# TISAX, az autóipar új információbiztonsági követelményrendszere

Dr. Horváth Zsolt

## Abstract

A világban a vállalatok számára egyre jelentősebb nemcsak saját, hanem beszállítóik információbiztonsági rendszereinek működése is. Ez kiemelten igaz az autóipar esetében, ahol az autóipari speciális elvárások miatt 2017-ben a VDA egy új autóipari információbiztonsági követelményrendszert és ehhez kapcsolódó auditálási rendszert hozott létre. Ez a követelményrendszer a TISAX, amelyet egységesen értelmezve és auditálva minden autóipari gyártó és megrendelő egységesen elfogad.

A TISAX fogalma és követelményei Magyarországon még újnak számítanak, és alig ismertek. Ugyanakkor már egyre több autóipari beszállítónál írják elő a gyártók ezt teljesítendő követelménynek, ami egyben az üzleti megrendelés egyik feltételévé is vált. Ez a szakcikk összefoglalja a TISAX folyamatról és követelményrendszerről azokat az általános tudnivalókat, amelyeket tudni szükséges és érdemes a megfelelő döntés meghozása előtt.

## 1. Bevezetés

A vállalatok működése az elmúlt évtizedekben jelentősen átalakult, és rohamosan megnőtt az informatikától való függősége. Korunkra már szinte elképzelhetetlen olyan vállalat, amely ne használna informatikai eszközöket, rendszereket a működése szinte minden területének támogatására, beleértve a kommunikációt, pénzügyi folyamatokat, a logisztikát, a termelést és termelésirányítást, stb.

Ezen informatikai támogatások megvalósításához egyre nagyobb számítástechnikai kapacitás, egyre erősebb informatikai infrastruktúra szükséges, valamint ezek üzemeltetéséhez megfelelő speciális szaktudás. Ezeket a feladatokat a vállalatok, különösen a kisebbek (pl. KKV szektor) sokszor kiszervezik, azaz külsős és erre szakosodott vállalkozásoknak adják át. A világ mai fejlődési trendjén azonban az informatikai infrastruktúrának jellemzően nemcsak az üzemeltetését szervezik ki, hanem magát az infrastruktúrát a rajta futó alkalmazásokkal is, és így azokat szolgáltatásként veszik igénybe. Lényegében ezek az ún. (különböző szintű) felhőszolgáltatások. Ezeknek rugalmas paraméterezhetősége, könnyű elérhetősége szinte bármilyen mobilkommunikációs eszközről, és nagyfokú üzemeltetési megbízhatósága vonzóvá teszi ezek használatát egyre több vállalkozás számára.

De az élet itt sem állt meg. Az internet eszközei és egyre újabb alkalmazásai, a közösségi

oldalak világa is ma már a vállalatok működésébe beépült, ahogy az IoT[1] világa illetve az Ipar 4.0 is egyre nagyobb teret nyer.

Ez a trend azonban a számos előnye mellett rengeteg új veszélyt is hozott magával. A vállalat működése ily módon nagyon nagymértékben kiszolgáltatottá vált az azt támogató informatikától, és az azt szolgáltató vállalatoktól. Hogyha az adott folyamatot (vagy tevékenységet) támogató informatikai szolgáltatás nem érhető el, vagy leáll, akkor már az a folyamat sem tud tovább működni. Hogyha az informatikai szolgáltatás hibázik, akkor az azonnal a támogatott folyamat hibás működését eredményezi. Ezek bármelyike pedig könnyen bekövetkezhet akárcsak a szoftver hibájából, akárcsak üzemeltetési vagy bármilyen kommunikációs problémából, stb. kifolyólag, és mindegyik azonnal igen jelentős kárt okozhat az adott vállalatnak. És akkor még nem is beszéltünk az információ bizalmassági kérdéseiről, hiszen a működésünk támogató rendszereiben lévő adatok számunkra bizalmas üzleti információkat, üzleti titkokat jelentenek, amelyeknek illetéktelenek általi megismerése beláthatatlan üzleti kárt, veszteséget és/vagy jogi következményeket vonhat maga után.

A mai világban nem szabad továbbá figyelmen kívül hagyni az interneten keresztüli bűnözést sem, ami már minden ember, mint magánszemély és minden vállalat számára egyre nagyobb veszélyeket rejt. Az internet világa, a kibertér elterjedésével a kiberbűnözés is egyre jelentősebbé válik, és a vállalatok számára az egyik legnagyobb veszélyforrást jelenti.

Összefoglalva minden vállalat működése elképzelhetetlen megfelelő stabil, megbízható és biztonságos információszolgáltatás nélkül, ami biztosítja számára az információknak a rendelkezésre állását, sértetlenségét (pontosságát és módosítatlanságát) valamint a bizalmasságát. Ezt a három tulajdonságot nevezzük az információ biztonságának, ami ily módon a vállalatok számára egyre nagyobb jelentőségű.

## 2. Információbiztonsági elvárások az autóiparban

### *a. Az információbiztonság jelentősége – az autóipar számára*

Az autóiparban fokozottan igaz ez a trend. Hiszen az autóiparra kiemelt minőségi és biztonsági követelmények jellemzők. A járművek működése során kis hiba is komoly balesetet, életveszélyt jelenthet, ezért a termékeknek sokkal szigorúbb biztonsági és minőségi követelményeknek kell megfelelniük. Az autógyárak a hatékonyságuk növelésére sokan jellemzően ún. JIT[2] rendszerben termelnek. Ez igen szigorú szervezési, minőségi és pontossági követelményeket jelent mind a teljes termelés megszervezésnek, mind az összes ide beszállító alvállalkozónak.

Az autóipar éppen ezért az információk biztonságának mind a három követelményére (bizalmasságra, rendelkezésre állásra és sértetlenségre) vonatkozólag nagyon szigorú beszállítói követelményeket fogalmaz meg a teljes beszállítói lánccal szemben. Ezek egy része bújtatva

[1] IoT (Internet of Thinks) – 'a dolgok internetje' kifejezés tulajdonképpen az egyre több hétköznapi dolog, mint cselekvés, szolgáltatás vagy csak valamely eszköz használatának interneten való követését, adatbázisban való feldolgozását és egyben távoli (automatikus vagy beavatkozáson alapuló) irányítását jelenti. Ezek az ún. okos dolgok, mint pl. okos-TV, okos-lakás, okos-bevásárlóközpont, okos-város, stb.

[2] JIT (Just in Time) – ez a kifejezés a gyártás során azt jelenti, hogy minden tevékenységhez az akkor szükséges nyersanyagok, alapanyagok vagy megfelelő résztermékek épp akkorra készülnek el vagy beszállítás során kerülnek oda a feldolgozás helyére, amikor az szükséges.

az autóipari minőségirányítási szabvány-követelményekben már eddig is megjelent. Az elmúlt években azonban egy új, direkt autóipari szempontokat figyelembe vevő információbiztonsági követelmény-rendszerben, a TISAX-ban tisztult le egységes formában. Ez a követelményrendszer egységesíti és összefoglalja az autóipari beszállítókra vonatkozó információbiztonsági elvárásokat, és a legtöbb esetben mintegy kiindulási feltételként fogalmazódik meg az autóipari beszállítóvá váláshoz.

Az autóipari beszállítói láncnak már eddig is igen szigorú követelményeknek kellett megfelelni tudni, ami a termékminőség követelményein túl kiterjedt az adott beszállítóknak a tevékenységükre vonatkozó képességi követelményeire is, azaz hogy mennyire képesek az adott beszállításokat folyamatosan, megfelelő pontossággal, időzítéssel és mindig a kívánt minőségben elvégezni. Ez azt jelenti, hogy a beszállítók minőségirányítási rendszerének az ISO 9001 szabványnál is szigorúbb követelményeknek kell megfelelni tudni, amit az autóipar által kifejlesztett, az ISO 9001-re épülő IATF[3] szabvány követelményei tartalmaznak.

Ez a szabvány megköveteli – többek közt – az adott autóipari beszállító teljes termelési (értékteremtő) láncára vonatkoztatott megbízható és stabil működési képességét, ami kiterjed a főfolyamatok működésének teljes infrastruktúrájának követelményeire, beleértve a teljes támogató és irányító informatikai infrastruktúrát is. Ennek a megbízható és folyamatos üzemeltetése, és védelme bármilyen hibázástól, fenyegetéstől vagy támadástól jelenti az informatika üzemeltetéséhez kapcsolódó informatikai biztonsági tevékenységeket, mint az információbiztonsági feladatok egy jelentős részét.

*b. Információbiztonság az IATF-ben [1, 2]*

Az információbiztonsági követelmények megjelentek az autóipari beszállítók minőségügyi szabványában, az IATF 16949:2016-ban (röviden az IATF-ben) is. Igaz, hogy ezek itt többnyire még bújtatottan jelentek meg, azaz nem közvetlen információbiztonsági követelményként megfogalmazva. Azonban a megfogalmazott minőségügyi követelmények teljesítése bizonyos információbiztonsági / informatikai biztonsági kontrollok megvalósítását kényszeríti ki. Ezek közül egyes követelmények direkt magában a szabványban eredetileg is benne megtalálhatók, viszont számos követelmény a szabvány megjelenése utáni kiegészítő követelmények (ún. „Sanctioned Interpretation") során épültek be a szabványba.

De nézzük, miről is van szó! Melyek azok az IATF trémakörök és követelmények, amelyeknek a megvalósítása komoly információbiztonsági követelményeket jelent? Ezek közül a legfontosabbak (a teljesség igénye nélkül) a következők:

- **A termelési és a támogató folyamatokat segítő infrastruktúra kibervédelme**
  - **o 6.1.2.3. Contingency plans (készenléti tervek)**

A termelő folyamatok és infrastruktúra fenntartását és folyamatos működtetését fenyegető kockázatokat folyamatosan fel kell mérni és megfelelő kockázatarányos intézkedésekkel kezelni kell, beleértve a szükséges vészhelyzeti és visszaállítási tervek elkészítését és karbantartását. Ha az érintett infrastruktúra informatikai infrastruktúra, akkor ez értelemszerűen az IT BCP/DRP meglétét várja el. Amikor

[3] IATF (International Automotive Task Force) – azaz ez a nemzetközi autóipari követelményrendszer az autóipari minőségirányítási rendszer követelményszabványa maga.

a kockázat forrása informatikai biztonsági jellegű, akkor ez értelemszerűen a megfelelő IT biztonsági kockázatfelmérést és IT kockázatkezelési intézkedést vonja maga után. Ennek a kihangsúlyozását az IATF kiegészítő követelmények két további pontban is konkretizálták:

**SI[4] 3:** 6.1.2.3.c) készenléti tervek készítése kötelező a következő esetekben: … az IT rendszerek kibertámadása esetére … (az SI 3 ezen belül is kiemeli a ransomware támadások eseteit)

**SI 17:** 6.1.2.3.e) a készenléti tervek rendszeres tesztelése során külön figyelmet kell fordítani a kibervédelem tesztelésére, a kibertámadások szimulációjára is.

- **o 7.1.3 Infrastructure (infrastruktúra)**

A folyamatok működéshez szükséges infrastruktúrákat fenn kell tartani, ennek részeként az informatikai infrastruktúrát is.

- **o 7.1.3.1. Plant, facility, and equipment planning (üzem, létesítmény és berendezés tervezése)**

**SI 18:** 7.1.3.1.c) a termelést támogató berendezések és rendszerek kibervédelmét meg kell valósítani.

A informatikai biztonság nem korlátozódhat csak az irodai és a támogató folyamatok számítógépeinek biztonságára. A termelésben és termelésirányításban használt informatikai infrastruktúra is ki van téve a kibertámadás veszélyének.

- **Mérőeszközök kalibrálása**
  - **o 7.1.5.3.1. Internal laboratory (belső laboratórium)**

ISO/IEC 17025 (vagy egyenértékű) szerinti, harmadik fél általi akkreditáció ajánlás a laboratórium megfelelésének igazolására.

- **o 7.1.5.3.2. External laboratory (külső laboratórium)**

**SI 10:** 7.1.5.3.2. ISO/IEC 17025 (vagy egyenértékű) szerinti, harmadik fél általi akkreditáció szintén ajánlás a laboratórium megfelelésének igazolására.

Az MSZ ISO/IEC 17025:2018 szabvány 7.11. Az adat- és információkezelés felügyelete c. követelménye egyértelműen előírja a laboratóriumi informatikai rendszerek validációját, továbbá ezeknek a rendszereknek az informatikai biztonsági kontrolljait, amelyek biztosítják a rendszerek védelmét jogosulatlan hozzáféréstől, hamisítástól és károsodástól, adatvesztéstől, az adatok sértetlenségének (integritásának) sérülésétől, stb.

Ezek a követelmények, – azaz a mérőeszközök működtetésének informatikai biztonsági kontrolljainak szükséges megléte, továbbá a mérőeszközökben lévő szoftverelemek validációja, – kiterjednek nemcsak a laboratóriumok mérőeszközeire, hanem értelemszerűen az összes gyártásban, termelésben és egyéb folyamatokban alkalmazott mérőműszerekre is.

- **Adatok mentése és archiválása**
  - **o 7.5.3.2.1. Record retention (Feljegyzések megőrzése)**

Létre kell hozni a feljegyzések megőrzésére egy szabályzatot, amely feleljen meg a törvényi, vevői és a szervezet belső elvárásainak. Autóiparon belül mind a VDA előírásaiban, mind gyakran az ügyfél specifikus követelményekben (CSR) a hosszú idejű adatmegőrzési követelmények a jellemzők. Elektronikus feljegyzések

[4] SI (Sanctioned Interpretation) – az IATF kiegészítő követelménye

esetén ez a mentési és archiválási rendszerre határoz meg további követelményeket.

- **o 8.5.2.1. Identification and tracebility – supplemental (Azonosítás és nyomon követhetőség – kiegészítés)**

Az összes autóipari termékre vonatkozó belső, vevői és jogszabályi nyomon követési követelmények elemzését el kell végezni, ideértve a nyomon követési tervek kidolgozását és dokumentálását, a munkavállalók, az ügyfelek és a fogyasztók kockázatainak vagy a termék meghibásodásának súlyossága alapján. Ennek keretében … d) biztosítani kell a dokumentált információk követelményeknek megfelelő megőrzését, amibe beleértendők az elektronikus formátumú dokumentált információk megőrzésének követelményei is.

- **o 10.2.3. Problem Solving (probléma megoldás)**

Dokumentált folyamatot kell fenntartani a problémák gyökér-ok keresésére és megoldására. Ennek értelemszerűen ki kell terjednie az adatmegőrzéssel és az informatikai rendszerekkel kapcsolatos problémákra is.

- **Adatvédelem és kommunikáció az ügyféllel**
  - **o 8.1.2 Confidentality (bizalmasság)**

A szervezetnek gondoskodnia kell a vevői szerződések alapján fejlesztett és gyártott termékek és fejlesztési projektek titkosságáról, beleértve mind a kapcsolódó termékinformációkat is. Ezek alapján külön megfontolandók a tervezési / fejlesztési folyamatokban a tervek (pl. CATIA állományok) bizalmas elektronikus kezelése, illetve a felhő szolgáltatások használata esetén azok biztonsági garanciái.

- **o 8.2.1.1 Customer communication — supplemental (ügyfél kommunikáció – kiegészítések)**

A szükséges adatokat és információkat (pl. számítógépes tervezési adatok, elektronikus adatcsere) az ügyfél által megadott számítógépes nyelven és formátumban kell tudni továbbítani az ügyfélnek. Ez követelményeket határoz meg mind az adatok elektronikus formátumára, mind az elektronikus kommunikáció megfelelően biztonságos kialakítására is.

- **Termékbe beágyazott szoftverek biztonsága**

A beágyazott szoftver egy speciális hardverközeli program, amelyet pl. egy gépjármű-alkatrészben (általában számítógépes chip vagy más nem felejtő memória) tárolnak, amely az adott alkatrész elektronikájának alapvető funkcióit biztosítja. A gépjárművek egyes informatikai vezérlő és ellenőrző programjai alapvetően ezeknek az alkatrészeknek ezeket a hardver-közeli alapfunkcióit használják. A gépjárművek informatikai rendszereinek működése szempontjából kiemelten kritikus ezeknek a beágyazott szoftvereknek a megbízható és biztonságos, hibamenetes működése. A következő szabványkövetelmények éppen ezért a beágyazott szoftverek biztonságára és biztonságos fejlesztésére határoznak meg követelményeket.

- **o 8.3.2.3 Development of products with embedded software (termékfejlesztés beágyazott szoftverekkel)**
- **o 8.3.4.2 Design and development validation (tervezés és fejlesztés validálása)**
- **o 8.3.6.1 Design and development changes — supplemental (változások a tervezésben és fejlesztésben – kiegészítések)**
- **o 8.4.2.3.1 Automotive product-related software or automotive products with**

**embedded software (autóipari termékekhez kapcsolódó szoftverek vagy beágyazott szoftverekkel felszerelt autóipari termékek)**

- **8.5.6.1 Control of changes — supplemental (Változáskezelés – kiegészítések)**

Ezekből látszik jól, hogy az IATF-ben komoly hangsúlyt fektettek a termelés és termeléstámogatási folyamatok folytonosságának, megfelelő és megbízható működésének a biztosítására. Ennek komoly előfeltétele az informatikai támogató és vezérlő rendszerek megfelelő, megbízható és biztonságos működése. Ezek így elsősorban az információbiztonságnak, és azon belül is elsősorban az informatikai biztonságnak a rendelkezésre állási és sértetlenségi aspektusaira vonatkoznak.

Ha megfordítjuk, és azt nézzük, hogy az informatikai üzemeltetés és információbiztonság mely területeire határoznak meg ezek az IATF elvárások követelményeket, akkor a következő területeket látjuk:

- Informatikai biztonsági kockázatfelmérés és kezelés
- Titoktartás és külső kommunikáció biztonsága
- Jogosultságmenedzsment
- Adatmentési és archiválási rendszerek
- Naplózás
- IT BCP/DRP (informatikai üzletmenet-folytonossági illetve katasztrófahelyzet utáni visszaállítási tervek)
- Kibervédelem és kibertámadások szimulációja
- Szoftverfejlesztés biztonsága

Tulajdonképpen önmagukban már ezek is jól mutatják az információbiztonsági elvárások autóipari jelentőségét és komolyságát, de az autóipar már ezen is túllépett, ezek fenntartása mellett további direkt információbiztonsági követelményeket határozott meg.

*c. Beszállítói információbiztonsági elvárások egységesítése*

Az autóipari gyártóknak és szervezeteknek további szigorú elvárásaik a beszállítóikkal szemben a saját adataik védelme, bizalmassága. A beszállítói együttműködés során a beszállítóknál a beszállítások tárgyát képező üzleti és termékadatokon kívül sokszor egyéb technológiai és/vagy a megrendelőre, termékeire vagy alkalmazottaira vonatkozó bizalmas adatok kezelése is lehetséges. Ezek biztonsága, kiemelten bizalmassága és illetéktelenek általi hozzáférés megakadályozása sokszor kiemelt jelentőségű.

Az elmúlt években ily módon kialakult, hogy (elsősorban) az autógyártók (OEM-ek) a beszállítóiktól az egyéb minőségirányítási elvárásokon túlmenően szigorú információbiztonsági követelmények teljesítését várták el. Erre mindegyik autógyártó kialakította saját információbiztonsági követelményrendszerét, amelyet a beszállítójának teljesítenie kellett, és amelyet általában saját auditorai ellenőriztek. Ez azt is jelentette, hogyha egy speciális alkatrész-gyártó egyszerre több autógyárnak szállított be, akkor mindegyik megrendelőnek az információbiztonsági rendszerre vonatkozó követelményrendszerét külön-külön teljesítenie kellett. Ezek egymással jelentős részben átfedésben voltak, de ugyanakkor mindegyiknek voltak saját külön egyéni elemei is, amelyek miatt lényegesen nagyobb felkészülési igényt jelentett az egyes követelményrendszereknek való külön-külön megfelelés biztosítása.

Ennek a problémának a feloldására és egyszerűsítésére dolgozott ki a VDA egy új, egységes

követelményrendszert és hozzá tartozó értékelési rendszert, amellyel ennek a követelményrendszernek való megfelelés egységesen értékelhető, azaz auditálható. A cél egy olyan követelményrendszer kidolgozása volt, amely egységesen a nemzetközi információbiztonsági irányítási rendszerszabvány követelményein alapszik, de továbbfejlesztve tartalmazza az autóipar jellemző információbiztonsági igényeinek való megfelelés követelményeit, és amelyet minden autóipari gyártó egységesen elfogad. Ezzel megszűnhet az egyes autógyártók különálló követelményeinek való – sokszor redundáns – a megfelelési kényszer.

Ez a követelményrendszer a TISAX, azaz a Trusted Information Securuty A2sessment Exchange, magyarul a megbízható információbiztonsági értékelések megosztása. A TISAX ilyen módon az ISO/IEC 27001 szabványra épült, és struktúrájában annak követelménystruktúráját vette át és azt egészítette ki további követelményekkel. A TISAX szerinti információbiztonsági irányítási rendszer alapvető célja az ügyfél (megrendelő) információinak védelme. Ennek megfelelően a TISAX követelményei vonatkoznak minden olyan folyamatra, személyre, eszközre, infrastruktúrára, adathordozóra, informatikai eszközre, stb. ami az ügyfél adataival kapcsolatban van, ahol azokat védeni szükséges.

# 3. A TISAX rendszer működése [3]

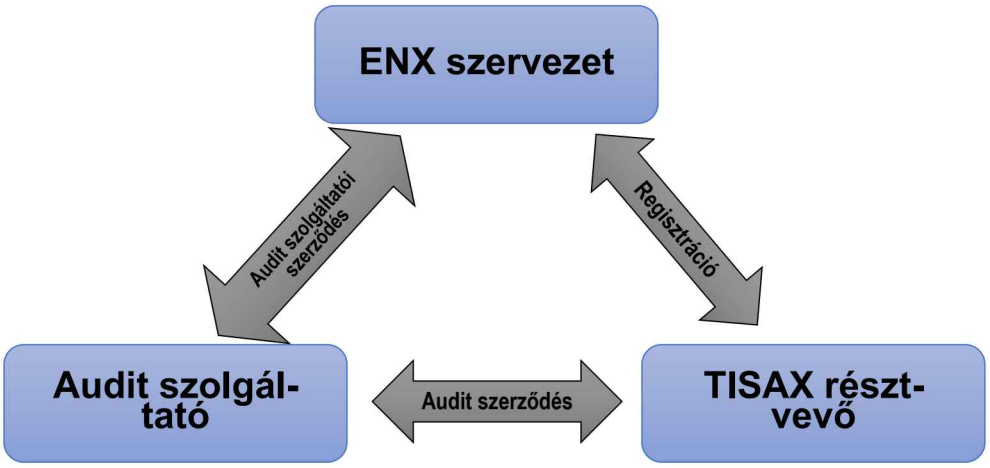
A TISAX rendszer működését az ENX szervezete tartja kézben és irányítja. A TISAX működési modellben alapvetően háromfajta szereplő létezik. Ezeket és ezek kapcsolatát az 1. sz. ábra mutatja be.

A TISAX folyamat alapvető szereplői:

- az **ENX szervezet** maga, aki az egész TISAX folyamatot irányítja, összefogja;
- az **Audit szolgáltatók**, akik az ENX által akkreditált tanúsító szervezetek, és akik szolgáltatásként a TISAX értékeléseket (auditokat) elvégzik;
- a **TISAX** résztvevők, akiknek be kell regisztrálni az ENX-hez, és akik
  - információbiztonsági irányítási rendszereiket auditáltatják, és az audit-eredményeit megosztják;
  - a beszállítóik audit-eredményeit igénylik.

A létrejött TISAX bevezetését, regisztrálását és egységes auditálását központilag az ENX (European Network Exchange) Association menedzseli, amely nemzetközi szervezetnek maga a VDA is egy tagszervezete. TISAX szerinti audit végrehajtására olyan tanúsító szervezetenek van joguk, amelyek erre szerződést kötnek az ENX-szel és teljesítik az ENX-nek a TISAX auditálási (értékelési) követelményrendszerét.

Azok a szervezetek (autóipari beszállítók), amelyek információbiztonsági irányítási rendszerük TISAX szerinti megfelelését igazolni szeretnék, azoknak be kell regisztrálniuk az ENX szervezethez, majd az egyik ENX által akkreditált TISAX auditszolgáltatóval szerződést kötve végre kell hajtaniuk az auditot. A sikeres audit befejeztével az eredményeiket regisztrálhatják az ENX adatbázisában, amelyhez való hozzáférést az általuk meghatározott mértékben megoszthatják a konkrét megrendelőikkel, vagy akár az ENX-hez regisztrált többi partnerrel és potenciális megrendelővel. Ezzel a TISAX szerinti megfelelőségük az ENX rendszerében nyilvántartott, és ez egy egységesen elfogadott követelményrendszer mindegyik (európai) autógyártó számára. Ez egyben jelentős idő és költség megtakarítást is jelent a beszállító szervezetek számára, az auditálás eredményeinek közös elfogadása által.




*1. ábra: A TISAX folyamat szereplői*

Innen látszik, hogy a TISAX résztvevők két csoportra oszthatók. Ezeket hívjuk aktív és passzív résztvevőknek, a következők szerint:

- **Aktív résztvevő** az, aki az értékelés (audit) tárgyát képezi, és ő kapja meg az auditja eredményeit, és ő osztja meg az ENX felületen a TISAX audit-eredményeit (a megrendelői fele);
- **Passzív résztvevő** az, aki az audit-eredményeket lekéri és használja (a szállítóitól);

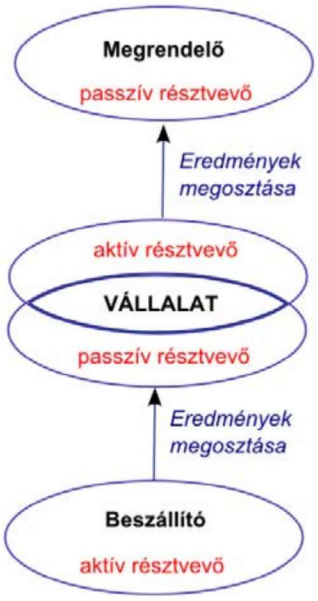
Minden résztvevőnek regisztrálnia kell az ENX-hez.

Egy résztvevő a beszállítói láncban lehet egyszerre aktív (a megrendelője fele) és passzív (a szállítója fele) résztvevő is. Ezt a kapcsolatot mutatja be a 2. sz. ábra.

Egy beszállító számára, aki a TISAX szerinti megfelelését igazolni szeretné és ezt már eldöntötte, a TISAX folyamat a következő lépésekre bontható:

### 1. Regisztráció

- Az ENX szervezethez tartozó regisztráció.
- El kell dönteni az értékelés (audit) hatókörét, célját, szintjét.
- A szervezet itt kapja meg az értékelési (audit) folyamatának az azonosítóját.




*2. sz. ábra: Aktív és passzív résztvevői szerepek a TISAX folyamatban*

### 2. Értékelés (audit)

#### *A. Felkészülés az értékelésre (önértékelés)*

- Az információbiztonsági irányítási rendszer kialakítása.
- Az önértékelés végrehajtása a VDA-ISA csekklista alapján.
- Az információbiztonság fejlesztése a hiányok kijavítására.

- Auditra felkészült, ha már elérte a csekklista szerinti kell-állapotot.
- Ez a szakasz a leghosszabb, és ez igényli a legtöbb külső és belső erőforrás befektetését.

### *B. TISAX Audit-szolgáltató kiválasztása*

- Csak ENX által regisztrált TISAX Audit-szolgáltató választható.
- Csak ENX-hez regisztrált résztvevő auditálható, ha már kész az önértékelése, amely alapján megfelel a követelményrendszernek.

### *C. TISAX értékelés (audit) végrehajtása*

- TISAX Audit-szolgáltató elvégzi az értékelési folyamatot a kívánt értékelési szinten.
- A TISAX értékelési (audit) folyamat szakaszai:
  a) ***„TISAX kezdeti értékelés”*** folyamata, a végén TISAX értékelési jelentés készül;
  b) Nem-megfelelések javítására az auditált szervezet intézkedési tervet készít, amelyet a TISAX audit-szolgáltató ***„Intézkedési terv értékelése”*** c. audit keretében felülvizsgál.
  c) Az auditált szervezet az elfogadott intézkedési terveket végrehajtja, majd azt követően a TISAX audit-szolgáltató ***„Követő értékelés”*** keretében auditálja annak megfelelését.

A b) és a c) szakaszok addig ismétlődnek, amíg van nem-megfelelés. Erre a TISAX kezdeti audit befejezését követően 9 hónap áll rendelkezésre. Ha az alatt nem sikerül az összes nem-megfelelést megszüntetni, akkor a TISAX audit eredménytelenül zárul le. A további felülvizsgálatok már csak új audit folyamat keretében végezhetők.

- A sikeres TISAX auditot követően a TISAX audit-szolgáltató lezárja a TISAX értékelési jelentést, amelyben már a TISAX megfelelést igazolja.

### 3. Az eredmények megosztása / publikálása

- A TISAX értékelési jelentés és a „TISAX címkék” (megfelelés igazolása) felkerülnek az ENX megosztási felületre.
- Az eredményeket a szervezet megoszt(hat)ja, csak a regisztrált résztvevők között.

A TISAX regisztráció során meg kell határozni a majdani TISAX audit hatókörét, célját és szintjét. Ezek a következőket jelentik:

**A TISAX szkóp (hatókör):**

- Az auditálás folyamata erre terjed ki – a TISAX audit-eredmény erre lesz érvényes.
- Tartalmazza
  1. A cégnevet,
  2. a telephelyeket (telephelyenként kapcsolódó adatokkal: cím, ágazati besorolás, telephelyi védelem, alkalmazotti létszám (azon belül létszám az IT / IT-biztonság / telephely védelem területein), kontaktszemély és elérhetőségei);
  3. meglévő tanúsítványok (ha vannak),
- Az értékelési hatókör szintjét, ami lehet sztenderd, bővített vagy szűkített. (Javasolt a sztenderd szint.)

**Az értékelés (audit) célja:**

- Ez választható 10 definiált cél közül, attól függően, hogy a beszállító szervezet milyen jellegű és bizalmasságú ügyfél adatokat kezel. Ennek megválasztását célszerű a megrendelő igényeihez igazítani.

- Ezek lehetnek:
  1. Magas védelmi igényű információk
  2. Nagyon magas védelmi igényű információk
  3. Csatlakozás magas védelmi igényű harmadik felekhez
  4. Csatlakozás nagyon magas védelmi igényű harmadik felekhez
  5. Adatvédelem
     Az európai általános adatvédelmi rendelet (GDPR) 28. cikke („Adatfeldolgozó") szerint
  6. Adatvédelem a személyes adatok különleges kategóriáival
     A 28. cikk („Adatfeldolgozó") szerint a személyes adatok különleges kategóriáival, az európai általános adatvédelmi rendelet (GDPR) 9. cikkében meghatározottak szerint.
  7. Prototípus komponensek és alkatrészek védelme
  8. A jármű prototípus védelme
  9. Tesztjárművek kezelése
  10. Prototípusok védelme rendezvények, film- vagy fotózás közben

**Az értékelési (auditálási) szint**

- Három TISAX értékelési szint lehetséges.
- Célszerű a megrendelővel is előre egyeztetni, hogy milyen szintű értékelést fogad el. Az egyes értékelési célok már meghatározzák a hozzájuk tartozó minimális értékelési szintet.
- Az egyes TISAX értékelési szintek (AL1…AL3):
  1. Értékelési szint (AL1 – Assessment Level 1): csak a szervezet 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, alapvetően dokumentáció-értékelés és távaudit módszerével, helyszíni vizsgálat csak szükség esetén.
  3. Értékelési szint (AL3 – Assessment Level 3): teljes és részletes helyszíni audit folyamat, a bizonyítékok ellenőrzésével és interjúkkal lefolytatva.

# 4. A TISAX követelményei [3, 4]

A TISAX szerinti információbiztonsági irányítási rendszer kialakításának elsődleges célja az autóipari gyártók / megrendelők adatainak biztonsága, azon belül is kiemelten a bizalmassága. Ugyan a TISAX követelményei foglalkoznak az információk rendelkezésre állásának és sértetlenségének követelményeivel is, de mint láttuk, az autóiparon belül az IATF ezekre már eleve szigorú követelményeket határozott meg.

A TISAX által védendő adatok elsődlegesen a megrendelők adatai, amelyek lehetnek például a szerződéses-rendeléses adatok, pénzügyi, szállítási adatok, műszaki specifikációk, tervrajzok, azokhoz kapcsolódó mérési ered-

mények, termelési – technológiai adatok, prototípus adatok ill. alkatrészek adatai, személyes adatok, stb.

Ezen adatok biztonságát mindenütt védeni kell, ahol ezek előfordulhatnak: papíralapú dokumentációkban és feljegyzésekben, de a különböző informatikai rendszerekben is. Az ezeket az adatokat tartalmazó informatikai rendszerek is sokfélék lehetnek, mint pl. termelési irányító és karbantartási programok, termelési tervező programok, ERP rendszerek, könyvelési programok, személyes adatokat kezelő programok, marketing / értékesítési programok, stb.

A TISAX szerinti információbiztonsági irányítási rendszer követelményeit az ENX szervezet publikussá tette. Ezt a követelményrendszert tartalmazza Excel formátumban a **VDA ISA** (Information Security Assessment) kérdőív, csekklista [3], ami szabadon letölthető az internetről. Ez a csekklista képezi az alapját mind a TISAX rendszer felkészülésének, a vállalati önértékelési folyamatnak, valamint az ENX által akkreditált TISAX audit-szolgáltatók értékelési (auditálási) követelményeinek is.
A TISAX követelményrendszere számos információbiztonsági folyamat megvalósítását írja elő, amelyeket adott célok érdekében a folyamatokhoz meghatározott kontroll-intézkedések alkalmazásával kell teljesíteni oly módon, hogy az adott folyamatok érettségi szintje az előírt szintet elérje. Ehhez bevezetett egy ötszintű folyamat-érettségi modellt.
Ennek a folyamat-érettségi modellnek a rövid egyszerűsített értelmezése a következő:

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

A VDA ISA Excel fájl a négy munkalapon tartalmazza a kitöltendő önértékelési csekklistákat. A négy munkalap a különböző auditcélok esetén kitöltendő. Ezek a következők:

- Információbiztonság. (Ez az alap csekklista, kitöltése minden esetben kötelező.)
- Csatlakozás 3-ik felekhez. (Opcionális, csak a megfelelő auditcél esetén kitöltendő.)
- Adatvédelem. (Opcionális, csak a megfelelő auditcél esetén kitöltendő.)
- Prototípus védelem. (Opcionális, csak a megfelelő auditcél esetén kitöltendő.)

Az egyes munkalapokon található kérdőívek tartalmazzák a megvalósítandó követelményeket, és ott a megfelelő mezők kitöltésével kell az önértékelést elvégezni és a megfelelő eredményeket és az eredményeket igazoló bizonyítékokat (vagy azok meghivatkozását) felvezetni.

A követelményrendszer alapját – különösen az Információbiztonság c. munkalapon – az

ISO/IEC 27001:2013 szabvány követelmény-struktúrája adta. A követelmények mennyiségére már abból is lehet következtetni, hogy a TISAX követelményrendszerben összesen értékelendő folyamatok száma 82. (Ez témakörönként: információbiztonság – 52 db, Csatlakozás 3-ik félhez – 4db, Adatvédelem – 4 db, Prototípus védelem – 22 db folyamatot jelent.) Minden egyes folyamathoz több kontroll előírt, amelyek számossága folyamatonként 2- 10 közötti.

A TISAX szerinti megfeleléshez szükséges minden értelmezhető információbiztonsági folyamat megvalósítása az elvárt érettségi szinten, az adott cél megvalósításához (legalább) a felsorolt kontrolloknak – mint követelményeknek – kell megfelelően működniük.

# 5. Összefoglalás

Az autóipari beszállítói követelményrendszerek már eddig is nagyon szigorú minőségbiztosítási követelményei mellett az információbiztonsági követelmények is egyre nagyobb jelentőséget kapnak. Az információk biztonságának, azaz az információk bizalmassága, rendelkezésre állása és sértetlensége több szempontból is kiemelten fontos szerepet játszik, mind szempontjából az információszolgáltatás folyamatossága és megbízhatósága a folyamatok működtetése szempontjából, mind az információk bizalmas jellegének megőrzése szempontjából.

Már az IATF követelményrendszere is – a minőségirányítási rendszer részeként – számos információbiztonsági követelményt tartalmaz, amelyek elsődleges célja a termelés és a folyamatok működtetésének és megfelelésének fenntartása. A megrendelői (OEM) adatok bizalmasságának megőrzésére a VDA egy új követelményrendszert dolgozott ki. Ez a TISAX, amely egy ISO/IEC 27001 alapú, de annál lényegesen részletesebb és szigorúbb követelményrendszer alapú információbiztonsági irányítási rendszer bevezetését és hatékony működtetését írja elő az autóipari beszállítóknak.

# 6. Felhasznált források

[1] IATF 16949:2016 Quality system management requirements for automotive production and relevant service parts organizations
[2] IATF 16949:2016 – Sanctioned Interpretations, https://www.iatfglobaloversight.org/wp/wp-content/uploads/2019/10/IATF-16949-SIs_Oct2019-1.pdf
[3] TISAX Participant Handbook, Date: 2019-05-20. Version: 2.1., ENX doc ID: 602, https://portal.enx.com/tphen.pdf
[4] Information Security Assessment (ISA) of the Verband der Automobilindustrie (Association of the German Automotive Industry, VDA). Date: 2019-05-09. Version: 4-1-1, https://www.vda.de/en/services/Publications/information-security-assessment.html

**Dr. Horváth Zsolt**

Az INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft. társtulajdonosa és ügyvezetője 2006 óta. EOQ MNB által regisztrált minőségirányítási és információbiztonsági rendszermenedzser és auditor. Tíz évig látta el a SIEMENS magyarországi szoftverházának, a SIEMENS PSE Kft-nek a minőségirányítási igazgatói feladatait. Több, mint húsz éve dolgozik a minőségirányítás és az információbiztonsági irányítás területén, több akkreditált tanúsító szervezet vezető auditoraként, valamint tanácsadóként és szakmai oktatóként. Számos szakmai konferencián elhangzott előadás és megjelent publikáció szerzője és társszerzője.