HÉTPECSÉT INFORMÁCIÓBIZTONSÁGI EGYESÜLET •
INFORMÁCIÓVÉDELEM MENEDZSELÉSE SZAKMAI FÓRUM

„AI GOVERNANCE GAP”

Amikor a DPO, a CAIO és a kockázatkezelés felelősségi körei nem fedik le egymást

Dalos-Kovács Gabriella

AI Officer as a Service • AI governance • AI stratégia • digitális transzformáció • ISO/IEC 42001 auditor • AI-kockázatkezelési szakértő (ISO/IEC 23894)

2026. szeptember 16. • Óbudai Egyetem, Budapest

SHADOW AI A SZÁMOKBAN

A GAP NEM ELMÉLET: FRISS MAGYAR ADATOK

TÖBB LEHETŐSÉG.
NAGYOBB FELELŐSSÉG.
TISZTÁBB DÖNTÉSEK.

85,9%

a felsővezetők ekkora hányada használ nem vállalati AI-eszközt munkára

Minél magasabb a beosztás, annál nagyobb az arány – a példamutatás ma fordítva működik.

66,9% a munkára AI-t használók nem vállalati eszközt is használnak

65,7% a szellemi munkát végzők AI-kontroll nélküli vagy saját eszközökre épülő környezetben dolgoznak

77,4% legalább 10% időmegtakarításról számol be

Fő érzékelt kockázatok:

hallucináció és téves döntés (55,3%) · érzékeny adat kiszivárgása (42,8%) · függőség és készségvesztés (30,7%)

És amit a kontroll környezet nem lát:

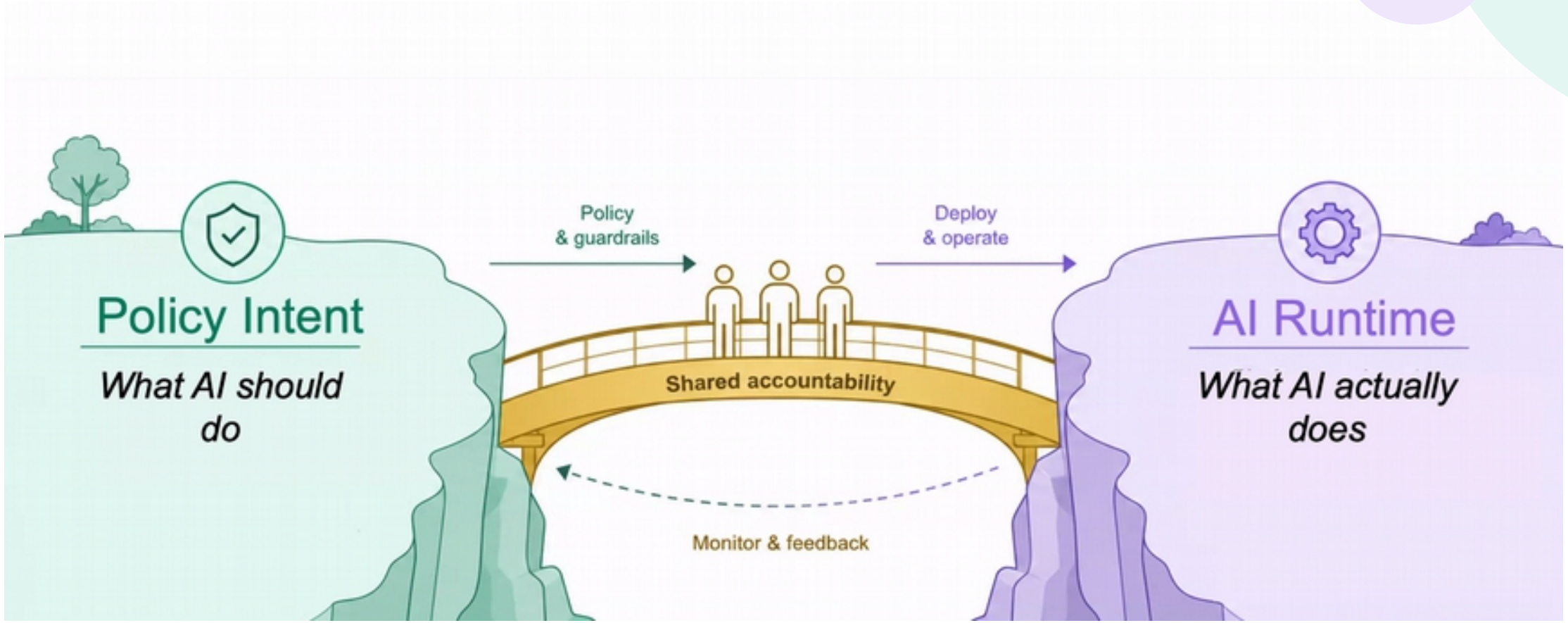
Csak 22,2% ismeri jól a belső irányelvet · az anonimizálók 27,1%-a nem teljes körűen vagy nem következetesen értelmezi az anonimizálást · bizonytalanság esetén csak 14,2% kér illetékes segítséget

Az AI-használat és az érzékelt produktivitási előny gyorsabban terjed, mint a szervezeti kontroll. Ez a governance gap – számokban.

Forrás: PwC Magyarország, 2026-os hazai AI-kutatás, N=2 896; a 18+ online vásárló internetezők körében nem, kor és lakóhely településtípusa szerint reprezentatív minta. Saját másodelemzés.

A RÉS, AMIRŐL MA BESZÉLÜNK

AZ AI GOVERNANCE GAP



A gap a szándék (amit az AI-nak tennie kellene) és a futásidejű valóság (amit ténylegesen csinál) között nyílik - és szervezeti kérdés, nem technológiai.

Ábra forrása: OneTrust - The new operating model for AI governance

FOGALOM

MIT JELENT AZ AI GOVERNANCE A GYAKORLATBAN?

Az AI governance azt határozza meg: a szervezetben ki, milyen AI-t, milyen célból, milyen adatokkal, milyen kockázatok mellett, milyen jóváhagyással és ellenőrzés alatt használhat.

01

Döntési jogkörök

Ki dönt, miről, milyen jóváhagyási kapuknál

02

Felelősségek

Minden AI rendszernek kijelölt gazdája van

03

Kontrollok

Működő, bizonyítható ellenőrzés - nem papíron

Az AI teljes életciklusán: Ötlet → Bevezetés → Használat → Monitoring → Kivezetés

Nem dokumentum a fiókban.
A napi működés része: a folyamatokba építve követik.

Integráció - nem új siló.
A meglévő rendszerekre épül: ISMS, kockázatkezelés, GDPR, audit.

A SZEREPLŐK

ÖT MANDÁTUM - ÉS AMI A FÖLDRE ESHET

DPO	CISO	CAIO	Kockázatkezelés	Üzleti döntéshozó
MANDÁTUM Személyes adatok, GDPR, érintetti jogok	**MANDÁTUM** Bizalmasság, sértetlenség, rendelkezésre állás	**MANDÁTUM** AI stratégia, use case portfólió, érték	**MANDÁTUM** Vállalati kockázati keretrendszer, riportok	**MANDÁTUM** Use case gazda: cél, haszon, erőforrás
VAKFOLT Nem személyes adatokhoz kötődő AI-kockázatok, modell minőség, üzleti hatás	**VAKFOLT** AI-kimenet helyes-e torzítás, üzleti megfelelőség, modell teljesítménye	**VAKFOLT** A független kontroll és assurance nem lehet kizárólag nála.	**VAKFOLT** AI-specifikus kockázati módszertan és mérőszámok nem feltétlenül adottak	**VAKFOLT** Elszámoltatható az eredményért és kockázatért – de a kontrollok más funkcióknál van

Ki az AI-kockázat gazdája? Ki kezeli az AI-incidenst? Ki dönt, ha a jogi, biztonsági és üzleti szempontok ütköznek?

A GAP TÉRKÉP.

ÖT TERÜLET, AHOL A HAGYOMÁNYOS FELELŐSSÉGI KÖRÖK KÖZÖTT RÉS MARAD

1 AI rendszerek kockázatelemzése	Az adatvédelem a személyes adatok kockázatait, az enterprise risk a vállalati kockázatokat kezeli – az AI-specifikus kockázatoknak külön módszertan és felelős kell.
2 AI incidens kezelése	Hallucinált ügyfélválasz: minőségi esemény, AI-incidens, adatvédelmi vagy biztonsági incidens? Ki triázsolja, ki eszkalálja, ki dönt a leállításról?
3 Vendor és beszerzési gate	Ki világítja át AI szempontból a beszállítót és az AI funkciót tartalmazó szoftvert a beszerzés előtt?
4 Shadow AI felderítése és kezelése	66,9% használ privát eszközt - a felderítés eszköz (CISO), a kezelés viszont szabályozási és kulturális kérdés.
5 AI képzés és AI literacy	Ki határozza meg, kinek milyen AI literacy-szintre van szüksége – és ki bizonyítja, hogy ez megtörtént?

Ahol nincs kijelölt felelős, ott a döntés eseti, a kontroll következetlen, az auditnyom pedig nehezen igazolható.

A GOVERNANCE KERETRENDSZER

AZ AI GOVERNANCE HÉT TERÜLETE

O — Oktatás és tudatosítás

Szerepkör-alapú tudás, képzés, tudatosság

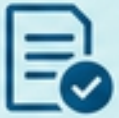
A — Adat governance

Adatminőség, eredet, integritás, hozzáférés és adat-életciklus

R — Kockázat és biztonság

AI-kockázat- és hatásértékelés, safety/security, kockázatkezelés

S — Megfelelőség, assurance és fejlesztés



AI Act, szabályzatok, dokumentáció, audit, mérés, incidens, folyamatos fejlesztés

F — AI-életciklus és működési kontrollok

Nyilvántartás, beszerzés, fejlesztés, tesztelés, human oversight, monitoring

S — Stratégia és vezetés

AI célok, use case portfólió, üzleti érték, kockázati étvágy

O — Ownership, accountability

AI owner és AI officer. Szerepek, felelősségek, döntési jogok, eszkaláció

A hét terület együtt fedi le mindazt, amit az AI governance-nek irányítania kell.

A MEGOLDÁS: DÖNTÉSI RENDSZER, NEM DOKUMENTUM

AI GOVERNANCE BOARD ÉS AI OFFICE

AI GOVERNANCE BOARD - dönt

- Vezetői szintű döntéshozó fórum, rendszeres ritmusban
- Tagjai: üzlet, CAIO, DPO, CISO, kockázatkezelés, jog, adat, IT
- Dönt: use case jóváhagyás, kockázati étvágy, prioritások, kivételek, eszkalációk
- Kimenete: döntésnapló, feltételek, kijelölt felelősök

AI OFFICE - működtet

- Állandó operatív funkció az AI vezető irányításával
- Működteti: AI Registry, use case intake, kontrollok, szabályzatok
- Multidiszciplináris csapat: DPO, CISO, jog, adat, HR, üzlet - itt zárulnak a rések
- Előkészíti a Board döntéseit: riportok, KPI

A Board dönt, az Office működtet. A négy szerep közös döntési és működési keretet kap - és az AI governance a meglévő vállalatirányítási struktúrába illeszkedik, nem mellé épül.

A KULCSSZEREPLŐ

AZ AI OFFICER: AKI A RENDSZERT NAPI SZINTEN VISZI

MI EZ A SZEREP?

- A szervezet AI működésének felhatalmazott felelőse
- Nem technológiai szerep: üzleti, jogi, biztonsági és adat szempontok
- Az AI Office-t vezeti, a Boardnak riportál
- Fractional: induláskor részidős vagy külső is - a mandátum a lényeg

MIT CSINÁL?

- AI stratégia és governance roadmap karbantartása
- AI Registry és use case portfólió működtetése
- Use case-ek érték-, kockázati és megfelelőségi értékelése
- EU AI Act és ISO/IEC 42001 felkészülés koordinálása
- Kivételek, incidensek, hiányzó kontrollok eszkalálása
- Vezetői riportok: KPI, kockázat, értékrealizáció
- AI literacy program és szabályzat kommunikáció
- A DPO, CISO, jog, adat, HR és üzlet összehangolása

Mandátum nélkül az AI Officer csak tanácsadó. Hatáskör, döntési fórum és eszkalációs út kell mellé - ezt a Board adja meg.

Benchmark: a szervezetek 76%-a nevezett ki Chief AI Officert, egy éve még 26% (IBM IBV CEO Study, 2026)

AZ ESZKÖZ

FELELŐSSÉGI MÁTRIX A KULCSDÖNTÉSEKRE - MINTA

Döntés	DPO	CISO	CAIO	Kockázat-kezelés	Üzleti terület
Use case befogadás és jóváhagyás	C	C	**A**	C	R
AI rendszer kockázatelemzése	C	C	C	**A**	R
Személyes adat AI feldolgozása	**A**	C	C	I	R
AI incidens kezelése	C	**A**	I	C	R
Vendor és beszerzési gate	C	C	**A**	C	R
AI képzés és AI literacy	I	C	**A**	I	R

A = elszámoltatható (döntéshozó) • R = végrehajtó • C = konzultált • I = informált

Nem a betűk pontos helye a lényeg, hanem hogy minden sorban pontosan egy „A” legyen - és az működjön is.

A LÉNYEG

ÖT RÉS - ÖT ZÁRÓ MECHANIZMUS

1	**AI rendszerek kockázatelemzése**	**Kockázatkezelés**	Kockázatbesorolási folyamat minden use case-re, a RACI-ban rögzített felelőssel - a use case gazda közreműködésével.
2	**AI incidens kezelése**	**CISO**	AI incidens típusok és besorolási szabály a meglévő incidenskezelési folyamatba építve - nem új, párhuzamos folyamat.
3	**Vendor és beszerzési gate**	**CAIO + Board**	AI szempontú átvilágítási kapu a beszerzésben, az AI Registry-hez kötve - enélkül nincs jóváhagyás.
4	**Shadow AI**	**AI Office**	Becsatornázás, nem büntetés: intake csatorna, engedélyezett eszközlista, a meglévő használat felmérése és rendezése.
5	**AI képzés és AI literacy**	**CAIO + HR**	Szerepkör szerinti AI literacy program (EU AI Act 4. cikk) - a részvétel és a hatás KPI-ként mérve.

Minden réshez egy gazda, egy folyamat és egy bizonyíték - nem újabb pozíció, hanem működő rendszer.

AZ INDULÁS

HOGYAN ÉRDEMES ELINDULNI

0-30 nap
Azonnali kockázatcsökkentés

- AI használat felmérése - a Shadow AI-val együtt
- AI Registry indítása a meglévő rendszerekre
- Azonnali szabály a kritikus adatkörökre

31-90 nap
Governance alapok

- Felelősségi mátrix és döntési jogok rögzítése
- Board, AI Office és AI Officer mandátum kialakítása
- Use case intake és kockázati besorolás
- Szabályzat kommunikáció és alapszintű képzés

3-12 hónap
Beépítés és mérés

- Kontrollok beépítése a működő 27001 rendszerbe
- ISO/IEC 42001 gap assessment és ütemterv
- KPI, incidens és értékrealizációs riport

A sorrend nem véletlen: előbb látni kell, mi fut a szervezetben - csak utána lehet felelősen dönteni róla.

Ahol a szerepkörök nem versengenek – hanem strukturáltan dolgoznak együtt.

A felelősségi rés nem újabb pozícióval, hanem működő irányítási rendszerrel zárható – döntési jogokkal, felelősségi mátrixszal, bizonyítható kontrollokkal.

Köszönöm a figyelmet!

Dalos-Kovács Gabriella • AI officer as a service • AI governance szakértő • ISO/IEC 42001 auditor • AI-kockázatkezelési szakértő (ISO/IEC 23894)

gabi@dalos.hu • linkedin.com/in/daloskovacsgabriella

Backup slides

KIEGÉSZÍTŐ ANYAG

AI FENYEGETÉSI LISTA INFOBIZTONSÁGI SZEMMEL

1

Prompt injection

Manipulált bemenet veszi át az irányítást

2

Adatszivárgás prompton át

Érzékeny adat kerül külső modellbe

3

Tanítóadat mérgezés

Fertőzött adat rontja a modellt

4

Modell lopás, kinyerés

Üzleti tudás és IP szivárgása

5

Hallucináció

Meggyőző, de téves kimenet

6

AI ellátási lánc

Szolgáltató, API, adatfüggőségek

7

Deepfake, social engineering

AI-val támogatott megtévesztés

8

Túlzott autonómia

Felügyelet nélküli agent műveletek

A lista gyorsan változik - a karbantartása governance kérdés: ki értékeli, ki dönt a kontrollokról?

Kapcsolódó keretrendszerek: OWASP Top 10 for LLM Applications • MITRE ATLAS • NIST AI RMF

KIEGÉSZÍTŐ ANYAG

AI BIZTONSÁG A MEGLÉVŐ INFOBIZTONSÁGI TERÜLETEKEN

Meglévő infobiztonsági terület	AI kiterjesztés - ide kerül az AI security
Hozzáférés és identitás kezelés	AI eszközök, API kulcsok, szerepkör alapú jogosultságok
Adatbiztonság és DLP	Adatklasszifikáció, prompt és kimenet szűrés
Naplózás, SOC, monitoring	AI naplózás, Shadow AI felderítés, incidens detektálás
Beszállítói biztonság	Modell szolgáltatók és AI ellátási lánc átvilágítása
Biztonságtudatosság és képzés	AI literacy, biztonságos prompt gyakorlatok
Üzletmenet folytonosság	AI függőségek felmérése, kiesési tervek
Biztonsági eszközpark	AI guardrail, posture management, agentic gateway

Nem új keretrendszer kell: a meglévő biztonsági képességek terjeszthetők ki az AI-ra.

KIEGÉSZÍTŐ ANYAG

ISO/IEC 27001-RŐL ISO/IEC 42001-RE: NEM NULLÁRÓL INDUL

KÖZÖS ALAP - ÚJRAFELHASZNÁLHATÓ

- ✓ A működési környezet megértése
- ✓ Vezetői felelősség és szerepkörök
- ✓ Kockázatkezelési folyamat
- ✓ Erőforrások, kompetenciák, képzések
- ✓ Dokumentált működés és kontrollok
- ✓ Belső audit és vezetőségi átvizsgálás
- ✓ Eltéréskezelés, folyamatos fejlesztés

ÚJ KÉRDÉSEK - AI SPECIFIKUS

- Milyen szerepet tölt be a szervezet az AI értékláncban?
- Milyen hatással van az AI az érintettekre?
- Ki felel az AI rendszerekért?
- Hogyan történik az AI kockázatok és hatások értékelése?
- Milyen emberi felügyelet működik?
- Hogyan mérik az AI teljesítményét és üzleti értékét?

A 27001 megfelelés jó kiindulás - de önmagában még nem jelent felelős AI működést.

A GAP NEM ELMÉLET: FRISS MAGYAR ADATOK

85,9%

a FELSŐVEZETŐK ekkora hányada használ nem vállalati AI eszközt - <u>is</u> - munkára

Minél magasabb a beosztás, annál nagyobb az arány - a példamutatás ma fordítva működik.

66,9%	a munkára AI-t használók nem vállalati eszközt <u>is</u> használnak
65,7%	a szellemi munkát végzők AI-kontroll nélküli vagy saját eszközökre épülő környezetben dolgoznak
77,4%	legalább 10% időmegtakarításról számol be

Fő érzékelt kockázatok:

hallucináció és téves döntés (55,3%) • érzékeny adat kiszivárgása (42,8%) • függőség és készségvesztés (30,7%)

És amit a kontroll környezet nem lát:

Csak 22,2% ismeri jól a belső irányelvet •

az anonimizálók 27,1%-a nem teljes körűen vagy nem következetesen értelmezi az anonimizálást • bizonytalanság esetén csak 14,2% kér illetékes segítséget

Az AI-használat és az érzékelt produktivitási előny gyorsabban terjed, mint a szervezeti kontroll.

Ez a governance gap – számokban.

Forrás: PwC Magyarország, 2026-os hazai AI-kutatás, [illegible] és lakóhely településtípusa szerint reprezentatív minta. Saját másodelemzés.

A GOVERNANCE KERETRENDSZER

AZ AI GOVERNANCE HÉT TERÜLETE

O Oktatás és tudatosítás

Szerepkör-alapú tudás, képzés, tudatosság

A Adat governance

Adatminőség, eredet, integritás, hozzáférés és adat-életciklus

R Kockázat és biztonság

AI-kockázat- és hatás-értékelés, safety/security, kockázatkezelés

S Megfelelőség, assurance és fejlesztés

AI Act, szabályzatok, dokumentáció, audit, mérés, incidens, folyamatos fejlesztés

F AI-életciklus és működési kontrollok

Nyilvántartás, beszerzés, fejlesztés, tesztelés, human oversight, monitoring

S Stratégia és vezetés

AI célok, use case portfólió, üzleti érték, kockázati étvágy

O Ownership, accountability

AI owner és AI officer. Szerepek, felelősségek, döntési jogok, eszkaláció

A hét terület együtt fedi le mindazt, amit az AI governance-nek irányítania kell.

AI Irányítás: Szerepkörök, Mandátumok és Vakfoltok

Az AI bevezetése során öt kulcsszereplőnek van meghatározott felelősségi köre, azonban a mandátumok és a tényleges kontrollok között rés-rések alakulhatnak ki. Ez az infografika rávilágít arra, hogy ki miért felel, és mi az, ami „a földre eshet" (gazdátlanul maradhat) a folyamat során.

DPO
(Adatvédelmi tisztviselő)

Személyes adatok védelme

GDPR, érintetti jogok és a személyes adatok kezelésének felügyelete.

VAKFOLT

Nem személyes AI-kockázatok, üzleti hatás

A nem személyes adatok AI-kockázatai és a modellek torzítása gyakran kívül esik a fókuszon.

CISO
(Információbiztonsági vezető)

Technikai biztonság

Bizalmasság, integritás és az informatikai rendszerek védelme.

VAKFOLT

AI-kimenet torzítása, modell teljesítménye

Az AI-modellek specifikus biztonsági és teljesítménybeli kockázatai és a torzítás gyakran rejtve marad.

CAIO
(Mesterséges Intelligencia vezető)

AI-stratégia értékközpontú vezetése

AI stratégia, értékteremtés és az AI-kezdeményezések koordinálása.

VAKFOLT

A független kontroll nem lehet kizárólag nála

A kontroll és a módszertan függetlenségének biztosítása kritikus, különösen az AI-specifikus mérőszámok tülijányában.

Kockázatkezelés

Vállalati keretrendszerek biztosítása

Kockázatkezelési módszertanok és megfelelőségi keretek kidolgozása.

VAKFOLT

Kontroll és Módszertan hiánya

Az AI-specifikus mérőszámok és a független ellenőrzési folyamatok korlátozottsága rendszerszintű kockázatot jelent.

Üzleti döntéshozó

Konkrét üzleti use case-ek erőforrás-gazdálkodása

Az AI projektek üzleti céljainak meghatározása és az erőforrások allokálása.

VAKFOLT

Felelőssség vs. Kontroll ellentmondása

Az üzleti döntéshozó felel az eredményért, de a tényleges kontrollok gyakran más funkciókkhál vannak.

KULCSKÉRDÉSEK AZ AI-KOCKÁZAT GAZDÁJÁRÓL:

KI AZ AI-KOCKÁZAT GAZDÁJA? **KI KEZELI AZ AI-INCIDENST?** **KI DÖNT ÉRDEKÜTKÖZÉS ESETÉN?**