

Unser Weg zur TISAX- Zertifizierung

Ein Kooperationsprojekt

Sebastian Porombka, ZKI Frühjahrstagung 2024, 5.3.2024

„Das Abenteuer“

Die Herausforderung:

*[...] Die Einrichtung verpflichtet sich zur Vorlage des TISAX-Prüflabels
„Info high bis zum XX.XX.XXXX [...]*

Die Akteure:

- Eine motivierte Maschinenbau-Arbeitsgruppe
- Die Stabsstelle Informationssicherheit
- Die Beratungsfirma, die auf das Label vorbereitet

Was ist TISAX?



- Trusted Information Security Assessment Exchange
- Prüf- und Austauschmechanismus von Prüfergebnissen nach dem branchenspezifischen Standard VDA-ISA
- TISAX ist Automotive-branchenspezifisch
- Kontrollfragen aus Informationssicherheit, Prototypenschutz und Datenschutz
- Referenziert andere Standards, z.B. ISO 27001
- „Scope“ kann festgelegt werden.
 - An der Universität Paderborn: Ein Lehrstuhl ☺

TISAX Prüfziele „Was muss gemacht werden?“

#	Prüfziel	Abkürzung
1	Umgang mit Informationen mit hohem Schutzbedarf	Info high
	Umgang mit Informationen mit <u>sehr hohem</u> Schutzbedarf	Info <u>very</u> high
3	Schutz von Prototypenbauteilen und -Komponenten	Proto parts
4	Schutz von Prototypenfahrzeugen	Proto vehicles
5	Umgang mit Erprobungsfahrzeugen	Test vehicles
6	Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings	Proto events
7	Datenschutz	Data
8	Datenschutz mit besonderen Kategorien personenbezogener Daten [...]	Special Data

Unser Ziel!

TISAX Reifegrade „Wie gut muss es sein?“

Reifegrad	In einem Wort	Beschreibung
0	Unvollständig	Es gibt keinen Prozess, [...]
1	Durchgeführt	[...] informeller Prozess [...]
2	Gesteuert	[...] Prozessdokumentation und Prozessdurchführungsnachweise sind vorhanden.
3	Etabliert	[...] Standardprozess [...] der in das Gesamtsystem integriert ist. Es existieren Nachweise, dass der Prozess über einen längeren Zeitraum nachhaltig und aktiv genutzt wurde.
4	Vorhersagbar	[...] Erheben von [...]
5	Optimierend	[...] kontinuierliche Verbesserung [...]

Mindestreifegrad



Beispiel: Information Security Assessment

Reifegrad	Kontrollfrage	Ziel	Anforderungen (muss)
3 	5.2.3: Inwieweit werden IT-Systeme vor Schadsoftware geschützt?	Ziel ist es, den Schutz der IT-Systeme vor Schadsoftware technisch und organisatorisch sicherzustellen.	+ Anforderungen an den Schutz vor Schadsoftware sind ermittelt. + Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware sind definiert und umgesetzt.

TISAX Assessment-Level und Prüfmethode „Wie wird es geprüft?“

Prüfmethode	Assessment-Level 1 (AL 1)	Assessment-Level 2 (AL 2)	Assessment-Level 3 (AL 3)
Selbsteinschätzung	Ja	Ja	Ja
Nachweise	Nein	Plausibilitätsprüfung	Eingehende Prüfung
Interviews	Nein	Als Webkonferenz	Persönlich, vor Ort
Vor-Ort-Prüfung	Nein	Auf Ihren Wunsch	Ja



- Ergebnisse werden nur auf Plausibilität geprüft!
- Rückfragen im Rahmen eines (Telefon-)Interviews

„Der Plan“

- Commitment des Arbeitsgruppeninhabers zu höheren Sicherheitsanforderungen in der Arbeitsgruppe
- Vorgehen: Implementierung eines Informationssicherheitsmanagementsystemes
 - nach BSI-Grundsatz
 - mit möglichst kleinem Informationsverbund (Genau der Lehrstuhl)
 - Mit allen notwendigen Leit-, Richtlinien, Prozessen
 - Sicherheitskonzept, Asset-Management (Verzeichnis der Informationswerte und Informationsträgern)
 - Erfassung von Kennzahlen um die Wirksamkeit zu belegen
- Minimale Verbindung zu zentralen Diensten der Hochschule

„Die Umsetzung“

- ISMS-Portal für die Arbeitsgruppe ist entstanden
 - ist nun der (!) Anlaufpunkt für alle Mitarbeiter in der AG
 - enthält alle (!) Prozesse / Richt- / Leitlinien die eingehalten werden müssen
 - enthält das komplette Asset-Management
 - enthält das Sicherheitskonzept
 - enthält die Abhängigkeiten zu anderen Betriebseinheiten
 - hält Kennzahlen zum Nachweis der Wirksamkeit
- Mögliche Blaupause für weitere Arbeitsgruppen



ISMS Portal der Arbeitsgruppe

The screenshot shows the Confluence interface for the 'Informationssicherheit' page. The page title is 'Informationssicherheit' and it was created by Sebastian Porombka and last modified by Eduard Kubi on 18 Sept. 2023. The page content includes a list of topics: Verhalten bei Informationssicherheitsereignissen, Richt- und Leitlinien, PDCA, IT-Dienste und IT-Dienstleistungen, Sicherheitszonenkonzept, Asset-Management, and VDA-ISA. Below this is a table of tasks (Aufgaben) with columns for description, due date, assignee, and the page where the task is displayed. The tasks are:

Beschreibung	Fälligkeitsdatum ↓	Bearbeiter	Aufgabe wird angezeigt auf
<input type="checkbox"/> @Eduard Kubi 25.09.2023 Startseite für den Bereich anlegen.	25.09.2023	Eduard Kubi	Lehrstuhl für Dynamik und Mechatronik Startseite
<input type="checkbox"/> @Eduard Kubi 25.09.2023 Systemausstattungen nachdokumentieren.	25.09.2023	Eduard Kubi	Verzeichnis der Informationsträger / IT-Systeme
<input type="checkbox"/> Mit Frau Jürgenhake die juristische Seite klären. Gibt es eine Möglichkeit, dass der Lehrstuhl das Geld zurück bekommen? Gibt es zentrale Mittel für so einen Verlust? @Sebastian Porombka		Sebastian Porombka	Sicherheitszonenkonzept
<input type="checkbox"/> @Eduard Kubi Gibt es Meldepflichten an die VAG-Gruppe bei Informationssicherheitsvorfällen? Wie muss das aussehen? Gibts da nen Portal? Email-Adresse? Telefonnummer? Was ist vereinbart? Auf folgender Seite Dokumentieren: https://confluence.uni-paderborn.de/confluence/display/LDM/Verhalten+bei+Informationssicherheitsereignissen		Eduard Kubi	Lehrstuhl für Dynamik und Mechatronik Startseite
<input type="checkbox"/> @Eduard Kubi Fragestellung: Sicherer / Korrekter Umgang mit Informationsträgern		Eduard Kubi	Richt- und Leitlinien

At the bottom of the page, there is a comment section with a 'Kommentar schreiben' button and a note: 'Bei Fragen oder Problemen wenden Sie sich bitte an den IMT Support unter imt@upb.de, oder per Telefon unter 05251-605544'.

„Die Umsetzung“

- Zentrale Dokumentation der umgesetzten Maßnahmen zum Nachweis während der Label-Prüfung 
 - Umsetzungshinweise zu den Kontrollfragen
 - Referenzen auf Dokumente und Aufzeichnungen zur Umsetzung

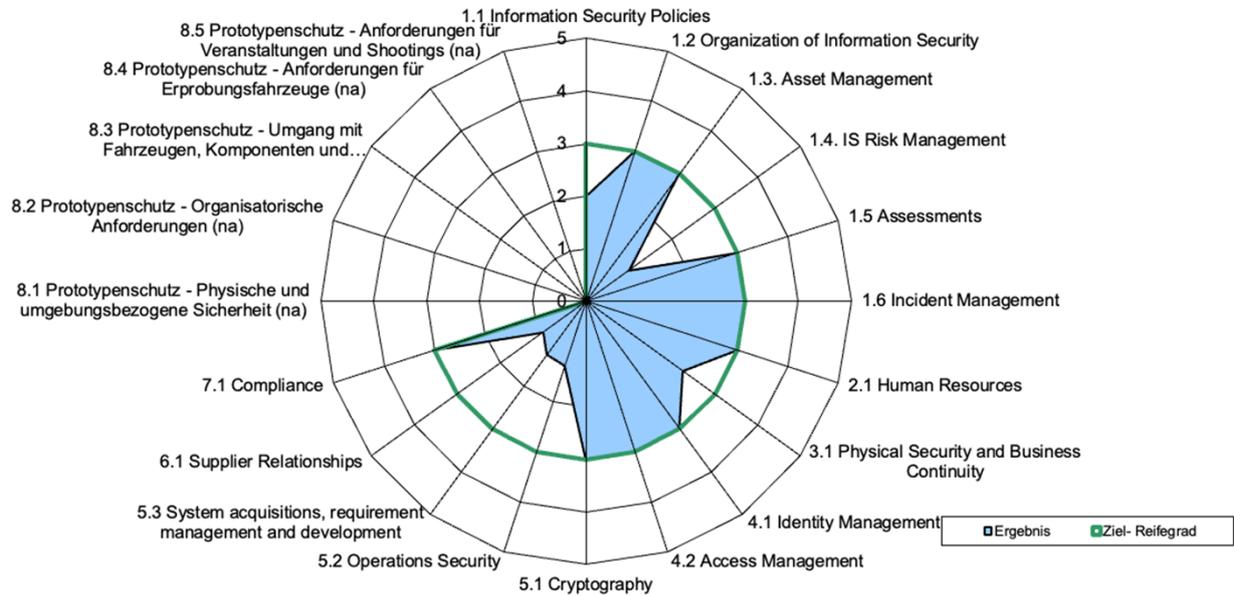
- „Interne“ Fortschrittsanzeige und Leitfaden im Rahmen der Prüfung 

Fortschritte / Leitfaden

Reifegrad	Kontrollfrage	Umgesetzte Anforderungen	Ort d. Dokumentation	Defizite
3	Access Management Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?	Lokale Vergabe durch den Administrator der Arbeitsgruppe. Review der Berechtigungen bei <ul style="list-style-type: none"> * Projektänderungen * Personaländerungen * mind. 1x pro Jahr 	* https://confluence.uni-paderborn.de/display/LDM/Richt+und+Leitlinien#RichtundLeitlinien-Vorgaben%C3%BCrDieVergabeunddasManagementvonZugriffsberechtigungen	
3	IT Security / Cyber Security Cryptography Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?	Richtlinie zur Nutzung kryptografischer Verfahren.	* https://confluence.uni-paderborn.de/display/LDM/Richt+und+Leitlinien	

Aktueller Reifegrad

Ergebnis: 2,28
Ziel: 3,00



„Die Umsetzung“

Letzte offene „Baustellen“ in der Dokumentation (die letzten 20%)

- Informationssicherheits-Risikomanagement (1.4)
- Zentrale Fragestellung bei der Einstellung von Mitarbeitern (2.2)
- Planung von Ausnahmesituationen (3.1)
- IT Change-Management (5.2.1)
- IT Monitoring (5.2.4)
- Systemauditierung (5.2.6)
- Informationssicherheit von Netzwerkdiensten (5.2.7)
- Supplier Relationships (6.1)

„Fazit“

- Gut machbar, wenn alle Leute an einer Leine ziehen
- Große Prozessunsicherheiten in der Schnittstelle zu zentralen Einrichtungen
 - Z.B. Schlüsselausgabe und Entzug, Einstellung von Mitarbeitern
 - Teilweise ein Vakuum in den Zuständigkeiten
- Der kleine Informationsverbund ist sehr agil in der Einführung und Umsetzung von Maßnahmen zur Informationssicherheit
- Es fehlt fast nur noch Dokumentation zu bestehenden Prozessen
- Die erste Prüfung der Unterlagen durch den beratenden Partner ist in greifbarer Nähe