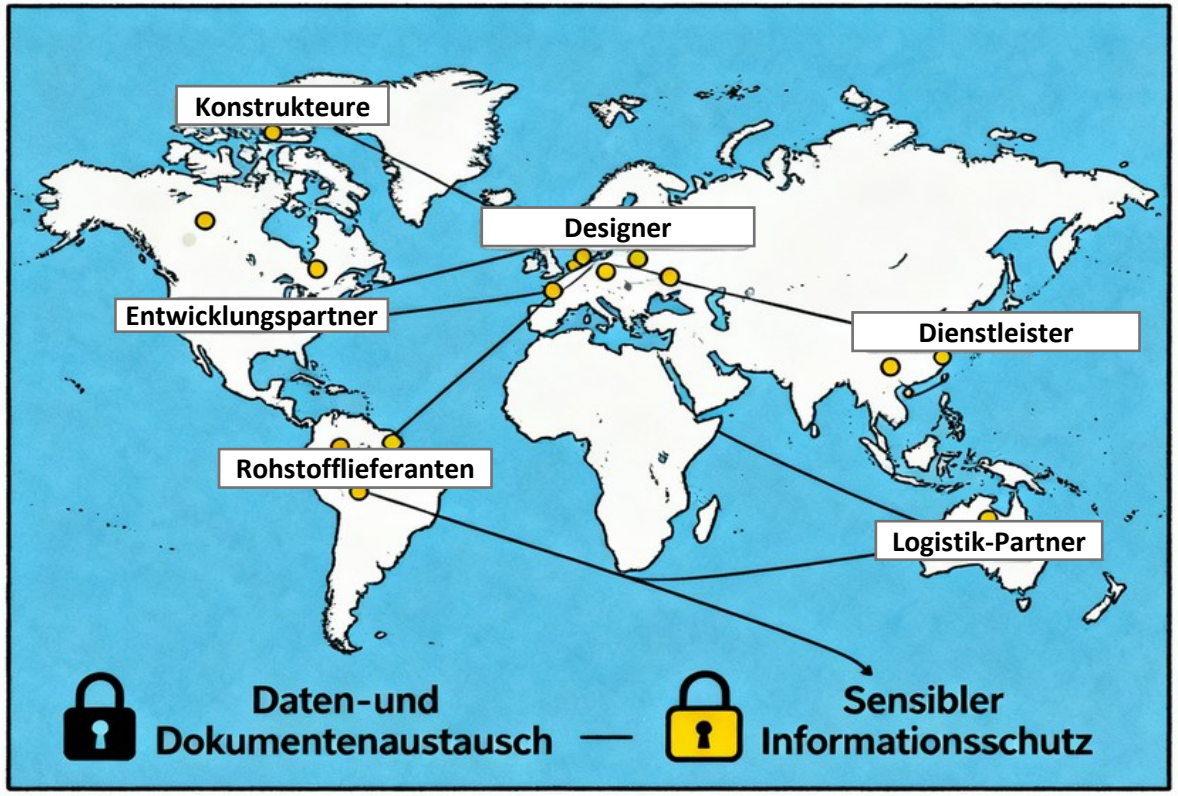
Mein Tag


TISAX Audit
Ein neuer Tag, ein neues Audit. Mal sehen, wie gut die vorbereitet sind...
Bernd Schart TISAX Auditor
Herr Schart, vielen Dank, dass Sie heute hier sind. Wir haben uns intensiv vorbereitet!
Willkanman Inorn TISAX-Assetamean
Ihre Leitlinie sieht sehr ordentlich aus! Sie haben ganze Arbeit geleistet!
Hmm... hier finde ich Abweichungen und Korrekturen
Lassen Sie uns das gemeinsam durchgehen.
Risiko extern!
Oh je, das haben wir übersehen!
passt dann alles?
Bekommen wir eine Zusammenfassung?
Glückwunsch zum bestandenen Assessment! Sie haben das großartig umgesetzt.
Bis zum nächsten Audit!


NORDATLANTIK
SÜDPAZIFIK
SÜDATLANTIK
INDISCHER OZEAN
SÜDLICHER OZEAN
EUROPA

Fahrzeugentwicklung, -Produktion, -Vertrieb





Wer bestimmt, was „Sicher“ bedeutet?

Herausforderungen

Branchenunabhängige Standards (ISO 27001/, IEC 62434, Prototypen, DSG-VO, Lieferketten…) decken den Schutzbedarf beim Umgang mit Informationen nicht ausreichend vollständig ab.

Anforderungen

Weltweit für die Automobilindustrie einsetzbarer Standardfragebogen, gewährleistet ein einheitliches Niveau der Informationssicherheit.

TISAX®

Branchenspezifisches und etabliertes unternehmensübergreifendes Prüf- und Austauschverfahren unter Governance der ENX Association.

Prüfergebnisse

Transparenz und Vertrauen in der Lieferkette durch gegenseitig anerkannte Assessments (ähnlich einer Zertifizierung).

TISAX® in Zahlen – Daten - Fakten

Stand 08/2025

+500

neu bewertete Standorte pro Monat

18

Zurzeit durch die ENX zugelassene TISAX® Prüfdienstleister weltweit

50%

der Standorte haben weniger als 100 Mitarbeiter

Mehr als 5.000

kritische Risiken wurden im Rahmen der TISAX® Assessments identifiziert

> 60.000

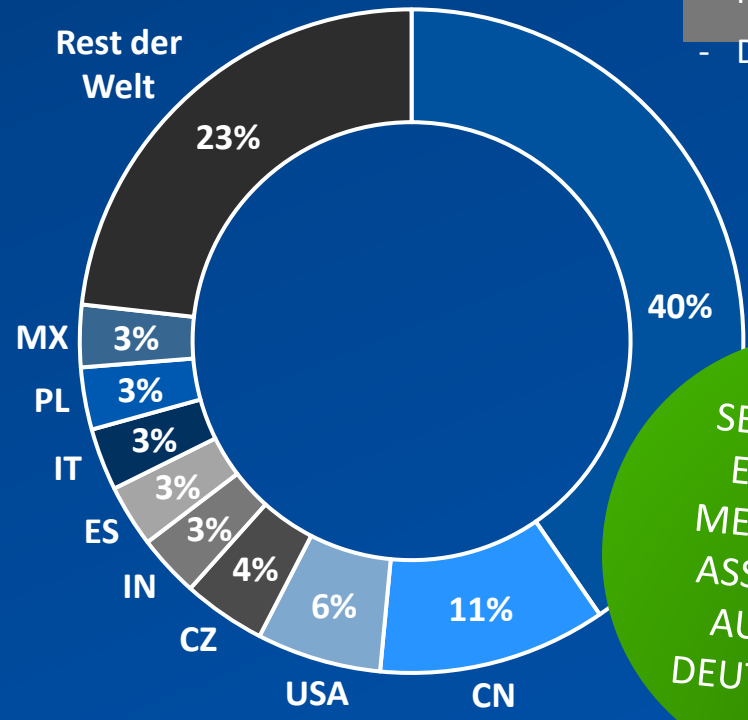
Verbesserungen der Informationssicherheit wurden seit 2018 gefunden

IN DEUTSCHLAND MEHR TISAX® LABEL ALS ISO 27001 ZERTIFIKATE

Über 17.500

Standorte in 90 Ländern haben ein gültiges TISAX® Label

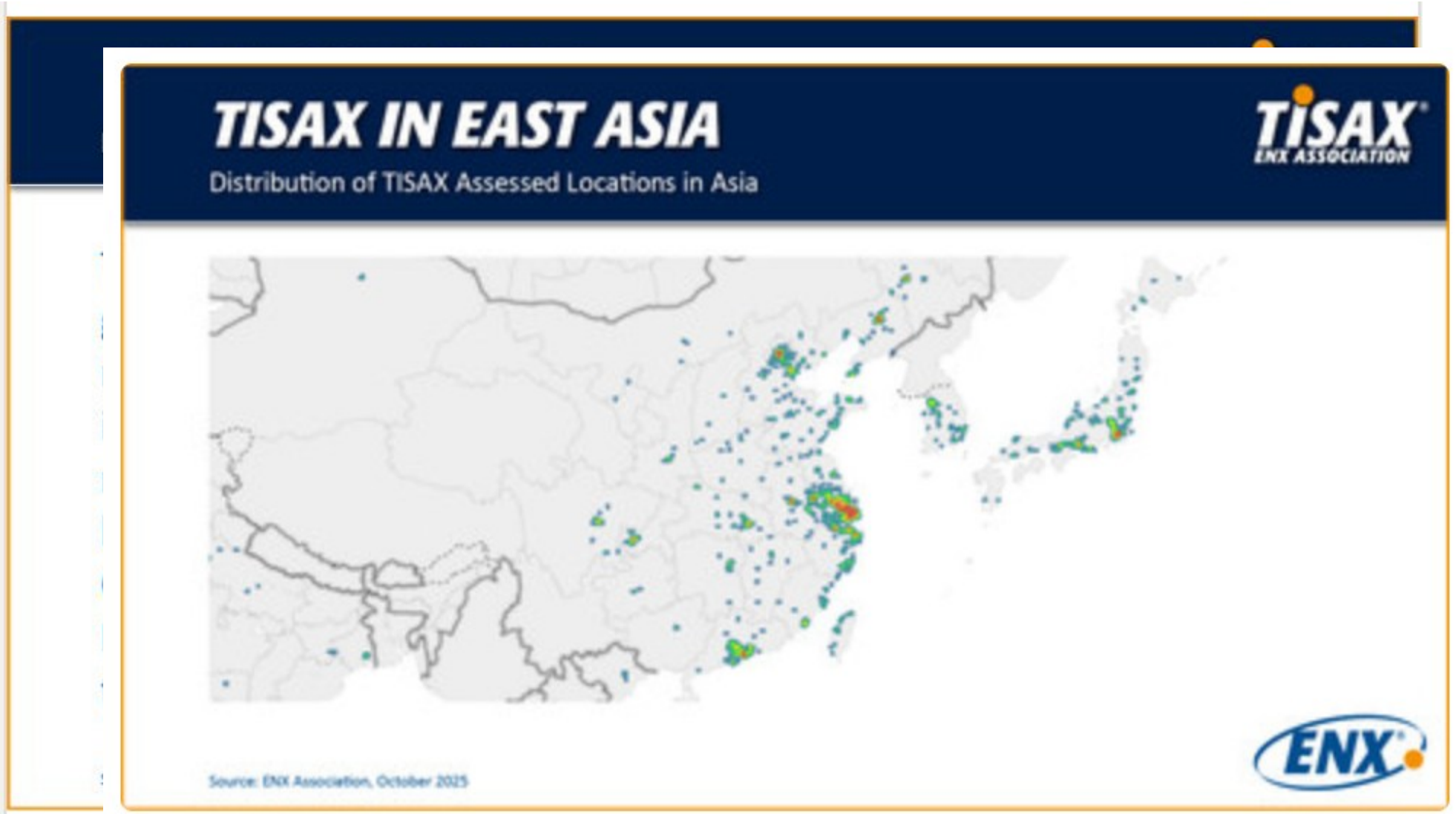
- Traditionelle Lieferanten
- Cloud, Mobility, IT
- Marketing
- Marktforschung
- Doku & Übersetzung



SEIT 06/2023: ERSTMALIG MEHR ALS 50% ASSESSMENTS AUßERHALB DEUTSCHLANDS

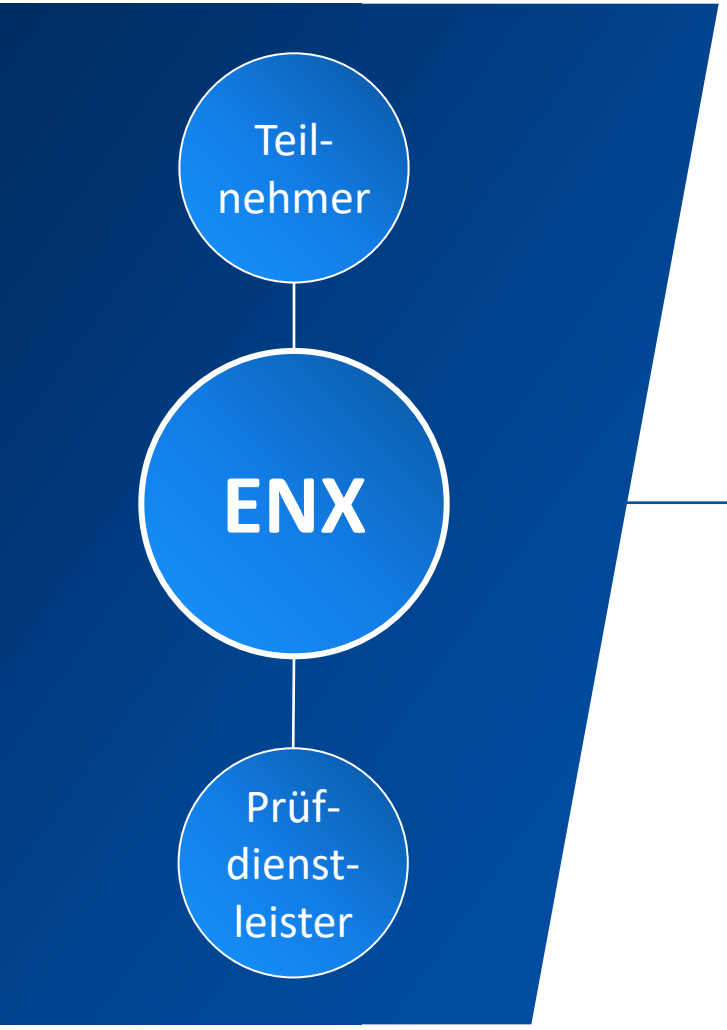
TISAX® in Zahlen – Daten - Fakten

Quelle: LinkedIn - ENX Association



Die Rolle der ENX Association

Governance Organisation, zentraler Koordinator und Qualitätssicherer im TISAX® Bewertungsprozess



- Betreiber des "**T**rusted **I**nformation **S**ecurity **A**ssessment E**x**change"
- Bereitstellung TISAX® Online-Plattform für Auditees und Prüfdienstleister
- Definition & Pflege der Anforderungen und Kriterien für Prüfdienstleister
- Zulassung und Kontrolle von Prüfdienstleistern
- Qualitätssicherung von Prozessen und Verwaltung von Prüfergebnissen
- Rechtliche Absicherung

TISAX® vs. ISO 27001 – Synergien und Differenzen

	ISO 27001	TISAX®
ZIELSETZUNG	Branchenspezifische Informationssicherheit für spezielle Bereiche + Best Practices (Updates alle 5 Jahre)	Branchenspezifische Informationssicherheit für die Automobilindustrie (Updates alle 3 Jahre)
GRUNDLAGE	ISO/IEC 27001 & 27002	VDA Information Security Assessment (ISA)
ANWENDUNGSBEREICH	Universell – unabhängig von Branche, Größe, Region	Automobilbranche (OEMs, Zulieferer, Entwicklungs- & Logistikpartner, …)
PRÜFERGEBNIS	ISO-Zertifikat (öffentlich, weltweit gültig)	TISAX® Label (nicht öffentlich, Austausch nur über TISAX® Plattform)
PRÜFSTELLEN	Akkreditierte Zertifizierungsstellen	Zugelassene Prüfdienstleister
GÜLTIGKEIT	3 Jahre (mit jährlichen externen Überwachungsaudits)	3 Jahre (mit jährlichen internen Überwachungsaudits)
FOKUS	ISMS-Prozesse, Informationsschutz, Risikomanagement	ISMS-Prozesse, Informationsschutz, Risikomanagement, spezifische physische Sicherheit, IT & OT, Lieferkette, Prototypenschutz, erweiterter Datenschutz
FLEXIBILITÄT	Umsetzungsfreiheit, solange Risiken behandelt sind	Fester Anforderungskatalog, nur geringer Interpretationsspielraum im Kontext der Organisation
PRÜFDAUER	Je nach Umfang, Branche, Unternehmensgröße, Region	1 bis 3 Tage

VDA Information Security Assessment

Bewertungsbereiche der aktuellen Version 6

Policies and Organisation

- Richtlinien
- Organisation
- Assetmanagement
- Risikomanagement
- Vorfall- und Krisenmanagement
- Wirksamkeitsprüfungen

1

Human Resources

- Sensible Stellen
- Verpflichtung und NDA
- Training
- Mobiles Arbeiten

2

Physical Security

- Sicherheitszonen
- Handhabung von Informationsträgern, mobilen IT-Geräten und Datenträgern

3

Identity & Access Mgmt.

- Identifikationsmittel
- Authentisierung
- Autorisierung/ Zugriffsverwaltung

4

IT Security / Cyber Security

- Kryptografie
- Betrieb
- Systemanschaffung, Anforderungsmanagement und Entwicklung

5

Supplier Relationships

- Informationssicherheit bei Auftragnehmern und Kooperations-partnern
- Geheimhaltungs-management

6

Compliance

- Regulatorische, gesetzliche und vertragliche Bestimmungen
- Datenschutz

7

Prototypen-schutz

- Umgebungsspezifische Sicherheit
- Umgang mit Fahrzeugen
- Versuchsfahrzeuge
- Veranstaltungen und Shootings

8

Datenschutz

- Policies, Organisation, Verarbeitungsverzeichnisse, TOMs, DS-Folgeab-schätzung, Datenüber-mittlung, Vorfälle, Weisungen

9

Spezielle Herausforderungen

… für Teilnehmer und Auditee

ISO 27001 (ca. 90%) mit spezifischen Ergänzungen wie u.a.

ISO 62434 (OT) und Prototypenschutz sowie erweiterte

Datenschutzanforderungen für Lieferanten

Hohe „Dokumentenlast“, besonders für KMUs

Budget für Nachbesserungen muss eingeplant werden

Frist für Nachbesserungen innerhalb 9 Monate

setzt Unternehmen zusätzlich unter Druck

Zeitrahmen für Vorbereitung rund 6-12 Monate

Berücksichtigung regelmäßiger Updates der ISA-Anforderungen bei Re-Assessments

Spezielle Herausforderungen

… für Prüfdienstleister und Auditoren

Auditoren benötigen

- ein sehr umfangreiches Wissen / Erfahrungen in diversen Disziplinen
- die ständige Aufrechterhaltung einschlägiger Zertifikate
- hohe Reisebereitschaft und Belastungsfähigkeit
- ausreichendes „Standing“

On duty sind zu berücksichtigen:

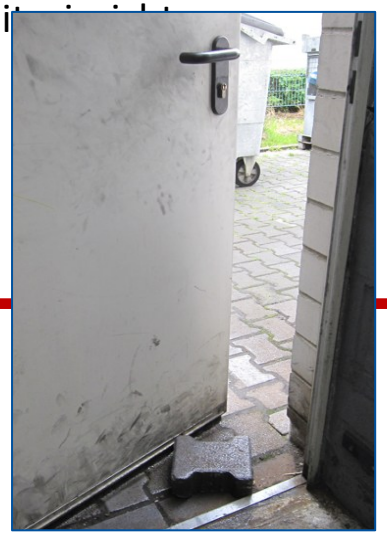
- Sprachbarrieren und Audits mit Dolmetscher
- interkulturelle Unterschiede
- auf Reisen: rechtzeitig und sicher am Ziel ankommen
- Mentalität der Menschen

Sicherheit aus der Praxis

Häufige Schwachstellen

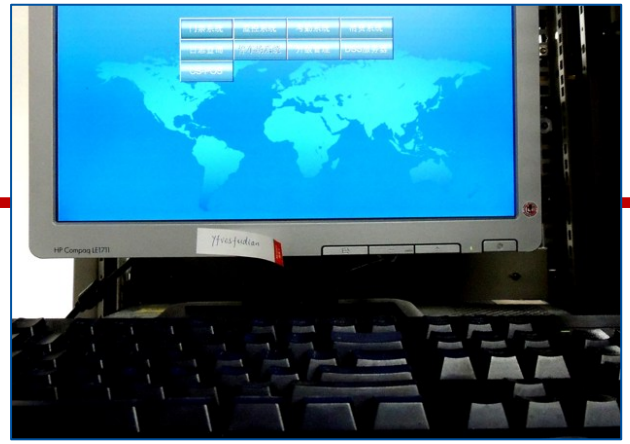
Sicherheitszonen

Oft nicht konsequent gesichert oder es gelten „Vorwände“ seitens der Implementation von Sicherhei



Incident Management

Nur Erfassung von IT-Ereignissen / -Vorfällen. Physische, personelle oder Ereignisse in Bezug auf Dritte werden vernachlässigt, erfolgen separiert oder werden nicht angemessen bewertet.



Asset Management

Oft nur Betrachtung sekundärer IT-Informations-Assets wie Datenträger.

OT-Sicherheit

… nicht immer im ISMS berücksichtigt.

Identifikationsmittel

Einsatz „kopierbarer“ RFID-Karten, Fehlende Sicherheitsanforderungen in der z.B. Krypto-Richtlinie.

Lieferantenmanagement

Oft fehlende Kriterien zur Informationssicherheit,
Auswahl folgt nicht einem Scoring sondern nach „Gefühl“ oder aus Sachzwängen

Die TOP-Findings

Internes Ranking unserer Auditoren

Assets	**Beim Thema Asset-Management werden nur Inventarlisten präsentiert,** jedoch die echten Werte des Unternehmens („Kronjuwelen“) bleiben unbetrachtet.
Identifikation	**Super, wenn man Identifikationsmittel einsetzt,** sie sollten aber technisch up-to-date sein.
Projekte	**Informationssicherheit muss auch in Projekten berücksichtigt werden:** Risikoanalyse gemacht? Richtig klassifiziert und entsprechend behandelt?
Risiken	**Eine Risikoanalyse sollte besser keine halbe Sache ein,** sondern auf einem etablierten Wertemanagement „fußen“.

FRAGEN?

OPERATIONAL SERVICES GMBH & CO. KG

Information Security Experts

Telefon: +49 375 6061 9918

information-security-experts@o-s.de

BERND SCHART

TISAX® Auditor

+49 15151 820 7713

bernd.schart@o-s.de

OPERATIONAL SERVICES
YOUR ICT PARTNER

Eine Konzerngesellschaft der

Backup

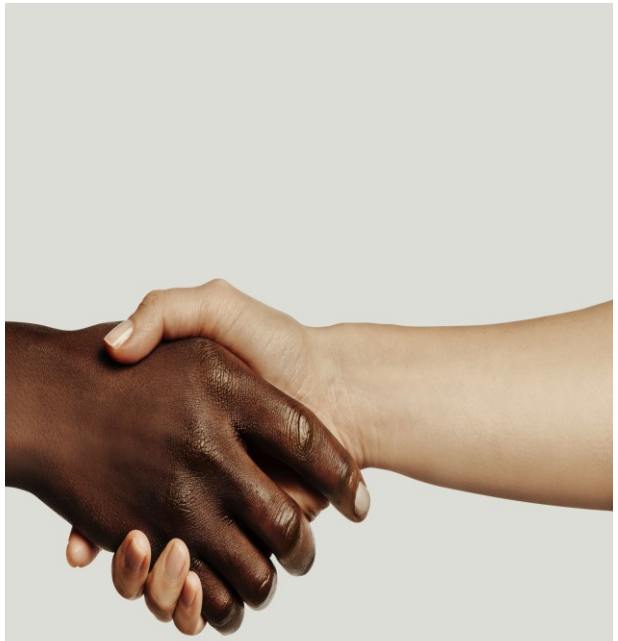
VDA Information Security Assessment – Fragenkatalog:

https://www.vda.de/de/aktuelles/publikationen/publication/vda-isa-katalog--version-6

Kulturelle Herausforderungen

Verhalten und Gesten werden unterschiedlich aufgefasst

1. **Eine halbe Stunde zu spät zu einem Termin?** Im Mittelmeerraum, in Lateinamerika und im südlichen Afrika kein Problem. In Deutschland oder Schweiz eine Beleidigung des Gastgebers.
2. **Lachen ist in Westeuropa ein Zeichen von Fröhlichkeit,** in Japan wird es als Anzeichen von Verwirrung, Unsicherheit oder Verlegenheit gedeutet.
3. **Kopfschütteln bedeutet „ja“ in Indien** und am Ende einer Frage geht die Stimme nach unten - ganz im Gegensatz zur westlichen Interpretation.
4. **Daumen hoch - in Lateinamerika heißt das „Alles klar“.** In Mitteleuropa bedeutet es einfach die Zahl 1. Muslime verstehen darunter jedoch ein grobes sexuelles Zeichen.
5. **Große Vorsicht beim OK-Zeichen (Daumen und Zeigefinger zum Kreis gehalten):** bei Tauchern und Piloten = „Alles klar“; Japaner = „Jetzt können wir über Geld reden“; Südfrankreich = „Nichts, wertlos“; iberische Halbinsel, Lateinamerika, Osteuropa, Russland = verstanden als sehr vulgäre sexuelle Geste.
6. **Ein Engländer versteht unter „compromise“ etwas Gutes –** eine Übereinkunft, ein Kompromiss, etwas Positives für beide Seiten. In den USA sieht man darin eine Lösung, bei der beide Seiten verlieren.



Auch der Handschlag ist nicht überall üblich.

Prüfziel und Assessmentlevel

PRÜFZIEL → TISAX®-PROZESS → PRÜFLABEL

INFORMATIONSSICHERHEIT

Vertrauliche **INFORMATIONEN**
→ Assessment Level 2 / 2.5

Streng vertrauliche **INFORMATIONEN**
→ Assessment Level 3

Hohe **VERFÜGBARKEIT** OT*-RELEVANT?
→ Assessment Level 2 / 2.5

Sehr hohe **VERFÜGBARKEIT** OT*-RELEVANT?
→ Assessment Level 3

* = Operational Technology - Betriebstechnologie

PROTOTYPENSCHUTZ

Schutz von **PROTOTYPENBAUTEILEN – UND KOMPONENTEN**
→ Assessment Level 3

Schutz von **PROTOTYPENFAHRZEUGEN**
→ Assessment Level 3

Schutz von **ERPROBUNGSFAHRZEUGEN**
→ Assessment Level 2**/ 3

Schutz von **PROTOTYPEN WÄHREND VERANSTALTUNGEN UND FILM- UND FOTOSHOOTINGS**
→ Assessment Level 2**/ 3

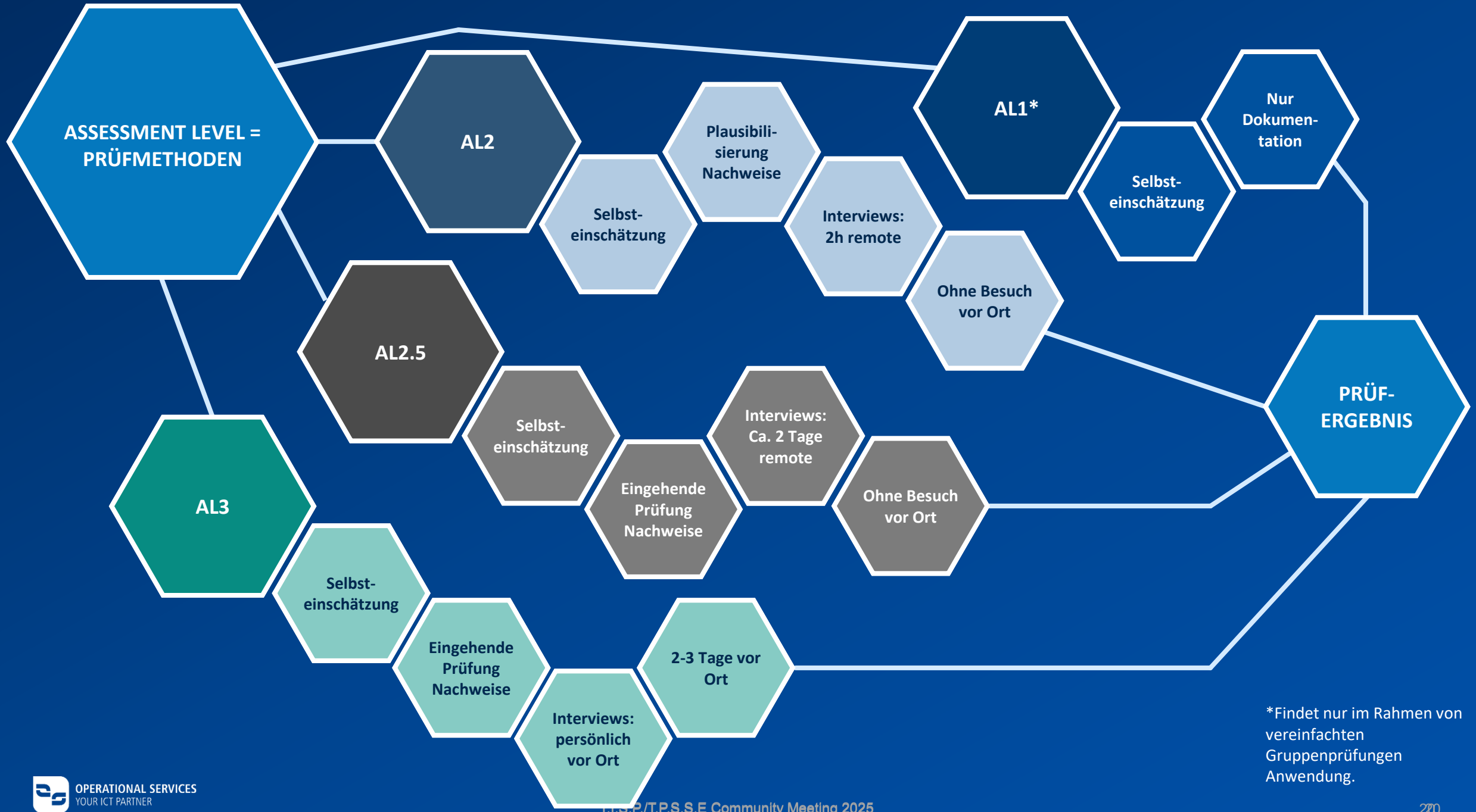
** Ohne eigene Liegenschaften

DATENSCHUTZ

DATENSCHUTZ
→ Assessment Level 2 / 2.5

DATENSCHUTZ
bei besonderen Kategorien personenbezogener Daten
→ Assessment Level 3

Die anzuwendende Prüfmethode wird je nach Prüfziel durch ENX vorgegeben!
Bei mehreren Prüfzielen wird das Gesamtaudit im höchsten zutreffenden Assessment Level durchgeführt.



*Findet nur im Rahmen von vereinfachten Gruppenprüfungen Anwendung.