Risk in Focus
2025

Az összefoglalót készítette:
A BELSŐ ELLENŐRÖK MAGYARORSZÁGI KÖZHASZNÚ SZERVEZETE
(BEMSZ)
KOCKÁZATKEZELÉSI ÁLLANDÓ BIZOTTSÁGA

Belső Ellenőrök
Magyarországi
Közhasznú Szervezete

30 BEMSZ
ALAPÍTVA: 1992.

1. Bevezető

A Belső ellenőrök nemzetközi szervezete (The Institute of Internal Auditors - IIA) 2024-ben is felmérte a szervezeteket érintő kockázatokat, melynek eredményét a “Risk in Focus 2025”[1] című kiadványban jelentette meg. A kockázatok rangsorolását globálisan és földrészekre bontva is elvégezték. Miközben sok területen egyezés tapasztalható a kockázatok megítélésében, a belső ellenőrök véleményében érezhetők a földrajzi elhelyezkedésből vagy a gazdasági fejlettségből fakadó helyi eltérések.
Globálisan az öt legmagasabbra értékelt kockázat a 2025-ös évre vonatkozóan a(z):

1. kiber- és adatbiztonság,
2. üzletfolytonosság (működési biztonság, krízis menedzsment, katasztrófa kezelés),
3. humán tőke (diverzitás, tehetséggondozás, megtartás),
4. digitális átalakulás okozta zavarok, új technológia és mesterséges intelligencia, valamint a
5. jogszabályi környezet változása.

A lista nagy részben harmonizál az európai és a hazai megítéléssel azzal különbséggel, hogy kontinensünkön az üzletmenet-folytonosság helyett a geopolitikai bizonytalanság került be a Top 5 kockázatba, Magyarországon azonban mindkét kockázat magas prioritással bír.

Kiemelt kockázatok Európában

Európa nemcsak gazdaságilag néz nehéz év elé, hanem a vállalkozások ezen túl is erős szembeszélre számíthatnak, különösen ami a politikai bizonytalanságot, az éghajlatváltozással összefüggő feladatokat, a szabályozók oldaláról megnyilvánuló nyomást és a munkaerő változó demográfiai trendjeit illeti. Azonban az akadályok közül is kiemelkedik a digitális átalakulás okozta zavarok (elterjedt angol kifejezéssel: „*digital disruption*”). A mesterséges intelligencián alapuló eszközök legújabb generációja a technológiai versenyt és az irántuk mutatkozó piaci igényeket fő stratégiai fókusszá tette, ugyanakkor ez a változás óriási kockázatot is hordoz magában. Ahhoz, hogy versenyelőnyhöz jussanak, egyszerre kell a vállalkozásoknak adaptálniuk az új technológiákat és fenntartaniuk a stratégiai gondolkodást, beleértve a kockázatmenedzselési képességeket.

TOP-6 európai kockázat

1. Kiber- és adatbiztonság
2. Humán tőke (diverzitás, tehetséggondozás, megtartás)
3. Jogszabályi környezet változása
4. Digitális átalakulás okozta zavarok, új technológia és mesterséges intelligencia
5. Makroökonómiai és geopolitikai bizonytalanság
6. Éghajlatváltozás, biológiai sokféleség és környezeti fenntarthatóság

[1] https://www.eciia.eu/wp-content/uploads/2024/09/Risk-in-Focus-2025-FINAL.pdf

A kockázati területek közül a “Risk in Focus 2025” öt elemre külön is felhívja az európai belső ellenőrök figyelmét, függetlenül azok rangsorolásától:

- Digitális átalakulás okozta zavarok, új technológia és mesterséges intelligencia
- Kiber- és adatbiztonság
- Humán tőke, sokszínűség, tehetséggondozás és megtartás
- Makroökonómiai és geopolitikai bizonytalanságok
- Éghajlatváltozás, biológiai sokféleség és környezeti fenntarthatóság

DIGITÁLIS ÁTALAKULÁS OKOZTA ZAVAROK, ÚJ TECHNOLÓGIA ÉS MESTERSÉGES INTELLIGENCIA

E kockázati terület súlyosságának megítélése emelkedett a leggyorsabban a kiemelt területek között: míg egy évvel ezelőtt a 6. helyen említették a felmérésben résztvevők, idén már a 4. helyre sorolták és 2028-ra a 2. legnagyobb kockázatnak várják. A kockázatra adott válaszok új belső ellenőrzési stratégiát és készségeket is megkövetelnek. A mesterséges intelligencia (MI) alkalmazásától azt várják, hogy javítani fogja Európa gyengélkedő versenyképességét és új piacokat nyit meg számára. Ugyanakkor csak kevés vállalatnak van kiforrott digitalizációs / MI stratégiája és annak alkalmazását felügyelő/irányító folyamatai, továbbá a bevezetést megvalósító emberi erőforrása. Emellett növekvő kiber, adat, reputációs és etikai kockázattal is számolni kell az MI alkalmazásakor, itt megemlítve az Európán kívüli területekről származó kockázatokat és azt, hogy mivel az MI egyes verziói szabadon elérhetőek és ingyenesek, a vállalat különböző szintjein – ellenőrizetlenül – használhatják. Fennállhat a veszélye annak is, hogy amennyiben helytelen adatforrásokra támaszkodik az MI, akkor a végeredmény is pontatlan lesz, ezért minden MI-vel készített dokumentum értelmezésénél fontos a – Globális Belső Ellenőrzési Normákba újonnan beemelt – szakmai szkepticizmus. A témában érdeklődők számára hasznos forrás lehet az MI belső ellenőrzés szempontjából történő megközelítést közreadó angol nyelvű “GLOBAL PERSPECTIVES & INSIGHTS – The Artificial Intelligence Revolution”[2] című kiadvány az IIA gondozásában.

Az MI szabályozói háttere nem egységes: az Európai Unió Mesterséges intelligencia törvénye (AI Act) a legrészletesebb, négyféle kockázati szintet (elfogadhatatlan, magas, korlátozott és minimális) határoz meg az MI-vel kapcsolatban. Ugyanakkor a belső ellenőrzési vezetők megjegyezték, hogy az egyes kategóriák definíciója nem kellően kidolgozott. Nemzetközi vállalatok esetében érdemes még megismerni az Egyesült Királyság által alkalmazott jogi hátteret és az OECD irányelvét is.

[2]https://www.theiia.org/en/content/articles/global-perspectives-and-insights/2023/global-perspectives-insights-the-artificial-intelligence-revolution/

KIBER- ÉS ADATBIZTONSÁG

Az egyre inkább az MI-által generált, többek között ún. deepfake (pl. egy belsős munkatárs megszemélyesítése segítségével végrehajtott) vagy hibrid támadásoknak „köszönhetően" a kiber- és adatbiztonság az előző évekhez hasonlóan a legmagasabb kockázatnak bizonyult. A „hagyományosnak mondható" külső behatolások is hatékonyabbá váltak: míg 2023-ban átlagosan 84 perc kellett a sikeres végrehajtáshoz, ez 2024-ben már 60 percre csökkent. 2024-ben két új Európai Uniós jogszabály segíti a digitális ellenállóképesség erősödését: a pénzügyi szektorban a Digital Operational Resilience Act (DORA), a nagy és középvállalati szektorban pedig a NIS2 Direktíva. Míg a DORA közvetlenül hatályos, a NIS2-t a nemzeti jogszabályokban kell implementálni. Mindkét jogszabály nagy hangsúlyt fektet a kockázatokat minimalizáló vállalatirányítási keretrendszerre, amelynek része a belső ellenőrzés is, így számára is írnak elő feladatokat. A belső ellenőrzés emellett abban is segítheti a vállalatokat, hogy felméri, a vállalatok hogyan adaptálták a rájuk vonatkozó előírásokat. Hasonlóan az MI témakörében említett kiadványhoz, az IIA a kiberbiztonság területén is ad angol nyelvű iránymutatást[3].

HUMÁN TŐKE

A megfelelő humán erőforrás rendelkezésre állásával, megtartásával, a tehetséggondozással és a diverzitással kapcsolatos kockázatokat a belső ellenőrzési vezetők az utóbbi három évben a második helyen említették. Érdekes, hogy ennek ellenére a felmérés résztvevőinek csupán negyede sorolta azon öt terület közé, amelyek a legtöbb belső ellenőrzési munkát igénylik – a felmérés az sugallja, hogy ez a kockázat nem kapja meg a szükséges belső ellenőrzési fókuszt. Több nemzeti IIA szervezet is készít útmutatót a viselkedési kockázat, valamint a kockázati és szervezeti kultúra vizsgálatához, továbbá javasolják, hogy a belső ellenőrök működjenek együtt a viselkedési szakemberekkel. Általános az a vélekedés, hogy a szervezeteknek hatékonyabb folyamatokra van szükségük, mind a munkaerő-felvétel, mind pedig a szervezeten belüli áthelyezés és a kilépés terén – a Risk in Focus 2025 értékelése szerint az európai munkavállalók körében a legalacsonyabb a munkahely iránti elköteleződés. A humán erőforrás stratégiáról és folyamatokról az EU Corporate Sustainability Reporting Directive (CSRD) keretében készült jelentésben is számot kell adnia a szervezeteknek, a jelentésről külső auditor ad véleményt, ugyanakkor a belső ellenőrzés is vizsgálhatja, hogy a vállalat stratégiai célkitűzései ezen a téren mennyire valósultak meg.

MAKROÖKONÓMIAI ÉS GEOPOLITIKAI BIZONYTALANSÁGOK

Az ellenőrzési vezetők a makroökonómiai és geopolitikai bizonytalanságokat tavaly a harmadik, míg idén az ötödik helyre rangsorolták. Az ún. "szürke-zónabeli agresszió" jelent új és jelentős kockázatot, vagyis az államok és államilag finanszírozott szereplők azon képessége, hogy zavart okoznak a termelésben és a kereskedelemben (például kibertámadásokon keresztül). Emellett a deepfake technológiák e kérdéskörben is megemlítésre kerültek, ugyanis ezek használata alkalmas arra, hogy befolyásolja

[3] https://www.theiia.org/en/content/articles/global-perspectives-and-insights/2025/cybersecurity/

a politikát. Harmadrészt a kereskedelmi embargók és szankciók is jelentősen befolyásolhatják a vállalatok üzleti modelljét. A vállalatok stressz tesztekkel és a stratégiák készítésekor különböző szcenáriók tervezésével kezelhetik a felmerülő komplex kockázatokat. A belső ellenőrzés abban nyújthat segítséget, hogy áttekinti ezeket a kockázatkezelési tevékenységeket. Az Európai Unió ezen témakörben alkalmazandó Corporate Sustainability Due Diligence direktívája (CSDDD) iránymutatással szolgál arra, hogy a vállalatok áttekintsék a beszállítói láncaikat, a belső ellenőrzés pedig értékelheti a direktíva (és a nemzeti jogszabályok) vállalati szintű implementációjának folyamatát.

ÉGHAJLATVÁLTOZÁS, BIOLÓGIAI SOKFÉLESÉG, KÖRNYEZETI FENNTARTHATÓSÁG

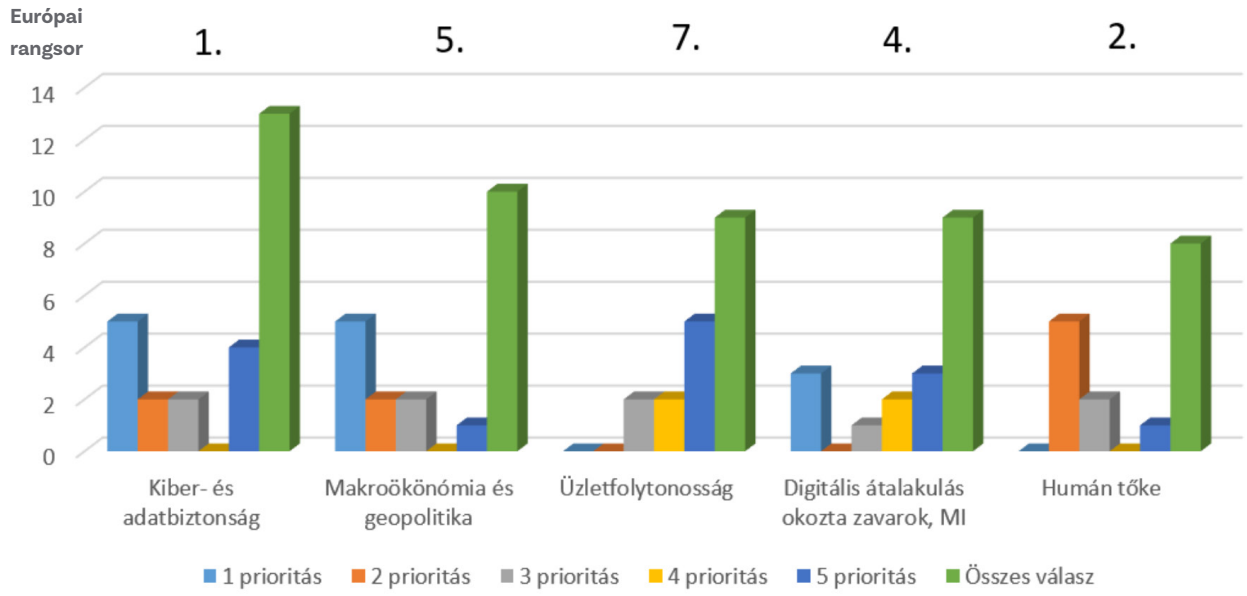
Ezt a kockázatot 2025-re tekintve csak a hatodik helyre rangsorolták a felmérés résztvevői, azonban a szabályozói oldalról tapasztalható növekvő nyomás (például az EU Corporate Social Responsibility direktívája) miatt a várakozások szerint feljebb fog kerülni a prioritási listán és 2028-ra várhatóan már a negyedik legmagasabb kockázat lesz. A vállalatok fókuszát is egyre jelentősebb mértékben fogja lekötni ez a terület és ezzel párhuzamosan kritikus fontosságú lesz a belső ellenőrzési funkció ilyen irányú képzése is. Annak ellenére, hogy a CSRD már hatályba lépett, a vállalatok jelentős részének adatgyűjtési folyamatai még kiforratlanok, ezért a belső ellenőrzés abban tud segíteni, hogy áttekinti a CSRD-nek megfelelő nyilvánosságra hozatal adatgyűjtési folyamatait és gap-elemzéseket végez.

Magyarországra vonatkozó adatok

Magyarországi szervezetek 2024-ben is részt vettek a felmérésben, többségük továbbra is a közszférában, illetve a pénzügyi és biztosítási szektorban működik.
A legfontosabbnak ítélt kockázatok rangsorában némi átrendeződés figyelhető meg a 2024 eredményekhez viszonyítva. Míg a *kiber- és adatbiztonságban* rejlő kockázat továbbra is az első helyen áll, a második és a harmadik helyről kiszorult a *humán tőkére* vonatkozó kockázat és a *törvényi és szabályozási változásban* rejlő bizonytalanság (ez utóbbi a 6. helyre került a rangsorban). Helyüket a *makroökonómiai és geopolitikai* bizonytalanság, illetve az *üzletfolytonosság* vette át, utóbbi tavaly még csak a 7. helyen szerepelt. A d*igitális átalakulás okozta zavarokban, új technológiákban, mesterséges intelligenciában* rejlő kockázatok rangsorban elfoglalt helye nem változott számottevően.

Az alábbi ábra jelzi azt a 5 fő kockázati területet, mellyel a válaszadók szerint a felmérésben részt vevő magyar szervezetek jelenleg szembesülnek, egyben érdekes összehasonlítással szolgál az európai válaszadók által felállított rangsorral:

A LEGFONTOSABB KOCKÁZATI TÉNYEZŐK MAGYARORSZÁGON



Összehasonlítva a magyar és az európai adatokat az 1. helyre sorolt kockázatban nincs eltérés, a továbbiak tekintetében azonban kis mértékben eltérő eredmények születtek, mint ahogy az ábrán is látható. Az európai értékelés szerint a 3. helyen a *jogszabályi környezet változásaiban* rejlő bizonytalanság szerepel, mely – ahogy már említettük – a magyarországi értékelésben a 6. helyre került.

A 3 éves kitekintésben (2025-2028) a vezető kockázati tényezők között közel ugyanazokat jelölték meg a magyar válaszadók és hasonló értékeléssel, mint rövidebb távra (azaz 2025-re), jelentősebb változásként említhető, hogy a *digitális átalakulás okozta zavarok, új technológiák, mesterséges intelligencia* kockázatát előrébb, a 2. helyre sorolták, illetve a legfontosabb 5 kockázat között megjelenik az *éghajlatváltozás és a fenntarthatóság* is.

A 2025-ös felmérésben újítás 2024-hez képest, hogy a kérdések között nem csak az szerepelt, hogy mely kockázatokat értékelik a leginkább aktuálisnak a szervezetek, hanem az is, hogy a belső ellenőrzési funkciójuk ehhez képest mely területekkel foglalkozik a legtöbbet. E kérdés tekintetében az alábbi rangsor született hazánkban:

1. Üzletfolytonosság (működési biztonság, krízis menedzsment, katasztrófa kezelés)
2. Törvényi és szabályozási változások
3. Pénzügyi, likviditási és fizetőképességet érintő kockázatok
4. Szervezetirányítás és vállalati jelentéstétel
5. Kiber- és adatbiztonság

Látható, hogy a legtöbb belső ellenőrzési erőforrás nem feltétlenül a leginkább releváns kockázatokra fordítódik. Ennek számtalan oka lehet, közülük egyik például a *kiber- és adatbiztonság* speciális kompetencia-igénye, mely nem minden belső ellenőrzési szervezetben áll rendelkezésre. Emellett az eltérés mögött állhat az is, hogy akadnak olyan belső ellenőrzési témák, amelyek gyakran, sok szervezetnél előírás szerint ismétlődő ellenőrzési feladatokat jelentenek pl. a *törvényi és szabályozási* megfelelés, a *pénzügyi* témájú ellenőrzések, valamint a *szervezetirányításhoz* kapcsolódó vizsgálatok. Az üzletfolytonosság témakörének, mint kiemelt belső ellenőrzési témának 1. helyre kerülése nem csak azt sejteti, hogy e terület magas kockázatot hordoz, hanem azt is, hogy a belső ellenőrzés ezen a területen rendelkezik kompetenciával, illetve észrevételei és javaslatai igenis hangsúlyos szerepet játszanak a kialakításában és működtetésében.

Specifikus téma - Mesterséges intelligencia (MI)

A kutatás rámutatott, hogy míg az elmúlt években a gazdálkodó szervezeteknek alig a fele jelezte azt, hogy legalább egy területen alkalmaz mesterséges intelligenciát, 2024-ben a vállalkozások háromnegyede szerint több területen van ilyen megoldása, vagy tervez további fejlesztéseket. Az ilyen fokú intenzív használata az innovatív technológiáknak egyaránt nagy kihívások elé állítja a vállalatvezetőket és a belső ellenőröket. A ChatGPT és növekvő számú versenytársainak fogyasztók számára is elérhető megjelenésével mind az ügyféligényeket, mind a vállalati folyamatokat is átrajzolta. Erre reagálva a vezető technológiai vállalatok folyamatos fejlesztéssel igyekeznek meglévő termékeikbe, szolgáltatásaikba beépíteni ezeket a megoldásokat, ezáltal új kihívásokat és egyúttal új lehetőségeket adva a felhasználók számára. Sokan állítják, hogy az MI alkalmazása nélkül elképzelhetetlen a jövőbeni üzleti siker, ezért minden vállalkozásnak stratégiai szinten is foglalkoznia kell az ilyen jellegű megoldásokkal. Ez nemcsak az üzleti modell, a nyújtott szolgáltatások fejlesztését jelenti, hanem a működési és szervezeti keretek újragondolását is. A ma már a mindennapi életben is könnyen elérhető MI megoldások miatt kiemelten fontos az, hogy a kiemelt stratégiai projekteken túlmutató (tehát egy-egy kiemelt üzleti területen bevezetésre kerülő innovatív megoldásokon túllépő), a napi működésbe begyűrűző lehetőségeket (úm. fordító programok, vizuális megjelenést támogató eszközök) monitorozza és értékelje a vállalat vezetése a kockázatkezelési rendszerének részeként, hiszen ezek jelentős információbiztonsági és adatkezelési kockázatokat eredményezhetnek.

[4]https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=OJ:L_202401689

Ahogy fentebb is kiemeltük, a szabályozó hatóságok igyekeznek utolérni a technológiai fejlődést. Az Európai Unió által 2024. júniusában elfogadott és publikált mesterséges intelligenciáról szóló rendelete[4] egy általános kockázatkezelési keretrendszert vezet be, sőt bizonyos megoldások használatát megtiltja. A mesterséges intelligencia definíciója és a főbb vállalatirányítási elvek követik az OECD által megfogalmazottakat. Az új szabályozás ugyanakkor sok értelmezési kérdést és üzleti dilemmát vet fel, így a vállalkozások kockázati étvágyának függvényében alakulnak a gyakorlati alkalmazások: egyes vállalkozások nem várják meg az értelmezések teljes kialakulását, így megfelelési kockázattal szembesülhetnek a korai bevezetésekkel, mások viszont, akik addig korlátozzák az MI implementálását, amíg a keretek nem válnak egyértelművé, versenyhátrányt szenvedhetnek el.

Az MI térnyerése nemcsak a belső ellenőrzés által vizsgálható folyamatok és területek esetében jelent kihívást a belső ellenőrök számára, hanem ezen megoldások használata saját audit tevékenységük során szintén megjelenik. Vannak olyan területek, ahol a belső ellenőri kapacitásokat meghatványozhatja egy-egy megoldás kialakítás és bevezetése, ugyanakkor a vizsgált terület adatainak, bizalmas információinak kezelése ugyanúgy megfelelő védelmet követel meg, mint az üzleti területek esetében.

Az MI összefonódó etikai és működési kockázatai miatt a belső ellenőröknek ezeket a területeket egyszerre több nézőpontból kell vizsgálniuk: adatvédelem, adatkezelés, átláthatóság, társadalmi kitettségek, környezeti hatások. Az MI kritikus eleme a bizalom, kiemelten a bizalom a személyes adatok védelme, az információ biztonság és a megfelelő információ szolgáltatás felé. Emiatt is emelik ki azt, hogy ebben az esetben különösen fontos a kritikus gondolkodás és a szakmai szkepticizmus, ahogy azt a Globális Belső Ellenőrzési Normák 4.3 normája is megfogalmazza.
A Risk in Focus 2025 összefoglalója kiemeli azokat a pontokat, ahol a belső ellenőrök segíthetik a szervezetet ezen kockázatok kezelésében:

1. Értékelje, hogy mennyire támogatott a szervezet mesterséges intelligencia és digitalizációs stratégiája átalakítási, vagy változáskezelési tervekkel.
2. Bizonyosság nyújtása arra vonatkozóan, hogy az egyes mesterséges intelligencia-projektek kapcsolódnak a szervezet fő stratégiai célkitűzéseihez.
3. Bizonyosság nyújtása arra vonatkozóan, hogy a szervezet irányítási folyamatai képesek ellenőrizni a mesterséges intelligencia alkalmazását a vállalaton belül.
4. Mérje fel, hogy a folyamatok mennyire felelnek meg a hatályos szabályozásoknak, például a mesterséges intelligenciáról szóló rendeletnek.
5. Adjon bizonyosságot arról, hogy a szervezet MI-stratégiáját megfelelő képzési, oktatási program támogatja, amely képes a kulcsfontosságú képességek megszerzésére, fejlesztésére és megtartására.
6. Annak biztosítása, hogy a szervezet mesterséges intelligencia használata etikus és megbízható a piac minden szereplője számára.

A Risk in Focus felmérés minden évben kettős célt szolgál: egyrészt egy jó lehetőség arra, hogy a vállalatvezetők össze tudják hasonlítani a különböző kockázatokat és azok hatásait, valamint a lokális prioritásokat, másrészt a belső ellenőrzési vezetők számára megkönnyítse a kockázatelemzést és a következő évi belső ellenőrzési tervezést. Úgy gondoljuk, hogy a hazai eredmények megismerése és összehasonlítása a nemzetközi trendekkel minden belső ellenőr számára hasznos információkkal szolgál.

Az összefoglaló elkészítéséért külön köszönet:

Doszpod Dénes MBA	RiGoCon Kft., ügyvezető, BEMSZ elnökségi tag, a Bizottság vezetője
Baki László CIA, CCSA	Magyar Nemzeti Bank, kiemelt vezető auditor
Bánhegyi Réka CIA	Magyar Nemzeti Bank, vezető auditor
Demjénné Gyöngy Judit	Generali Biztosító, adatirányítási vezető
Geiszlinger Árpád CIA, CRMA	Szerencsejáték Zrt., Belső ellenőrzési vezető
Polgár Péter	BEMSZ Közszféra Állandó Bizottság vezetője
Simon-András Henrietta CIA	MOL Nyrt. belső ellenőr