A TISAX®, az autóipari beszállítói információbiztonság bevezetésének tapasztalatai

*„**Az információbiztonsági követelményrendszerek aktuális változásai**” c. EOQ MNB konferencia (2024.03.26.)*

Dr. Horváth Zsolt
INFOBIZ Kft.

TISAX® – információbiztonsági követelmények az autóiparban

TISAX® =
Trusted Information Security Assessment Exchange,
azaz
a „megbízható információbiztonsági értékelések megosztása”

Mi is az a TISAX®?

- az **ENX (European Network Exchange) Association** terméke és bejegyzett védjegye, és az ENX maga menedzseli;
- egy egységes információbiztonsági értékelési (auditálási) rendszer az európai autóipar számára (2017 óta);
- cél az autóiparon belüli egységes elfogadottság;
- sikeres értékelés (audit) esetén az értékelés érvénye 3 év;
- csak dedikált, ENX által akkreditált tanúsító szervezetek auditálhatnak;
- az ISO/IEC 27001 szabványra épül, de annál sokkal részletesebb;

A TISAX® értékelés előnyei, haszna

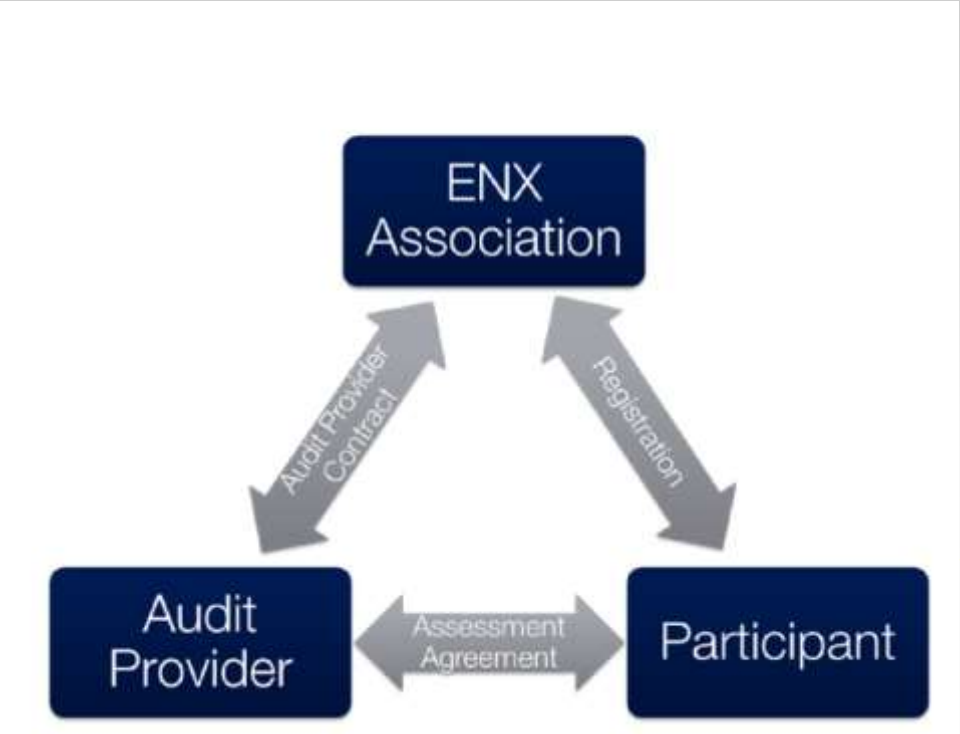
Mi a TISAX® szisztéma célja?

Az autóipari gyártó / megrendelő adatainak biztonsága – kiemelten a bizalmassága

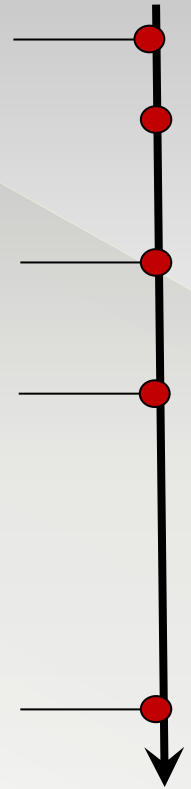
- **Mik ezek az adatok?** → *szerződéses-rendeléses adatok, műszaki specifikációk, tervrajzok, azokhoz kapcsolódó mérési eredmények, termelési – technológiai adatok, prototípus adatok ill. alkatrészek, személyes adatok, …*
- **HOL?** → *Mindenütt ahol ezek az adatok előfordul(hat)nak! (pl. gazdasági, menedzsment területeken, irodákban, tárgyalókban, értékesítésnél, fejlesztésnél, tervezőknél, termelésben, logisztikánál, IT-nál, stb.)*

Kik a TISAX® folyamat szereplői?

- **ENX Egyesület** – *az egész TISAX® folyamatot irányítja, összefogja*
- **Audit szolgáltatók** – *az ENX által akkreditált tanúsító szervezetek, akik szolgáltatásként a TISAX ® értékeléseket (auditokat) elvégzik*
- **Résztvevők**
  - *Akik értékelve lesznek, és az értékeléseik eredményeit megosztják*
  - *Akik az értékelések eredményeit igénylik*



Egy TISAX® projekt lefutása



1. Követelmény / Döntés
2. Audit előkészítés
3. ISMS implementálása
4. (Initial) Audit
5. Nem-megfelelőségek javítása
(CAPA és Follow-up auditok, max. 9 hónap)
6. TISAX® jel megszerzése
7. TISAX® jel érvényességi ideje
(3 év)
8. Re-audit

A TISAX® követelmények

- A követelmények letölthetők publikusan az ENX honlapjáról
- **ISA** (Information Security Assessment) csekklista (Excel formátumban)
- **Tartalmaz:**
  - **Információbiztonsági követelményeket** (ISO 27001 alapon, de testre szabva, kiegészítve, szigorítva)
    - 3 követelményblokk teljesítése:
      - **IS** (általános információbiztonsági rendszer) – kötelező
      - **Proto** (prototípus termékek biztonsága) – opcionális
      - **Data** (személyes adatkezelés) - opcionális
  - **5-szintű érettségi modellt** (SPICE alapon)

→ ***ez az alapja az önértékelésnek is, és az értékelésnek is!***

TISAX megfelelés, ha …

… **teljes mértékben teljesülnek** a következő követelmények (már a V.6. verzióban):

- **Minden folyamat** *(IS modul: 45 db kötelező; Prototípus modul: 22 db opcionális; Adatvédelem modul: 12 db opcionális)*
  - bevezetett, működik,
  - eléri a kitűzött célt és
  - érettségi szintje eléri a 3-as szintet
- Minden működő folyamathoz meghatározott mindegyik kontroll
  - bevezetett és működik,
  - dokumentáltan szabályozottan (megfelelve a folyamat 3-as szintjének), és
  - gyakorlata igazolható, azaz élő példa bemutatható rá.

A TISAX® auditok szintjei

Alapvetően három TISAX értékelési szint lehetséges:

… és még az AL 2,5 is!

1. Értékelési szint (*AL1 – Assessment Level 1*)

csak a vállalat saját önértékelése, az auditor csak a témák meglétének teljességét vizsgálja, tartalmát nem (egyszerűbb esetekben elégséges lehet, ENX TISAX címke nincs)

2. Értékelés szint (*AL2 – Assessment Level 2*)

az értékelés során az önértékelés eredményeinek „hihetőségi vizsgálata” a benyújtott dokumentációk és bizonylatok alapján (dokumentáció értékelés és távaudit, helyszíni vizsgálat csak szükség esetén)

3. Értékelési szint (*AL3 – Assessment Level 3*)

teljes és részletes helyszíni értékelési folyamat, a bizonyítékok ellenőrzésével és interjúkkal lefolytatva

A TISAX értékelési cél – AL-szint megfeleltetés

No.	Értékelési cél	Jelölés	Min. AL
1.	***Magas védelmi igényű információk***.	*Info high*	*2*
2.	***Nagyon magas védelmi igényű információk***	*Info very high*	***3***
3.	**Bizalmas** (a magas védelmi igénynél dominál a bizalmassági elvárás)	Confidential	2
4.	**Szigorúan bizalmas** (a nagyon magas védelmi igénynél dominál a bizalmassági elvárás)	Stictly confidential	**3**
5.	**Magas rendelkezésre állású** (a magas védelmi igénynél dominál a magas rendelkezésre állási elvárás, pl. termelési tevékenységek, …)	High available	2
6.	**Nagyon magas rendelkezésre állású** (a nagyon magas védelmi igénynél dominál a magas rendelkezésre állási elvárás, pl. termelési tevékenységek, …)	Very high available	**3**

A TISAX értékelési cél – AL-szint megfeleltetés

No.	Értékelési cél	Jelölés	Min. AL
7.	**Prototípus alkatrészek** (akik a saját telephelyükön gyártanak, tárolnak vagy használnak prototípus részegységeket vagy alkatrészeket)	Proto parts	3
8.	**Prototípus járművek** (akik a saját telephelyükön gyártanak, tárolnak vagy használnak külön védelmi igényűnek besorolt prototípus járműveket)	Proto vehicles	3
9.	**Tesztjárművek** (akik teszteket végeznek vagy tesztvezetést csinálnak külön védelmi igényűnek besorolt járművekkel)	Test vehicles	3
10.	**Prototípus események** (akik rendezvényeket, fotó- vagy filmbemutatásokat csinálnak külön védelmi igényűnek besorolt járművekkel)	Proto events	3
11.	**Személyes adatok** (személyes adatkezelési tevékenységek esetén, …)	Data	2
12.	**Különleges személyes adatok** (különleges személyes adatok – mint pl. egészségügyi, vallási, stb – adatkezelési tevékenységei esetén, …)	Special data	3

Az „Információbiztonság” al-témakörei

1. Információbiztonsági szabályozások és szervezet	• *Információbiztonsági szabályzatok* • *Az információbiztonság szervezete* • *Vagyonelemek kezelése* • *IS kockázat menedzsment* • *Értékelés* • *Incidens- és krízishelyzet kezelés*
2. Humán erőforrások biztonsága	• *Humán erőforrások*
3. Fizikai biztonság	• *Fizikai biztonság és üzletmenet-folytonosság*
4. Azonosítás és hozzáférések kezelése	• *Azonosítás menedzsment* • *Hozzáférés felügyelet*
5. IT-biztonság / kiber-biztonság	• *Kriptográfia* • *Üzemeltetés biztonsága* • *Rendszerek beszerzése, követelménykezelés és fejlesztés*
6. Beszállítói kapcsolatok biztonsága	• *Beszállítói kapcsolatok*
7. Megfelelés (Compliance)	• *Compliance*

A „Prototípus-védelem” al-témakörei

A „Prototípus-védelem” modul a fizikailag prototípusokkal, azok alkatrészeivel vagy részegységeivel foglalkozók esetén írja elő az arra vonatkozó, kiemelt szintű fizikai és szervezési információbiztonsági kontrollokat.

Ezek fő témakörei:

8.1. Fizikai és környezeti biztonság
8.2. Szervezeti követelmények
8.3. A járművek, alkatrészek és részegységek kezelése
8.4. A tesztjárművekre vonatkozó követelmények
8.5. A bemutató eseményekre és fotózásra vonatkozó követelmények

Az „Adatvédelem” al-témakörei (v.6)

Az „Adatvédelem” modul a személyes adatok kezelésével kapcsolatos (GDPR-nak való megfelelési) előírásokat, információbiztonsági kontrollokat tartalmazza.

Ezek fő témakörei:

9.1. Adatvédelmi szabályozások
9.2. Az adatvédelem szervezete
9.3. Adatkezelési tevékenységek átláthatósága
9.4. Adatvédelmi hatáselemzés
9.5. Adattovábbítás
9.6. Érintetti kérelmek és incidensek kezelése
9.7. Emberi erőforrások (munkavállalók)
9.8. Adatkezelői utasítások

A követelmény-szintek magyarázata

Szint	Mely kontrollok esetén alkalmazandó
KELL (must)	Minden kontrollra kötelező alkalmazni, nem hagyható el!
AJÁNLOTT (should)	Minden kontrollra kötelező alkalmazni, csak alapos (és dokumentált) indokkal hagyható el!
MAGAS VÉDELMI IGÉNYEK	Csak a „magas védelmi igényű” és a „nagyon magas védelmi igényű” kategóriák, ilyen besorolású adatokat tartalmazó folyamatok és adatkezelések esetén KELL alkalmazni!
NAGYON MAGAS VÉDELMI IGÉNYEK	Csak a „nagyon magas védelmi igényű” kategóriák, ilyen besorolású adatokat tartalmazó folyamatok és adatkezelések esetén KELL alkalmazni!
SGA esetén további követelmények	*Egyszerűsített csoportos audit (SGA – Simplified Group Assessment) esetén érvényes további követelmények.*

Az érettségi szintek

Szint	Megnevezése	Jellemzése
0	**Hiányos**	Nem létezik a folyamat, vagy a folyamat nem éri el a kitűzött célt.
1	**Kialakított**	Van bevezetett folyamat, és vannak eredményei.
2	**Menedzselt**	A cél elérésére meghatározott folyamatok léteznek, és dokumentáltan szabályozottak. Működése a tervezett, felelősségek és erőforrások biztosítottak, lefolytatás és eredmények folyamatos megfigyelése.
3	**Sztenderdizált**	Dokumentáltan szabályozott sztenderd folyamat, testre-szabási (alkalmazási) irányelvekkel. Erőforrások menedzseltek, személyzetnek kialakított képzések, menedzselt kontrolling, …
4	**Mért**	Megfelel a 3. szintnek, továbbá a folyamat mért és mérés alapján szabályozott.
5	**Optimalizált**	Megfelel a 4. szintnek, továbbá dedikált személyzet felelős a folyamat folyamatos továbbfejlesztéséért.

A TISAX önértékelés végrehajtása

A **VDA-ISA_EN_6-x-x** Excel csekklista kérdéslistát tartalmazó oldalainak kitöltésével

Tartalmazza:

- **Témakörök** (1…8) – értékelendő területek (+ Adatvédelem)
  - **Folyamatok** (1.1, 1.2, …) – értékelendő területeken belüli témák
    - Önálló témáknak, mint folyamatoknak az adott **célt** meg kell valósítaniuk
    - Az adott célt megvalósító folyamatnak az elvárt **érettségi szinten** kell ezt tennie
    - Az adott cél megvalósításához (legalább) a felsorolt **kontrolloknak** – mint követelményeknek – kell megfelelően működniük. (Kontrollok bevezetettsége: az előírt követelmény-szintnek megfelelve!)
- **Bevezetendők és ellenőrzendők folyamatonként:** ***cél megvalósulása, dokumentáltság, gyakorlat, érettségi szintek, kontrollok működése***

Az ISA csekklista kitöltése

KITÖLTENI

Válaszok leírása, hogyan teljesítjük a követelményeket

Evidenciák (bizonyítékok) felsorolása

Megállapítások (jellemzően hiányok) felsorolása

Követelmények

Folyamat neve és célja

Information Security Assessment Questionary

ISA Classic	ISA New	Maturity level	Beschreibung der Umsetzung	Referenz Dokumentation	Feststellungen/Prüfergebnis	Control question	Objective
	1					IS Policies and Organization	
	1.1					Information Security Policies	
						To what extent are information security policies available?	The organization nee policy. This reflects th information security Additional policies m size and structure of
05.1	1.1.1						

A VDA ISA csekklista kitöltése

Követelmények

Folyamathoz a kötelező kontrollok

Folyamathoz az ajánlott kontrollok

Folyamathoz (csak a) magas védelmet igénylő adatok kontrolljai

Folyamathoz (csak a) nagyon magas védelmet igénylő adatok kontrolljai

	K	L	M	N	
	Requirements (must)	Requirements (should)	Additional requirements for high protection needs	Additional requirements for very high protection needs	Usa for
ty n. he	+ The requirements for information security have been determined and documented: - The requirements are adapted to the organization's goals, - A policy is prepared and is released by the organization. + The policy includes objectives and the significance of information security within the organization.	+ The information security requirements based on the strategy of the organization, legislation and contracts are taken into account in the policy. + The policy indicates consequences in case of non-conformance. + Further relevant information security policies are prepared. + Periodic review and, if required, revision of the policies are established. + The policies are made available to employees in a suitable form (e.g. Intranet). + These policies (or extracts thereof) are provided to external business partners depending on the respective case. + Employees and external business partners are informed	None	None	

IBIR bevezetés lépései

1. Alkalmazási terület (szkóp) és politika meghatározása
2. A szervezeti keretek és erőforrások tisztázása
3. A védendő (információs) vagyon felmérése
4. Fenyegetettségek felvétele, kockázatok felmérése
5. Védelmi intézkedések, kontrollok meghatározása
6. Védelmi intézkedések és IBIR folyamatok dokumentálása
7. Állomány oktatása, tudatosítás
8. Életbe léptetés

Kontrollok, szabályozások területei

- IBIR szervezeti működés és adminisztratív biztonsági szabályozások (kockázati alapon)
- Információbiztonsági területek működésének szabályozásai
  - *Fizikai biztonság (objektum- és területvédelem, papír alapú adatok biztonsága);*
  - *Humán biztonság;*
  - *Informatikai biztonság és kibervédelem (vonatkozik mindenkire, akik az IT infrastruktúrával kapcsolatban vannak – használják, üzemeltetik, fejlesztik);*
  - *Személyes adatok biztonsága (GDPR megfelelés)*
- Vállalati folyamatokba épített információbiztonsági szempontok
- Incidensek kezelése és üzletmenet-folytonosság biztosítása (vészhelyzetek esetén is)

Kérdések és válaszok

INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft.

: https://infobiz.hu/

Dr. Horváth Zsolt

: +36 70 4198599

: horvathzs@infobiz.hu