

Mennyiben segíti az AI Act követelményeire való felkészülést a sikeresen teljesített NIS2 audit?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/57

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.28	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

- A sikeres NIS2 audit jó kiindulópont, de nem jelenti automatikusan az MI-rendelet (AI Act) követelményeinek való megfelelést. Az audit azt igazolja, hogy a Szervezet elektronikus információs rendszerei megfelelnek a Kiberbiztonsági tv. és a 7/2024. (VI. 24.) MK rendelet védelmi intézkedéseinek, az MI-rendelet viszont az egészséget, a biztonságot és az alapvető jogokat védi, és a megfelelést az egyes MI-rendszereken kéri számon.
- A két szabályozás a kiberbiztonsági metszetben fedi egymást. A kockázatelemzés, a naplózás, az incidenskezelés, az ellátási lánc, a változáskezelés, az üzletmenet-folytonosság és a képzés auditált gyakorlata hasznosítható, az adatkormányzás, az emberi felügyelet, a műszaki dokumentáció, a megfelelőségértékelés és az alapjogi hatásvizsgálat viszont az auditból nem következik.
- Szolgáltatói szerepkörben az audit a 15. cikk szerinti kiberbiztonsági követelmény hagyományos rétegét és a 17. cikk szerinti minőségirányítási rendszer szervezeti elemeit alapozza meg, az MI-specifikus fenyegetésekre (adatmérgezés, modellmérgezés, modellkijátszás) viszont nem ad kontrollt. Alkalmazói szerepkörben a 26. cikk szerinti intézkedések, a naplómegőrzés és az incidensjelzés háttérét adja, az emberi felügyelet, a tájékoztatás és az alapjogi hatásvizsgálat auditon kívüli feladat.
- A NIS2 audit nem teremt megfelelőségi védelmet, az MI-rendelet a 15. cikkénél csak a Kiberbiztonsági rendelet szerinti tanúsítványt és a Kiberrezilienciáról szóló rendelet szerinti megfelelést ismeri el. Az auditjelentés bizonyíték, nem tanúsítvány.
- Az időzítés kedvező. Az (EU) 2026/1744 rendelet a magas kockázatú rendszerekre vonatkozó kötelezettségek alkalmazását 2027. december 2-ára, illetve 2028. augusztus 2-ára halasztotta, így a következő NIS2 auditciklus egybeesik az MI-felkészüléssel. A kettőt érdemes egy programként kezelni.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy a Kiberbiztonsági tv. hatálya alá tartozó szervezet (a továbbiakban „Szervezet”) 2026 első felében a Kiberbiztonsági tv. 16. §-a szerinti kiberbiztonsági auditon esett át, és az auditor a védelmi intézkedések megfelelőségét megállapította. A Szervezet saját fejlesztésű és külső szállítótól beszerezett MI-rendszereket is használ, köztük az MI-rendelet III. melléklete szerinti területet érintőket. A vezetés arra keres választ, hogy a sikeres audit mennyiben könnyíti meg az MI-rendelet szerinti felkészülést, és hol kell külön erőforrást tervezni.

Az állásfoglalás az alábbi kérdéseket vizsgálja:

- Általánosságban mennyiben jelent segítséget a teljesített NIS2 audit az MI-rendelet követelményeinek teljesítésében?
- Mennyiben segít, ha a Szervezet magas kockázatú MI-rendszer szolgáltatója?
- Mennyiben segít, ha a Szervezet magas kockázatú MI-rendszer alkalmazója?

Nem tárgya az állásfoglalásnak az általános célú MI-modellek szabályozása, a tiltott gyakorlatok köre, az 50. cikk szerinti átláthatóság és az ágazati jog sajátos követelményei.

3. GYAKORLATI JAVASLATOK

3.1 Amit az auditból közvetlenül át lehet emelni

Az auditált nyilvántartások, eljárások és bizonyítékok az alábbi területeken hasznosíthatók, a többi követelményt az auditra tekintet nélkül fel kell építeni (lásd a 4. pontot és az 1. mellékletet).

- a) Leltár és besorolás. Az elektronikus információs rendszerek nyilvántartását MI-leltárral kell kiegészíteni, amely rögzíti a futtató rendszert, a Szervezet szolgáltatói vagy alkalmazói szerepkörét és a 6. cikk szerinti besorolást.
- b) Kockázatelemzés. A rendszerszintű kockázatelemzés módszertana megtartható, de a fenyegetéskatalógust az MI-specifikus fenyegetésekkel, a védendő értékeket pedig az egészséggel, a biztonsággal és az alapvető jogokkal ki kell bővíteni.
- c) Naplózás és incidenskezelés. A naplózási szabályzatot ki kell terjeszteni az MI-rendszerek automatikusan generált naplóira, legalább hat hónapos megőrzéssel. Az eseménykezelési tervbe be kell építeni a súlyos incidens fogalmát és bejelentési útját.
- d) Ellátási lánc és változáskezelés. A szállítói szerződéseket ki kell egészíteni a használati utasítás és a szolgáltatói együttműködés rögzítésével, a változáskezelésbe pedig be kell építeni a jelentős módosítás vizsgálatát, mert az az alkalmazót szolgáltatóvá teheti.
- e) Képzés. A kiberbiztonsági képzési program kiegészíthető az MI-jártasság fejlesztésével, külön modullal az emberi felügyeletet ellátóknak.

3.2 A javasolt eljárás

A felkészülést az alábbi lépésekben javasoljuk.

- a) MI-leltár és szerepkör-elemzés, a szolgáltatói vagy alkalmazói szerepkör és a kockázati besorolás meghatározása a Bizottság besorolási iránymutatás-tervezete alapján.
- b) Gap elemzés az auditjelentés és az 1. melléklet szerinti megfeleltetés alapján, majd a meglévő szabályzatok és eljárások kiterjesztése az MI-rendszerekre.
- c) MI-specifikus kontrollok és dokumentáció felépítése, majd integrálás a következő auditciklusba, közös bizonyítéktárral és felelősségi renddel.
- d) Ha magas kockázatú MI rendszert üzemeltet a szervezet szolgáltatói szerepkörben akkor ajánlott az EN 18286 (2026) szabvány alkalmazása.
- e) Egyéb esetben megfontolandó, de nem kötelező az ISO/IEC 42001 szabvány szerinti MI-irányítási rendszer kialakítása

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

A NIS2 irányelvet a magyar jogba a Kiberbiztonsági tv. és végrehajtási rendeletei ültették át,¹ a kiberbiztonsági audit pedig törvényi kötelezettség, amely az e törvény szerinti követelményeknek való megfelelést vizsgálja.

[...] az 1. § (1) bekezdés e) pontja szerinti szervezet az e törvény szerinti kiberbiztonsági követelményeknek való megfelelés bizonyítására köteles két évente, illetve a 23. § (1) bekezdése szerint illetékes kiberbiztonsági hatóság általi elrendelés esetén kiberbiztonsági auditot végeztetni. [2024. évi LXIX. törvény 16. § (1) bekezdés]

Az audit tárgya a Kiberbiztonsági tv. szerinti követelményrendszer, amelynek középpontjában a biztonsági osztályba sorolás és az osztályhoz rendelt védelmi intézkedések állnak, a védendő érték pedig a rendszer és az adat bizalmassága, sértetlensége és rendelkezésre állása. Az első audit határideje a legtöbb érintett szervezetnél 2026. június 30. volt, a következő audit ezért 2028 első felére esik.²

Az MI-rendelet más logikát követ. Termékbiztonsági jellegű szabályozás, amely nem a szervezetet, hanem az egyes MI-rendszert vizsgálja, és a kötelezettségeket a szerepkörhöz rendeli. A szolgáltató az MI-rendszert fejleszti vagy fejleszteti, és saját neve alatt forgalomba hozza vagy üzembe helyezi, az alkalmazó a felügyelete alá tartozó rendszert szakmai tevékenysége körében használja. A magas kockázatú rendszerek kockázatkezelése nem az informatikai rendszer biztonságát, hanem a rendszer által az egészségre, a biztonságra és az alapvető jogokra jelentett kockázatot állítja a középpontba.³ A NIS2 audit tehát azt igazolja, hogy a Szervezet rendszereit megfelelően védik, az MI-rendelet azt kérdezi, hogy a rendszer az embereknek nem árt-e, az audit ezért csak a két kérdés metszetében segít.

Az időzítést a 2026. július 27-én hatályba lépett (EU) 2026/1744 rendelet határozza meg.⁴

*c) a III. fejezet 1., 2. és 3. szakaszát – a 6. cikk (5) bekezdése kivételével – a következő időpontoktól kell alkalmazni:
i. 2027. december 2. a 6. cikk (2) bekezdése és a III. melléklet alapján nagy kockázatúnak minősített MI-rendszerek tekintetében; és*

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS2); 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.); 418/2024. (XII. 23.) Korm. rendelet; 7/2024. (VI. 24.) MK rendelet; 1/2025. (I. 31.) SZTFH rendelet

² 2024. évi LXIX. törvény 10. § (1) és (4) bekezdés; 7/2024. (VI. 24.) MK rendelet 2. § (1) bekezdés és 2. melléklet, továbbá az NBSZ NKI hatósági kézikönyvei (nki.gov.hu, 2026); az audit határidejéről a 2025. évi XXXII. törvény és az SZTFH 2025. június 27-i tájékoztatója (sztfh.hu)

³ Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (MI-rendelet) 3. cikk 3. és 4. pont, 9. cikk (2) bekezdés a) pont

⁴ Az Európai Parlament és a Tanács (EU) 2026/1744 rendelete (2026. július 8.), a mesterséges intelligenciáról szóló digitális omnibusz csomag (HL L, 2026/1744, 2026. július 24.), 1. cikk 40. pont

ii. 2028. augusztus 2. a 6. cikk (1) bekezdése és az I. melléklet alapján nagy kockázatúnak minősített MI-rendszerek tekintetében; [(EU) 2024/1689 rendelet 113. cikk harmadik bekezdés c) pont, az (EU) 2026/1744 rendelettel megállapított szöveg]

A magyar végrehajtási keretet a 2025. évi LXXV. törvény és a 344/2025. (X. 31.) Korm. rendelet adja, az MI piacfelügyeleti hatósági feladatokat 2026 őszén a Tudományos és Technológiai Minisztérium keretében működő MI Piacfelügyeleti Hatóság látja el.⁵

4.2 Mit ér az audit általánosságban?

4.2.1 A közös metszet

Az MI-rendelet a magas kockázatú rendszerektől megfelelő szintű kiberbiztonságot követel, és külön nevesíti az MI-specifikus sebezhetőségeket.

(5) A nagy kockázatú MI-rendszereknek reziliensnek kell lenniük a jogosulatlan harmadik felek arra irányuló kísérleteivel szemben, hogy a rendszer sebezhetőségeinek kiaknázása révén megváltoztassák a rendszer használatát, kimeneteit vagy teljesítményét.

A nagy kockázatú MI-rendszerek kiberbiztonságának biztosítását célzó műszaki megoldásoknak megfelelőnek kell lenniük a releváns körülmények és a kockázatok szempontjából.

Az MI-specifikus sebezhetőségek kezelésére szolgáló műszaki megoldásoknak adott esetben magukban kell foglalniuk azon intézkedéseket, amelyek a tanítóadat-készlet manipulálását megkísérítő támadásoknak (adatmérgezés) vagy a tanítás során használt előtanított összetevők manipulálását megkísérítő támadásoknak („modellmérgezés”), a modell hibájának előidézésére szolgáló bemeneteknek (támadó szempontú példák vagy modellkijátszás), a bizalmasság elleni támadásoknak vagy a modellhibáknak a megelőzésére, felderítésére, az azokra való reagálásra, azok megoldására és ellenőrzésére irányulnak. [(EU) 2024/1689 rendelet 15. cikk (5) bekezdés]

Az első két albekezdés a hagyományos kiberbiztonsági réteg, itt az audit a legtöbbet ér. A hozzáférés-felügyelet, az azonosítás és hitelesítés, a konfigurációkezelés, a sérülékenységszűrés, a kártékony kód elleni védelem, a monitorozás és a kommunikáció védelme a katalógus törzsanyaga, és az MI-rendszert futtató infrastruktúrára változtatás nélkül alkalmazható. A harmadik albekezdés viszont olyan fenyegetéseket sorol, amelyekre a katalógusnak nincs kontrollja. Az ENISA és a Bizottság Közös Kutatóközpontja szerint az

⁵ 2025. évi LXXV. törvény; 344/2025. (X. 31.) Korm. rendelet; mihivatal.gov.hu. A Kormány 2026. őszi törvényalkotási programja a kiberbiztonsági felügyelet átalakítását is tartalmazza.

általános információbiztonsági szabványok az MI-rendszerek kockázatait csak részben fedik, ezért a bevált kiberbiztonsági gyakorlatot MI-specifikus kontrollokkal kell kiegészíteni.⁶

A kockázatkezelésnél az MI-rendelet maga nyit kaput a meglévő folyamatok felé.

(10) A nagy kockázatú MI-rendszerek azon szolgáltatói esetében, amelyek az uniós jog egyéb vonatkozó rendelkezéseinek értelmében belső kockázatkezelési folyamatokra vonatkozó követelmények hatálya alá tartoznak, az (1)–(9) bekezdésben leírt szempontok az említett jog alapján létrehozott kockázatkezelési eljárások részét képezhetik vagy azokhoz társulhatnak. [(EU) 2024/1689 rendelet 9. cikk (10) bekezdés]

A Kiberbiztonsági tv. 6. § (2) bekezdése szerinti kockázatmenedzsment keretrendszer ilyen, uniós jogon alapuló folyamat,⁷ a magas kockázatú MI-rendszer kockázatkezelése tehát ebbe illeszthető, ha a fenyegetéskatalógus és a hatásskála az egészségre, a biztonságra és az alapvető jogokra is kiterjed. A módszertan átvihető, a tartalom nem.

Hasonló a helyzet a naplózásnál, az incidenskezelésnél és az ellátási láncnál. A naplózandó események meghatározása és a naplók rendszeres elemzése minden biztonsági osztályban kötelező, az MI-rendelet pedig az események automatikus rögzítését és a naplók legalább hat hónapos megőrzését várja el. A naplókezelés infrastruktúrája adott, az MI-rendszer szintjén rögzítendő eseményeket viszont külön kell meghatározni. Az eseménykezelési képesség és a jogszabály szerinti jelentés szintén minden osztályban kötelező, de a súlyos incidens fogalma, címettje és határideje eltér a kiberbiztonsági incidensétől. Az ellátási lánc szabályzata és a beszerzési követelmények jó alapot adnak az MI-szállítói szerződésekhez, a 25. cikk (4) bekezdése szerinti írásbeli megállapodás tartalmát azonban külön kell kidolgozni.⁸

4.2.2 Ahol az audit nem segít

A magas kockázatú rendszerek követelményeinek nagyobb része olyan kérdést szabályoz, amelyet a NIS2 nem ismer. Ilyen az adatkészletek minőségét és reprezentativitását megkövetelő adatkormányzás, a rendeltetést, a korlátokat és az emberi felügyelet módját leíró műszaki dokumentáció, a pontossági mérőszámok, a megfelelőségértékelés, a CE-jelölés és a

⁶ 7/2024. (VI. 24.) MK rendelet 2. melléklet 2., 6., 8., 15., 17. és 18. fejezet, például 15.9.1. [A][J][M] és 18.13.1. [A][J][M]; ENISA, Cybersecurity of AI and Standardisation (2023. március); Junklewitz és társai, Cybersecurity of Artificial Intelligence in the AI Act, JRC134461 (2023. szeptember); prEN 18282 (CEN-CENELEC JTC 21), szavazási szakasz 2026 nyarán. A Bizottság szerint 2026. augusztus 3-ig az MI-rendelethez egyetlen harmonizált szabvány sem jelent meg a Hivatalos Lapban (digital-strategy.ec.europa.eu)

⁷ 2024. évi LXIX. törvény 6. § (2) bekezdés; 7/2024. (VI. 24.) MK rendelet 2. melléklet 15.4.1. [A][J][M] a rendszerszintű kockázatelemzésről

⁸ A naplózásról 7/2024. (VI. 24.) MK rendelet 2. melléklet 4.2.1. [A][J][M] és 4.13.1. [A][J][M], valamint (EU) 2024/1689 rendelet 12. cikk (1) és (2) bekezdés, 19. cikk (1) bekezdés, 26. cikk (6) bekezdés; az incidenskezelésről 7/2024. (VI. 24.) MK rendelet 2. melléklet 9.9. [A][J][M], 9.27.2. [A][J][M] és 9.34. [A][J][M]; az ellátási láncról 7/2024. (VI. 24.) MK rendelet 2. melléklet 19.2.1. [A][J][M], 19.13. [A][J][M] és 16.7. [A][J][M], valamint 2024. évi LXIX. törvény 6. § (5) bekezdés d) pont

regisztráció.⁹ Ezekre az audit sem kontrollt, sem bizonyítékot nem ad, legfeljebb a dokumentálás és a bizonyítékkezelés kultúráját.

4.2.3 A megfelelési vélelem hiánya

Külön kérdés, hogy a sikeres audit jogi értelemben beszámítható-e. Az MI-rendelet a 15. cikkénél két vélelmet ismer, a Kiberbiztonsági rendelet szerinti tanúsítványt vagy megfelelési nyilatkozatot, valamint a Kiberrezilienciáról szóló rendeletnek való megfelelést.¹⁰

(3) Amennyiben a nagy kockázatú MI-rendszerek az (EU) 2024/2847 rendelet hatálya alá tartoznak, és teljesülnek az említett rendelet 12. cikkének (1) bekezdésében meghatározott feltételek, úgy kell tekinteni, hogy az ilyen rendszerek megfelelnek az e rendelet 15. cikkében meghatározott kiberbiztonsági követelményeknek. [(EU) 2024/1689 rendelet 42. cikk (3) bekezdés, az (EU) 2026/1744 rendelettel beiktatott szöveg]

A NIS2 audit egyik körbe sem tartozik, mert nem tanúsítási rendszer és nem gyártói megfelelésértékelés. Az auditjelentés ezért nem tanúsítvány, hanem bizonyíték, amely a műszaki dokumentáció kiberbiztonsági intézkedésekről szóló részében felhasználható. Fordítva viszont a Kiberbiztonsági tv. elismeri a tanúsított IKT-terméket a követelmények igazolására,¹¹ így egy ilyen MI-termék beszerzése mindkét irányban könnyítést hozhat.

4.3 Szolgáltatói szerepkörben, magas kockázatú rendszer esetén

A szolgáltató kötelezettségeit a 16. cikk sorolja fel.¹² Ezek közül a 17. cikk szerinti minőségirányítási rendszer az, ahol az auditált szervezeti működés a legtöbbet ér.

(1) A nagy kockázatú MI-rendszerek szolgáltatóinak minőségirányítási rendszert kell bevezetniük, amely biztosítja az e rendeletnek való megfelelést. [...]
g) a 9. cikkben említett kockázatkezelési rendszer; [...]
i) a 73. cikkel összhangban a súlyos incidens bejelentésével kapcsolatos eljárások; [...]
m) elszámoltathatósági keret, amely meghatározza a vezetőség és az egyéb személyzet felelősségi körét az e bekezdésben felsorolt valamennyi szempont tekintetében. [(EU) 2024/1689 rendelet 17. cikk (1) bekezdés g), i) és m) pont]

Ezek mögé, valamint a k) pont szerinti nyilvántartás és az l) pont szerinti ellátásbiztonság mögé a Szervezet a meglévő kockázatmenedzsment keretrendszerét, incidenskezelési eljárását,

⁹ (EU) 2024/1689 rendelet 10., 11., 13. és 14. cikk, 15. cikk (1)–(4) bekezdés, 43., 47., 48. és 49. cikk, IV. melléklet

¹⁰ (EU) 2024/1689 rendelet 42. cikk (2) bekezdés; az Európai Parlament és a Tanács (EU) 2019/881 rendelete (Kiberbiztonsági rendelet); az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (Kiberrezilienciáról szóló rendelet) 12. cikk (1) bekezdés, fő szabályai 2027. december 11-től alkalmazandók

¹¹ (EU) 2024/1689 rendelet IV. melléklet 2. pont h) alpont; 2024. évi LXIX. törvény 6. § (8) bekezdés

¹² (EU) 2024/1689 rendelet 16. cikk

dokumentumkezelését, ellátási lánc szabályzatát és a Kiberbiztonsági tv. szerinti vezetői felelősségi rendet állíthatja. Az a)–f) pont szerinti tervezési, fejlesztési, tesztelési és adatgazdálkodási eljárások, valamint a h) pont szerinti forgalomba hozatal utáni nyomon követés az auditból nem következik. A rendelet a minőségirányítás formáját nem köti. Az ISO/IEC 42001 (2023) D melléklete az ISO/IEC 27001 szerinti rendszerrel való integrációra épít, a 17. cikkhez készült EN 18286 (2026) szabvány viszont szakmai elemzések szerint önálló szerkezetet követ, ezért a 27001 vagy a 42001 szerinti tanúsítás nem azonos az MI-rendelet szerinti minőségirányítással.¹³

A kiberbiztonsági incidenst a Szervezet az incidenskezelő központnak jelenti be, a súlyos incidenst a piacfelügyeleti hatóságnak, főszabály szerint tizenöt, kiterjedt jogsértésnél két, haláleset esetén tíz napon belül. A súlyos incidens fogalma nem a rendszer biztonságából, hanem a személynek, a vagyonnak, a környezetnek vagy az alapvető jogoknak okozott sérelemből indul ki, ezért a két fogalom egymástól függetlenül is megvalósulhat. Az auditált eseménykezelési képesség a közös alap, erre kell a két bejelentési láncot ráépíteni. A stabilitás követelménye az üzletmenet-folytonossági tervezéssel, a forgalomba hozatal utáni nyomon követés a monitorozással kapcsolható össze, a teljesítmény és a kockázat változásának követése azonban új tartalom.¹⁴

4.4 Alkalmazói szerepkörben, magas kockázatú rendszer esetén

Az alkalmazó 26. cikk szerinti kötelezettségei közül kettő épül közvetlenül az auditált gyakorlatra, a használati utasítás szerinti használatot biztosító technikai és szervezési intézkedések, valamint a naplók megőrzése.

(6) A nagy kockázatú MI-rendszerek alkalmazóinak meg kell őrizniük az adott nagy kockázatú MI-rendszer által automatikusan generált naplókat, amennyiben az ilyen naplók az ellenőrzésük alatt állnak a nagy kockázatú MI-rendszer rendeltetésének megfelelő – legalább hat hónapos – időtartamig, kivéve, ha az alkalmazandó uniós vagy nemzeti jog, különösen a személyes adatok védelmére vonatkozó uniós jog másként rendelkezik. [(EU) 2024/1689 rendelet 26. cikk (6) bekezdés első albekezdés]

Az intézkedések tartalmát a használati utasítás adja meg, a végrehajtás keretét a Szervezet információbiztonsági szabályzata, hozzáférés-felügyelete, konfigurációkezelése és képzési rendje. A naplók megőrzése a naplózási szabályzat kiterjesztésével teljesíthető, figyelemmel az adatvédelmi jog megőrzési korlátaira.

A többi alkalmazói kötelezettség auditon kívüli. Az emberi felügyeletet megfelelő szakértelemmel, képzéssel és hatáskörrel rendelkező személyekre kell bízni, ez szerepkör kérdése, nem kontrollé. Az alkalmazó felel az általa ellenőrzött bemeneti adatok relevanciájáért,

¹³ ISO/IEC 42001 (2023) D melléklet; EN 18286 (2026), CEN-CENELEC, harmonizált szabványként még nem jelent meg a Hivatalos Lapban; Cloud Security Alliance, EU AI Act Compliance, prEN 18286 and ISO 42001 (2026)

¹⁴ 2024. évi LXIX. törvény 6. § (5) bekezdés e) pont és (7) bekezdés; (EU) 2024/1689 rendelet 3. cikk 49. pont, 15. cikk (4) bekezdés, 72. cikk és 73. cikk (1)–(4) bekezdés; 7/2024. (VI. 24.) MK rendelet 2. melléklet 7.2.1. [A][J][M]

a működést a használati utasítás alapján nyomon követi, kockázat észlelésekor a szolgáltatót és a piacfelügyeleti hatóságot tájékoztatja, a használatot pedig felfüggeszti. A munkáltató a munkahelyi bevezetés előtt tájékoztatja a munkavállalók képviselőit és az érintett munkavállalókat, az érintett személyeket pedig arról, hogy esetükben magas kockázatú MI-rendszert használnak. Az adatvédelmi hatásvizsgálathoz a szolgáltatótól kapott információkat kell felhasználni, a közjogi szervek, a közszolgáltatást nyújtó magánszervezetek, valamint a hitelképesség-értékelő és az élet- és egészségbiztosítási kockázatértékelő rendszerek alkalmazói pedig alapjogi hatásvizsgálatot végeznek, amelybe az adatvédelmi hatásvizsgálat releváns részei beemelhetők, ehhez az Európai Adatvédelmi Testület és a NAIH anyagai adnak fogódzót.¹⁵

Két csapdát külön kiemelünk. Az alkalmazó szolgáltatóvá válik, ha a magas kockázatú rendszeren jelentős módosítást hajt végre, vagy egy rendszer rendeltetését magas kockázatúvá változtatja, ezért a változáskezelésbe be kell építeni a szerepkörváltás vizsgálatát. A 4. cikk szerinti MI-jártasság fejlesztéséhez a Kiberbiztonsági tv. szerinti képzési program keretét ad, a tartalmat azonban az MI-rendszerre és a felügyelet módjára kell szabni.¹⁶

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (MI-rendelet), az (EU) 2026/1744 rendelettel módosított, 2026. július 27-től hatályos egységes szerkezetű szöveg; az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS2); az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (Kiberrezilienciáról szóló rendelet); az Európai Parlament és a Tanács (EU) 2019/881 rendelete (Kiberbiztonsági rendelet)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.); 418/2024. (XII. 23.) Korm. rendelet; 7/2024. (VI. 24.) MK rendelet; 1/2025. (I. 31.) SZTFH rendelet; 2025. évi XXXII. törvény; 2025. évi LXXV. törvény az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról; 344/2025. (X. 31.) Korm. rendelet
- Európai Bizottság, a nagy kockázatú MI-rendszerek besorolásáról szóló iránymutatás tervezete (2026. május 19.) és az MI-rendelet szabványosításáról szóló tájékoztató (2026. augusztus 3.); ENISA, Cybersecurity of AI and Standardisation (2023) és Multilayer Framework for Good Cybersecurity Practices for AI (2023); JRC, Cybersecurity of Artificial Intelligence in the AI Act (2023); CEN-CENELEC, EN 18286 (2026) és prEN 18282; NBSZ NKI hatósági kézikönyvek a 7/2024. (VI. 24.) MK rendelet 2.

¹⁵ (EU) 2024/1689 rendelet 26. cikk (1), (2), (4), (5), (7), (9) és (11) bekezdés, 27. cikk (1) bekezdés és az (EU) 2026/1744 rendelettel módosított (4) bekezdés; Európai Adatvédelmi Testület, 3/2024. számú nyilatkozat (2024. július 16.) és 28/2024. számú vélemény (2024. december 17.); NAIH, képzési anyagok az MI és az adatvédelem összefüggéseiről (2025. június 12.) és tájékoztató a generatív MI-ről (2026. szeptember 2.), naih.hu

¹⁶ (EU) 2024/1689 rendelet 25. cikk (1) bekezdés b) és c) pont, 3. cikk 23. pont és 4. cikk (1) bekezdés; 2024. évi LXIX. törvény 6. § (5) bekezdés a) pont; 7/2024. (VI. 24.) MK rendelet 2. melléklet 3.2.1. [A][J][M] és 3.9.1. [A][J][M]

mellékletéhez (2026); SZTFH tájékoztató az auditra vonatkozó határidő módosításáról (2025. június 27.); az MI Piacfelügyeleti Hatóság tájékoztatója (mihivatal.gov.hu)

- Európai Adatvédelmi Testület, 3/2024. számú nyilatkozat és 28/2024. számú vélemény; NAIH, az MI és az adatvédelem összefüggéseiről szóló képzési anyagok (2025) és tájékoztató a generatív MI-ről (2026); ISO/IEC 42001 (2023); ISO/IEC 27001 (2022); Cloud Security Alliance, EU AI Act Compliance, prEN 18286 and ISO 42001 (2026)

I. MELLÉKLET. A NIS2 AUDIT ÉS AZ MI-RENDELET KÖVETELMÉNYEINEK MEGFELELTETÉSE

A táblázat a magas kockázatú MI-rendszerekre vonatkozó főbb követelményeket veti össze a 7/2024. (VI. 24.) MK rendelet 2. melléklete szerinti, auditált védelmi intézkedésekkel. A szögletes zárójel azt jelöli, hogy az adott intézkedés az alap [A], a jelentős [J] és a magas [M] biztonsági osztályban kötelező-e.

Az MI-rendelet követelménye	Auditált NIS2 háttér (7/2024. MK rendelet 2. melléklet, Kiberbiztonsági tv.)	Lefedettség	Amit külön kell megtenni
Kockázatkezelési rendszer (9. cikk)	Kiberbiztonsági tv. 6. § (2) kockázatmenedzsment keretrendszer; 15.4.1. rendszerszintű kockázatelemzés [A][J][M]	Részleges	Fenyegetéskatalógus és hatáskála kiterjesztése az egészségre, a biztonságra és az alapvető jogokra; MI-specifikus fenyegetések; életciklus-alapú, iteratív működtetés
Adatkormányzás (10. cikk, 4a. cikk)	Nincs megfelelője, az adatosztályozás és az adathordozók védelme csak a bizalmasságot érinti	Nincs	Tanító-, validálási és tesztadatkészletek minősége, reprezentativitása, torzításvizsgálat, dokumentálás
Műszaki dokumentáció és használati utasítás (11., 13. cikk, IV. melléklet)	Rendszerdokumentáció, auditjelentés mint bizonyíték a kiberbiztonsági intézkedésekről (IV. melléklet 2. pont h) alpont)	Csekély	A IV. melléklet szerinti teljes tartalom, rendeltetés, korlátok, teljesítmény, emberi felügyelet leírása
Naplózás és naplómegőrzés (12., 19. cikk, 26. cikk (6) bekezdés)	4.2.1. naplózandó események [A][J][M]; 4.13.1. naplók elemzése [A][J][M]	Jelentős	MI-rendszer szintű események meghatározása, legalább hat hónapos megőrzés, alkalmazónál a szolgáltatói naplók átvétele
Emberi felügyelet (14. cikk, 26. cikk (2) bekezdés)	Nincs megfelelője	Nincs	Felügyeleti funkciók tervezése, felügyelő személyek kijelölése, képzése és hatásköre
Pontosság és stabilitás (15. cikk (1)–(4) bekezdés)	7.2.1. üzletmenet-folytonossági terv [A][J][M]; mentések (7.35.)	Részleges	Mérőszámok, tesztelés, visszacsatolási hurkok kezelése, redundancia a modell szintjén
Kiberbiztonság (15. cikk (5) bekezdés)	Hozzáférés-felügyelet (2. fejezet), azonosítás és hitelesítés (8.), konfigurációkezelés (6.), 15.9.1. sérülékenységek ellenőrzése [A][J][M], kártékony kód elleni védelem (18.8.), 18.13.1. monitorozás [A][J][M], rendszer- és kommunikációvédelem (17.)	Jelentős	Adatmérgezés, modellmérgezés, modellkijátszás és bizalmasság elleni támadások elleni kontrollok (prEN 18282 szerint)
Minőségirányítási rendszer (17. cikk)	Információbiztonsági szabályzat, vezetői felelősségi rend (Kiberbiztonsági tv. 6. §), dokumentum- és nyilvántartás-kezelés, ellátásbiztonság	Részleges	Tervezési, fejlesztési, tesztelési és adatgazdálkodási eljárások; forgalomba hozatal utáni nyomon követés; EN 18286 (2026)
Súlyos incidens bejelentése és alkalmazói jelzés (73. cikk, 26. cikk (5) bekezdés)	9.9. eseménykezelési képesség [A][J][M]; 9.27.2. jogszabály szerinti jelentés [A][J][M]; 9.34. eseménykezelési terv [A][J][M]	Részleges	Súlyos incidens fogalma, piacfelügyeleti hatóság mint címzett, 15, 2 és 10 napos határidők, szolgáltató tájékoztatása, használat felfüggesztése
Ellátási lánc és szállítói együttműködés (25. cikk (4) bekezdés, 26. cikk (1) bekezdés)	19.2.1. ellátási lánc szabályzat [A][J][M]; 19.13. beszerzési módszerek [A][J][M]; 16.7. beszerzési követelmények [A][J][M]; Kiberbiztonsági tv. 6. § (5) d)	Jelentős	Írásbeli megállapodás az MI-rendelet szerinti információkról és hozzáférésről, használati utasítás átvétele és betartatása
Változáskezelés és jelentős módosítás (25. cikk (5) bekezdés)	Konfigurációkezelés (6. fejezet), 6.2.1. alapkonfiguráció [A][J][M]	Részleges	Jelentős módosítás és rendeltetés-változás vizsgálata, szerepkörváltás kezelése

cikk (1) bekezdés, 3. cikk 23. pont)			
Forgalomba hozatal utáni nyomon követés (72. cikk)	18.13.1. rendszer monitorozása [A][J][M]	Csekély	Nyomonkövetési terv a műszaki dokumentáció részeként, teljesítmény- és kockázatkövetés
MI-jártasság (4. cikk)	Kiberbiztonsági tv. 6. § (5) a) képzési kötelezettség; 3.2.1. biztonságtudatossági képzés [A][J][M]; 3.9.1. szerepkör alapú képzés [A][J][M]	Részleges	MI-specifikus tartalom, a felügyeletet ellátó személyek célzott képzése
Alapjogi hatásvizsgálat és tájékoztatás (27. cikk, 26. cikk (7) és (11) bekezdés)	Nincs megfelelője	Nincs	Alapjogi hatásvizsgálat az érintett alkalmazói körben, munkavállalók és érintettek tájékoztatása, összekapcsolás az adatvédelmi hatásvizsgálattal
Megfelelőségértékelés, EU-megfelelőségi nyilatkozat, CE-jelölés, regisztráció (43., 47., 48., 49. cikk)	Auditkultúra, bizonyítékezelés	Csekély	Belső ellenőrzésen alapuló eljárás (VI. melléklet) vagy bejelentett szervezet bevonása, nyilatkozat, regisztráció az uniós adatbázisban