„Információvédelem menedzselése”
CXIX. Szakmai Fórum
Budapest, 2026. január 21.

AI kockázatok szabványokban

Móricz Pál
vezető tanácsadó, ügyvezető igazgató
Szenzor Gazdaságmérnöki Kft.

Szenzor
GAZDASÁGMÉRNÖKI KFT.

Kockázat fogalma

- *„A bizonytalanság hatása a célok elérésére” (ISO 31000:2018)*
  - lehet pozitív és negatív
- Nem statikus fogalom
  - egy-egy kockázat változhat
  - változik, mik a kockázatok

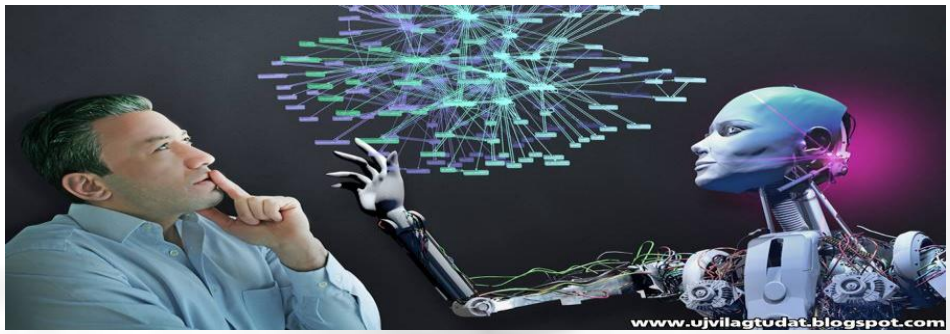
Kockázatkezelés

- Ismert tevékenység esetén
  - kockázatok többnyire ismertek
  - kezelésük kialakult
  - negatív kockázatokra (kötelező) jogszabályok, útmutató standardok (ezek sem statikusak…)
- Új eszközök
  - új (még nem ismert, nem kezelt) kockázatok
    - megismerés során lehet ezeket azonosítani, illetve
    - alakulnak ki a válaszintézkedések
  - jó/bevált gyakorlatok elterjesztésére új szabványok (AI szabványcunami is indult)

NIS2/Kiberbizttv, 27001 – AI risk

- formálisan nem szerepel bennük AI, de
- a kockázatfelmérés, kezelés követelmény, van/lehet AI-hoz kapcsolódó kockázat
- érinthet kontrollokat, pl.:
  - adat/információ, EIR osztályozás, kezelés,
  - fenyegetés feltárás, sebezhetőség kezelés,
  - biztonság a felhőszolgáltatásokban,
  - hozzáféréskezelés, adatkiszivárgás,
  - naplózás, monitoring,
  - fejlesztés, változáskezelés,
  - elfogadás, engedélyezés, stb.

AI Act



- **AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/1689 RENDELETE** 2024.06.13
- a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (AI Act)
- Kockázattól függő szabályok
- Hatályba lép 2026.08.02,
  de jártasság (fejlesztő, használó) és tiltott AI rendszerek követelmények már 2025.02.02

AI Act - tárgy

a) szabályok az Unión belüli forgalomba hozatalra, üzembe helyezésre és használatra
b) bizonyos MI-gyakorlatokra vonatkozó tilalmak
c) a nagy kockázatú MI-rendszerekre vonatkozó különös követelmények és az ilyen rendszerek üzemeltetőire vonatkozó kötelezettségek
d) bizonyos MI-rendszerekre vonatkozó harmonizált átláthatósági szabályok
e) az általános célú MI-modellek forgalomba hozatalára vonatkozó harmonizált szabályok
f) szabályok a piaci nyomon követésre, a piacfelügyeletre, az irányításra és a végrehajtásra
g) innovációt támogató intézkedések, különösen a kkv-kra összpontosítva, ideértve az induló innovatív vállalkozásokat is.

ISO/IEC 23894:2023

- **MSZ ISO/IEC 23894:2025 Informatika. Mesterséges intelligencia. Útmutató a kockázatmenedzsmenthez** (angol nyelvű, magyar fedőlappal)
- ISO 31000:2018 Kockázatmenedzsment szabvány adaptálása AI-ra, fejlesztőknek, felhasználóknak
  - AI kockázatmenedzsment alapelvek
  - Keretrendszer (vezetés, elkötelezettség, integrálás, tervezés, bevezetés, kiértékelés, fejlesztés)
  - Kockázatmenedzsment folyamatok (kommunikáció és konzultáció, scope, kontexusok, kritérium, felmérés, kezelés, jelentés és átvizsgálás)
  - A melléklet: Célok (átláthatóság, AI szakértelem, képzés és teszt adat elérhetőség, minőség, környezeti hatás, tisztesség/pártatlanság)

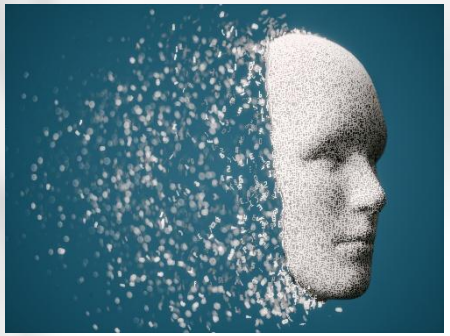
ISO/IEC 42001:2023

- **MSZ ISO/IEC 42001:2024 Informatika. Mesterséges intelligencia. Irányítási rendszer**
- Menedzsment szabvány struktúra (4-10 fejezet)
  - Kontexusok, vezetés, tervezés, támogatás, működtetés, figyelemmel kísérés, fejlesztés
  - Tervezés és működtetés fejezetekben kockázat felmérés, kezelés mellett AI hatás felmérés is
  - Mellékletek

    A. Kontroll lista (A2-A10 fejezet, 38 kontroll) indoklással lehet kizárás, SoA

    B. Bevezetési útmutató

    C. Lehetséges célkitűzések és kockázati források
  - D. Az AI menedzsment rendszer használata területekre, ágazatokra



Kontroll fejezetek

A.2. AI-ra vonatkozó irányelvek
A.3. Belső szervezet
A.4. Erőforrások az AI rendszerhez
A.5. Az AI rendszer hatásainak felmérése
A.6. Az AI rendszer életciklusa
A.6.1 Menedzsment útmutató az AI rendszer fejlesztéséhez
A.6.2 Az AI rendszer életciklusa
A.7. Az AI rendszer adatai
A.8. Információk az AI rendszer érdekelt felei számára
A.9. Az AI rendszer használata
A.10. Harmadik fél és vevő kapcsolatok

C melléklet

- AI-hoz kapcsolódó lehetséges célkitűzések és kockázati források
- Célkitűzések:
  - Elszámoltathatóság, AI szakértelem, rendelkezésre állás, képzés, minőség, tesztadatok, környezeti hatás, méltányosság, karbantarthatóság, magánélet védelme, robusztusság, biztonság, védelem
- Kockázat források:
  - környezet komplexitás, átláthatóság, magyarázhatóság, automatizálási szint, gépi tanuláshoz kapcsolódó kockázatforrások, rendszer hardver életciklus események, technológiai felkészültség

ISO/IEC 42005:2024 (1/2)

MSZ ISO/IEC 42005:2025 Informatika. Mesterséges intelligencia (AI). AI rendszerek hatásvizsgálata
(angol nyelvű, magyar fedőlappal)

4. AI rendszer hatásvizsgálati folyamat bevezetés

- *folyamat dokumentálás, szervezetbe integrálás, időütemezés, scope meghat., erőforrás allokálás, küszöbértékek, végrehajtás, eredmények elemzés, jelentés, jóváhagyás, monitoring és átvizsgálás*

5. Dokumentálás

- *scope, AI rendszer információk (leírás, funkciók, célok, tervezett és nemtervezett használat),*
- *adat információk és minőség (dokumentálás is),*

ISO/IEC 42005:2024 (2/2)

5 Dokumentálás (folytatás):

- *algoritmus és modell információk (szervezet általi, illetve fejlesztési algoritmus, AI-ban használt modell és modell fejlesztési információk),*
- *környezet (földrajzi, nyelvi, komplexitás és korlázok),*
- *érdekelt/érintett felek,*
- *aktuális és lehetséges hatások (előny/károk, visszaélés, bántalmazás),*
- *szabályozás előnyökre, károkra*

C melléklet: Harm and benefit taxonomy (tbl.)

E melléklet: Examle templates

ISO/IEC DIS 27090 (2025.04)

Kiberbiztonság. AI. Útmutató az AI rendszerekben lévő biztonsági fenyegetések és hibák kezeléséhez

5. Az információbiztonság alkalmazása

6. Az AI-t fenyegető veszélyek

7 Kockázatcsökkentő intézkedések és azok kölcsönhatása a fenyegetésekkel és más kockázatcsökkentő intézkedésekkel

Annex A. Mapping attacs to AI systems life cycle and to assets

Annex B. AI specific versions of conventional attacs

Elérhetőség

Móricz Pál **Mobil: 20-931-0584**

p.moricz@szenzor-gm.hu

Szenzor Gazdaságmérnöki Kft.

1087 Budapest, Könyves Kálmán körút 76.

Telefon: (+36)-1-331-5523

E-mail: szenzor@szenzor-gm.hu

Honlap: www.szenzor-gm.hu

„Változással a sikerért”