MAGYAR KÖZLÖNY 8. szám

MAGYARORSZÁG HIVATALOS LAPJA
2025. január 31., péntek

Tartalomjegyzék

III. Kormányrendeletek

A Kormány 7/2025. (I. 31.) Korm. rendelete a távhőszolgáltatás versenyképesebbé tételéről szóló 2008. évi LXVII. törvény és a megújuló energiaforrásból vagy hulladékból nyert energiával termelt villamos energia, valamint a kapcsoltan termelt villamos energia kötelező átvételéről és átvételi áráról szóló 389/2007. (XII. 23.) Korm. rendelet veszélyhelyzet ideje alatt történő eltérő alkalmazásáról

[1] A megújuló energiatermelők támogatási rendszereit a megváltozott piaci körülményekhez szükségszerű igazítani. Ennek részeként a szabadpiacra önként kilépő kötelező átvételre jogosult termelők továbbra is élvezhetik az adómentességet, a kiszámíthatóbb, tervezhetőbb finanszírozás céljából a kötelező átvételi árat a megelőző évi infláció mértékére figyelemmel, a megelőző év kötelező átvételi ára alapján vagy a megelőző év kötelező átvételi ára alapján éves indexálással állapítják meg.

[2] A kötelező átvételi támogatási rendszer kiszámíthatóbb és tervezhetőbb finanszírozása céljából a kötelező átvételi ár mértéke a megelőző év inflációjának mértékére tekintettel kerül meghatározásra.

[3] A Kormány az Alaptörvény 53. cikk (1) bekezdésében meghatározott eredeti jogalkotói hatáskörében, figyelemmel a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény 80. és 81. §-ára, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. § Az Ukrajna területén fennálló fegyveres konfliktusra, illetve humanitárius katasztrófára tekintettel, valamint ezek magyarországi következményeinek az elhárítása és kezelése érdekében veszélyhelyzet kihirdetéséről és egyes veszélyhelyzeti szabályokról szóló 424/2022. (X. 28.) Korm. rendelet (a továbbiakban: 424/2022. Korm. rendelet) szerinti veszélyhelyzet ideje alatt a távhőszolgáltatás versenyképesebbé tételéről szóló 2008. évi LXVII. törvény 10. § 1. pont 1.5. alpontjában foglaltaktól eltérően a villamos energia kötelező átvételi rendszerében értékesítő termelőkre az energiaellátó fogalmát nem kell alkalmazni.

2. § (1) A 424/2022. Korm. rendelet szerinti veszélyhelyzet ideje alatt a megújuló energiaforrásból vagy hulladékból nyert energiával termelt villamos energia, valamint a kapcsoltan termelt villamos energia kötelező átvételéről és átvételi áráról szóló 389/2007. (XII. 23.) Korm. rendelet (a továbbiakban: KÁT rendelet) 3. § (4) bekezdésében és 5. számú mellékletében foglaltakat a (2)–(5) bekezdés szerinti időszakokra vonatkozóan a következőkben foglalt eltérésekkel kell alkalmazni.

(2) A megújuló energiaforrásból termelt villamos energia kötelező átvételi és prémium típusú támogatásáról szóló rendelet szerinti prémium típusú támogatás szabályai szerinti elszámolásra váltó KÁT termelőre vonatkozó kötelező átvételi árak kivételével a KÁT rendelet 5. számú melléklete szerinti indexálás nem alkalmazandó 2025. január 1-jétől a veszélyhelyzet végéig, de legfeljebb a 2029. év végéig, hanem a kötelező átvételi árak a tárgyévet megelőző évre megállapított szinten maradnak.

(3) Ha a Központi Statisztikai Hivatal által a tárgyévet megelőzően utoljára közzétett, a megelőző év azonos időszakához viszonyított aktuális (utolsó) éves fogyasztói árindex értéke az 1,06-ot eléri, akkor a tárgyévre a (2) bekezdés nem alkalmazandó.

(4) A KÁT rendelet 3. § (4) bekezdése szerinti közzététel során a Magyar Energetikai és Közmű-szabályozási Hivatal (a továbbiakban: Hivatal) a (2)–(3) bekezdést is figyelembe vevő számítást végzi el.

(5) A Hivatal a honlapján 2025. január 31. napjáig közzéteszi a 2025. évre vonatkozóan a KÁT rendelet 3. § (4) bekezdése szerinti alkalmazandó kötelező átvételi árakat és azok időben egyenletes termelés feltételezésével számított átlagát.

3. § Ez a rendelet a kihirdetése napján 23 órakor lép hatályba.

4. § E rendelet 2. § (2)–(4) bekezdésében foglalt rendelkezéseit a 2025. évre vonatkozó ármegállapítási eljárás során is alkalmazni kell.

Orbán Viktor s. k.,
miniszterelnök

IV. A Magyar Nemzeti Bank elnökének rendeletei, valamint az önálló szabályozó szerv vezetőjének rendeletei

A Szabályozott Tevékenységek Felügyeleti Hatósága elnökének 1/2025. (I. 31.) SZTFH rendelete a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról

[1] Kiemelten fontos a nemzet biztonsága érdekében a fenyegetések és kockázatok elleni védekezés, amely magában foglalja a személyek, eszközök, információk és infrastruktúrák védelmét. Mindez egyben jelenti a fizikai biztonságot – így különösen az épületek, berendezések védelmét – és az információbiztonságot, ideértve az adatok védelmét.

[2] A hálózatba kapcsolt digitális eszközöknek, rendszereknek a fizikai és virtuális térben történő egyidejű használata az élet mindennapi részévé vált. A hálózatok sérülékenységére kockázatot jelentő, a kibertérben felmerülő – ma már a világ bármely pontjáról érkező – kiberfenyegetések folyamatosan növekvő száma miatt a kiberbiztonsági szabályozás célja a kibertámadások megelőzése és a már bekövetkezett incidensek hatásainak csökkentése.

[3] A nemzetgazdaság biztonságos működése érdekében kiemelten fontos az elektronikus információs rendszerek fenyegetéseinek mérséklése és a kulcsfontosságú ágazatokban a szolgáltatások folyamatosságának biztosítása.

[4] A globális védekezés szükségességét felismerve alkotta meg az Európai Unió az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvet, amely egy egységes védelmi háló kialakítását célozza meg, biztosítva a gazdaság működéséhez szükséges szervezetek magas szintű védelmét.

[5] A Szabályozott Tevékenységek Felügyeleti Hatósága elnöke rendeletének célja a fenti célkitűzésekkel összhangban a kiberbiztonsági követelmények teljesülésének vizsgálatára irányuló kiberbiztonsági audit alapvető szabályainak lefektetése, valamint a kiberbiztonsági audit rendeletben korlátozott díjának meghatározása. A kiberbiztonsági audit célja, hogy egy független auditor vizsgálja meg azt, hogy az audittal érintett szervezetek elektronikus információs rendszerei mennyire ellenállóak a kiberbiztonsági fenyegetésekkel szemben.

[6] A hazai gazdaságban a vállalkozások alkotják a gazdasági struktúra gerincét. A rendelet megalkotását megelőzően a Szabályozott Tevékenységek Felügyeleti Hatósága és a Magyar Kereskedelmi és Iparkamara több alkalommal is egyeztetett annak érdekében, hogy a rendelet hatálya alá tartozó cégek kiberbiztonságra fordított adminisztrációs terhei és költségei mérsékeltek maradjanak.

[7] A kiberbiztonság ugyanakkor nemcsak az adatok védelmét szolgálja, hanem hozzájárul a vállalatok pénzügyi stabilitásához, és hosszú távon megerősítheti a vállalatok versenyképességét is, hiszen egy erős kiberbiztonsági rendszer növeli az ügyfelek bizalmát, és védelmet nyújt a potenciális károkkal szemben.

[8] A cselekvő állam részeként a Szabályozott Tevékenységek Felügyeleti Hatóságának célja, hogy a megfelelő kiberbiztonsági intézkedések biztosítsák az adatok bizalmasságát, sértetlenségét és rendelkezésre állását, ami hozzájárul Magyarország és az Európai Unió biztonságához, ellenálló képességének és versenyképességének növeléséhez.

[9] A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 81. § (6) bekezdés c) pontjában kapott felhatalmazás alapján, a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § n) és q) pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

1. § (1) A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 16. § (1) bekezdése szerinti kiberbiztonsági auditot (a továbbiakban: kiberbiztonsági audit) a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről szóló SZTFH rendelet alapján nyilvántartásba vett auditor végezhet.

(2) A kiberbiztonsági audit során az auditor ellenőrzi

a) a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja szerinti azon szervezet, amely egyúttal a Kiberbiztonsági tv. 2. és 3. melléklete szerinti szervezet is, valamint a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja és – a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerinti mikrovállalkozás kivételével – a Kiberbiztonsági tv. 1. § (1) bekezdés e) pontja szerinti szervezet (a továbbiakban együtt: szervezet) valamennyi elektronikus információs rendszerének biztonsági osztályba sorolása, valamint

b) a szervezet – auditor által kijelölt – elektronikus információs rendszerei biztonsági osztályának megfelelő, a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MKr.) szerinti védelmi intézkedések alkalmazását, és felméri a védelmi intézkedések

megfelelőségét bizonyítékok begyűjtésére és az azok objektív kiértékelésére irányuló módszeres, független és dokumentált eljárás lefolytatásával.

(3) A kiberbiztonsági audit kiterjed

a) a kockázatmenedzsment keretrendszer és a biztonsági osztályba sorolás,

b) az elektronikus információs rendszerekhez kapcsolódó, a szervezet elektronikus információs rendszereinek védelmével összefüggő dokumentumok – ideértve a szervezet belső szabályozó eszközeit, szerződéseket –, illetve eljárások,

c) az elektronikus információs rendszerekben alkalmazott hardver, szoftver vagy firmware elemekben megvalósított funkciók, kezelésükre vonatkozó bizonyítékok, a kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltatóval szembeni elvárások,

d) az elektronikus információs rendszerek védelmét támogató folyamatokban részt vevő valamennyi természetes személy ilyen irányú tevékenysége,

e) az elektronikus információs rendszerek védelme tekintetében a személyi feltételek és az ehhez kapcsolódó munkaköri felelősségek, valamint

f) a szervezet által meghatározott eljárások gyakorlati megvalósulása

vizsgálatára.

2. § (1) A kiberbiztonsági auditot

a) „alap" biztonsági osztályba sorolt elektronikus információs rendszer esetén „alap", „jelentős" vagy „magas" biztonsági osztályra,

b) „jelentős" biztonsági osztályba sorolt elektronikus információs rendszer esetén „jelentős" vagy „magas" biztonsági osztályra,

c) „magas" biztonsági osztályba sorolt elektronikus információs rendszer esetén „magas" biztonsági osztályra

nyilvántartásba vett auditor végezheti.

(2) A kiberbiztonsági audit során az MKr. szerinti védelmi intézkedések vizsgálatának módszereként

a) a dokumentumvizsgálat,

b) az interjú,

c) a teszt vagy

d) a Kiberbiztonsági tv. 22. § (1) bekezdése szerinti vizsgálati tevékenységek

alkalmazhatóak.

(3) A kiberbiztonsági auditban közreműködő vizsgáló laboratórium jogosult a (2) bekezdésben felsorolt vizsgálati módszereket alkalmazni.

3. § (1) Az 1. § (2) bekezdés b) pontja szerinti vizsgálat kiterjed a szervezet

a) „alap" biztonsági osztályba sorolt elektronikus információs rendszereinek legalább 40%-ára, de ha van, legalább egy „alap",

b) „jelentős" biztonsági osztályba sorolt elektronikus információs rendszereinek legalább 60%-ára, de ha van, legalább egy „jelentős",

c) „magas" biztonsági osztályba sorolt elektronikus információs rendszereinek legalább 70%-ára, de ha van, legalább egy „magas"

elektronikus információs rendszerére.

(2) Az 1. § (2) bekezdés b) pontja szerinti vizsgálatnak a szervezet összes elektronikus információs rendszerének legalább 50%-ára ki kell terjednie.

(3) A kiberbiztonsági audit elvégzésére vonatkozó megállapodás (a továbbiakban: megállapodás) megkötése céljából a szervezet az elektronikus információs rendszereinek biztonsági osztályba sorolását tartalmazó 1. melléklet szerinti nyilvántartást, valamint a kitöltött, a szervezetre vonatkozó 2. melléklet szerinti kérdőívet az auditor rendelkezésére bocsátja. A 2. melléklet szerinti kérdőívhez tartozó kitöltési útmutatót a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: Hatóság) honlapján közzéteszi.

(4) A szervezet az auditor részére átadja a korábban lefolytatott kiberbiztonsági audit eredményét, valamint az annak során keletkezett bizonyítékokat, az elektronikus információs rendszerekre és eszközökre, szervezetre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat, illetve a független, képesített ellenőr által készített ellenőri jelentéseket.

(5) Az auditor a (3) és (4) bekezdés szerinti adatok alapján, az (1) és (2) bekezdés alkalmazásával jelöli ki az 1. § (2) bekezdés b) pontja szerinti vizsgálattal érintett elektronikus információs rendszereket.

(6) Ha a szervezetnél már végeztek kiberbiztonsági auditot, akkor a kijelölésnél az auditornak figyelembe kell vennie a korábban lefolytatott kiberbiztonsági auditot, és az (5) bekezdés szerinti kijelölést úgy kell elvégeznie, hogy az a korábban lefolytatott kiberbiztonsági audittal együttesen kiterjedjen

a) az „alap" biztonsági osztályba sorolt elektronikus információs rendszerek legalább 70%-ára és

b) az összes „jelentős" vagy „magas" biztonsági osztályba sorolt elektronikus információs rendszerre.

(7) A korábban lefolytatott kiberbiztonsági auditot követően létrehozott, valamint a korábban lefolytatott kiberbiztonsági audit eredményeként „nem felel meg" értékelést kapott elektronikus információs rendszereket az auditornak az 1. § (2) bekezdés b) pontja szerinti vizsgálatra ki kell jelölnie.

4. § (1) A kiberbiztonsági audit – általános forgalmi adó nélkül számított – legmagasabb díját a 3. melléklet tartalmazza.

(2) A szervezet a megállapodásban meghatározza azokat a kapcsolattartó személyeket, akik a kiberbiztonsági audit során gondoskodnak a 2. § (2) bekezdés a) pontja szerinti dokumentumvizsgálathoz szükséges dokumentumok auditor részére történő rendelkezésre bocsátásáról, valamint biztosítják a 2. § (2) bekezdés b)–d) pontja szerinti vizsgálatok elvégzésének feltételeit.

(3) Az auditor meghatározza a kiberbiztonsági audit lefolytatásának ütemezését, ennek keretében rész- és véghatáridőt határozhat meg a Kiberbiztonsági tv.-ben a kiberbiztonsági audit elvégzésére meghatározott határidőkre figyelemmel.

(4) A szervezet által a kiberbiztonsági audit során átadott dokumentumok, az audit eljárás és eredménytermékeinek nyelve a magyar, amitől a felek a megállapodásban eltérhetnek.

5. § (1) A kiberbiztonsági audit megkezdése előtt az auditor auditálási tervet készít, amely tartalmazza

a) a kiberbiztonsági audit lefolytatásában részt vevő személyek megnevezését,

b) „jelentős" vagy „magas" biztonsági osztályba sorolt elektronikus információs rendszerre kiterjedő audit esetén a közreműködő vizsgáló laboratóriumot és a vizsgáló laboratórium által a kiberbiztonsági audit során elvégzendő tevékenységek körét,

c) a szervezet által átadott, a 4. melléklet szerinti eltérések és helyettesítő védelmi intézkedések nyilvántartását,

d) az 1. § (2) bekezdés b) pontja szerinti vizsgálatra kijelölt elektronikus információs rendszerek megnevezését,

e) az auditálási folyamatban azoknak az eljárásoknak a meghatározását, amelyekben az szervezet aktív közreműködése szükséges, megjelölve a közreműködés módját, valamint

f) az auditálási folyamat tervezett ütemezését.

(2) Az auditálási tervet az auditor a szervezet részére átadja.

(3) Az auditor jogosult a kiberbiztonsági audit során minden, a szervezet és elektronikus információs rendszerei biztonságával kapcsolatba hozható dokumentum megismerésére.

(4) Az elektronikus információs rendszerek biztonságáért felelős személy a kiberbiztonsági audit során az auditor által meghatározott módon – helyszínen, illetve távolról – biztosítja és végigköveti a kiberbiztonsági audit folyamatát.

(5) A kiberbiztonsági audit során az auditor az 5. melléklet szerinti auditori módszertan alapján jár el.

(6) Az 1. § (2) bekezdés b) pontja szerinti vizsgálat során az MKr. szerinti egyes követelménycsoportok esetében alkalmazandó vizsgálati módszereket, valamint a követelménycsoportok kiberbiztonsági audit eljárás szempontjából lényeges jellemzőit a 6. melléklet tartalmazza. Az MKr. szerinti követelménycsoportok esetében vizsgálandó, a követelményben megfogalmazott biztonsági cél teljesülését biztosító elemi követelményeket a 7. melléklet tartalmazza.

(7) A kiberbiztonsági audit lezárásakor az auditor a kiberbiztonsági audit során keletkezett bizonyítékokat és az audit eredményét tartalmazó, a 8. melléklet szerinti tartalommal összeállított magyar nyelvű auditjelentést legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel ellátott, nyomtatható formátumban megküldi a vizsgált szervezetnek.

(8) Az auditor a (7) bekezdés szerinti auditjelentést, valamint annak a Hatóság által a honlapján meghatározott, gépi feldolgozást biztosító specifikáció szerinti változatát haladéktalanul, de legkésőbb az auditjelentés kiállítását követő 7 napon belül megküldi a Hatóság részére.

(9) Az auditor a kiberbiztonsági auditjelentés mellékleteként auditigazolást állít ki, amely tartalmazza
a) a kiállító auditor megnevezését, székhelyének címét és a Hatóság általi nyilvántartásba vételekor kapott azonosító számát,
b) a szervezet megnevezését és székhelyének címét,
c) az auditigazolás kiállításának dátumát,
d) a vizsgált elektronikus információs rendszerek számát,
e) a szervezet ellenálló-képességi indexének az 5. melléklet 2.3.2. pontjában foglalt táblázat C oszlopa szerinti szövegszerű értékelését.

6. § (1) Az auditor részére a szervezet által átadott információk, adatok, dokumentumok magas szintű védelmét az auditor adminisztratív, fizikai, illetve logikai eszközökkel biztosítja.
(2) Az auditor a vizsgálati eredményeket és az azokhoz tartozó bizonyítékokat kizárólag a vizsgált szervezet és a Hatóság részére adhatja át.
(3) A szervezet az auditor által átadott bizonyítékokat a kiberbiztonsági audit lezárásának időpontjától számított 5 évig megőrzi.

7. § Ez a rendelet a kihirdetését követő 3. napon lép hatályba.

8. § Ez a rendelet az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

Dr. Nagy László s. k.,
elnök

1. melléklet az 1/2025. (I. 31.) SZTFH rendelethez

Elektronikus információs rendszerek nyilvántartása

	A	B	C	D	E	F	G
1.	Elektronikus információs rendszer (a továbbiakban: EIR) megnevezése	Az EIR által támogatott üzleti cél	MKr. 1. melléklete szerinti besorolási szempont azonosító	Szempont teljesülése bizalmasság szempontjából (Igen/Nem)	Szempont teljesülése sértetlenség szempontjából (Igen/Nem)	Szempont teljesülése rendelkezésre állás szempontjából (Igen/Nem)	Indoklás
2.			Az „alap” biztonsági osztály esetében legfeljebb csekély káresemény következhet be, mivel				
3.			2.2.2.1.				
4.			2.2.2.2.				
5.			2.2.2.3.				
6.			2.2.2.4.				
7.			A „jelentős” biztonsági osztály esetében közepes káresemény következhet be, mivel				
8.			2.2.3.1.				
9.			2.2.3.2.				
10.			2.2.3.3.				
11.			2.2.3.4.				
12.			2.2.3.5.				
13.			A „magas” biztonsági osztály esetében nagy káresemény következhet be, mivel				
14.			2.2.4.1.				
15.			2.2.4.2.				
16.			2.2.4.3.				
17.			2.2.4.4.				
18.			2.2.4.5.				
19.			2.2.4.6.				
20.			2.2.4.7.				

A szervezetre vonatkozó kérdőív

	A	B
1.	**Kérdés**	**Válasz**
2.	A szervezet előző üzleti évi nettó árbevétele	
3.	Azonosított EIR-ek száma (db)	
4.	„Alap" biztonsági osztályba sorolt EIR-ek száma (db)	
5.	„Jelentős" biztonsági osztályba sorolt EIR-ek száma (db)	
6.	„Magas" biztonsági osztályba sorolt EIR-ek száma (db)	
7.	„Jelentős" biztonsági osztályba sorolt EIR-ekben található egyedi fejlesztésű szoftverek száma (db)	
8.	„Magas" biztonsági osztályba sorolt EIR-ekben található egyedi fejlesztésű szoftverek száma (db)	
9.	Nyilvános szolgáltatások száma (db)	
10.	Publikus doménnevek száma (db)	
11.	Üzemeltetett szerverek száma (db)	
12.	Magyarországi telephelyek száma (db)	
13.	A szervezet munkavállalóinak száma (fő)	
14.	A szervezet végez-e rendszerüzemeltetést? (igen/nem)	
15.	A szervezet saját szervertermet üzemeltet? (igen/nem)	
16.	A szervezet végez-e informatikai fejlesztési tevékenységet? (igen/nem)	
17.	A szervezet kizárólag integrált szolgáltatást nyújtó kész (dobozos) szoftvereket használ? (igen/nem)	
18.	A szervezetnél van-e egyedileg fejlesztett kódot futtató EIR? (igen/nem)	
19.	A szervezet igénybe vesz-e Software-as-a-Service szolgáltatást?	
20.	Mennyi felhasználói végpont található a szervezetnél? (db)	
21.	ebből desktop, laptop (db)	
22.	ebből céges mobiltelefon (db)	
23.	Magántulajdonú végpontról EIR-elérés engedélyezett-e?	
24.	A szervezet EIR-jeinek felhasználószáma (db)	
25.	ebből munkavállaló	
26.	ebből szolgáltatásként igénybe vevő külső fél	

A kiberbiztonsági audit legmagasabb díja

1. A kiberbiztonsági audit – általános forgalmi adó nélkül számított – legmagasabb díját a következők szerint kell kiszámítani.

1.1. A szervezet előző üzleti évi nettó árbevétele alapján a következő táblázat szerinti szorzószámot kell figyelembe venni.

	A	B
1.	**A szervezet előző üzleti évi nettó árbevétele**	**Szorzószám**
2.	árbevétel ≤ 1 milliárd Ft	0,9
3.	1 milliárd Ft < árbevétel ≤ 5 milliárd Ft	1,1
4.	5 milliárd Ft < árbevétel ≤ 10 milliárd Ft	1,9
5.	10 milliárd Ft < árbevétel ≤ 15 milliárd Ft	2,5
6.	15 milliárd Ft < árbevétel ≤ 25 milliárd Ft	2,75
7.	25 milliárd Ft < árbevétel ≤ 40 milliárd Ft	3
8.	árbevétel > 40 milliárd Ft	4

1.2. A szervezet 1. mellékletben szereplő elektronikus információs rendszereinek darabszáma alapján a következő táblázat szerinti szorzószámot kell figyelembe venni.

	A	B
1.	**EIR-ek darabszáma**	**Szorzószám**
2.	1–5	1
3.	6–15	2,5
4.	16 vagy annál több	4

1.3. A szervezet 1. mellékletben szereplő elektronikus információs rendszerei biztonsági osztálya alapján a következő szorzószámot kell figyelembe venni:
1.3.1. ha a szervezet valamennyi elektronikus információs rendszerének biztonsági osztálya „alap” biztonsági osztály, a szorzószám 1,
1.3.2. – az 1.3.3. pont kivételével – ha a szervezet bármely elektronikus információs rendszerének biztonsági osztálya „jelentős” biztonsági osztály, a szorzószám 3,
1.3.3. ha a szervezet bármely elektronikus információs rendszerének biztonsági osztálya „magas” biztonsági osztály, a szorzószám 5.

1.4. A kiberbiztonsági audit – általános forgalmi adó nélkül számított – legmagasabb díja az 1.1., 1.2. és az 1.3. pont szerinti szorzószámok, valamint 1 750 000 forint szorzataként előálló összeg.

4. melléklet az 1/2025. (I. 31.) SZTFH rendelethez

Eltérések és helyettesítő védelmi intézkedések nyilvántartása

	A	B	C	D	E	F	G	H
1.	Érintett EIR megnevezése	Követelménycsoport hivatkozás az MKr. 2. melléklete szerint	Relevancia	Releváns esetben helyettesítő kontrollcsoport	Eltérés vagy helyettesítő védelmi intézkedés okának típusa az MKr. 1. melléklet 3.2.1–3.2.7. pontja és 4.2–4.2.4. pontja alapján	A kontrollcsoport szempontjából releváns összes fenyegetés az MKr. 3. melléklete szerint	A kontrollcsoport szempontjából releváns összes fenyegetés kockázati szintje	A maradvány-kockázatok felvállalásának indoklása
2.								
3.								
4.								

5. melléklet az 1/2025. (I. 31.) SZTFH rendelethez

Auditori módszertan

1. A vizsgálati módszerek

1.1. Általános szabályok

1.1.1. Az audit módszertan a NIST Special Publication 800-53A Revision 5 dokumentum alapján került kialakításra.

1.1.2. A vizsgálatok célja annak megállapítása és bizonyítékokkal történő alátámasztása, hogy
1.1.2.1. az MKr. szerinti elvárt védelmi intézkedések megvalósítása nem tartalmaz hiányosságokat és hibákat,
1.1.2.2. az MKr. szerinti védelmi intézkedések tervezett módon, megfelelően működnek.

1.1.3. Az MKr. szerinti egyes követelménycsoportok értékelésére az 1.2.1–1.2.3.2. pont szerinti vizsgálati módszerek alkalmazandóak.

1.1.4. A bizonyítékok rendelkezésre bocsátásának, a dokumentumok vizsgálatra történő átadásának, az interjúkérdések megválaszolásának, illetve a tesztek feltételei biztosításának elmulasztása az adott követelményre „nem megfelelt" döntést eredményez.

1.2. Általános vizsgálati módszerek

1.2.1. Dokumentumvizsgálat

1.2.1.1. A dokumentumvizsgálat során az elektronikus információs rendszerek biztonsági osztályától, a szervezet sajátosságaitól, az adott követelménycsoporttól függően az auditor a szervezet által rendelkezésére bocsátott dokumentumok alapján elemzi a bizonyítékokat a védelmi intézkedéseknek való megfelelés szempontjából.

1.2.1.2. A dokumentumvizsgálat különösen a következő dokumentumokra terjed ki:
1.2.1.2.1. magas szintű irányítási dokumentumok, ideértve az informatikai biztonsági stratégiát, informatikai biztonsági politikát, rendszerbiztonsági tervet, kockázatértékelési, kockázatkezelési politikát,
1.2.1.2.2. a szervezet belső szabályozó eszközei, eljárásokra vonatkozó előírások, utasítások, útmutatók, ideértve az informatikai biztonsági szabályzatot, hozzáférés-szabályozást, képzésekkel kapcsolatos szabályozásokat, felhasználói, illetve adminisztrátori útmutatókat, összeférhetetlenséggel, viselkedési elvárásokkal kapcsolatos szabályozást, a szabályzatok, utasítások felülvizsgálatára, frissítésére, jóváhagyására vonatkozó szabályozást, rendszerkonfiguráció módosítására és ellenőrzésére vonatkozó eljárásokat, azonosítási és hitelesítési eljárásokat, követelményeket, azonosítók kezelését, informatikai eszközöket, szoftverek beszerzésével, telepítésével kapcsolatos eljárásokat, engedélyezési folyamatot, fizikai és személyi biztonsággal kapcsolatok szabályozásokat,
1.2.1.2.3. rendszerleírásokkal és nyilvántartásokkal kapcsolatos dokumentációk, ideértve a rendszerterveket, rendszerleltárt, szoftverleltárt, rendszer-architektúra leírást, rendszer-konfigurációk leírását, szoftvernyilvántartást, kriptográfiai eljárások nyilvántartását, kriptográfiai mechanizmusok követelményeit, kriptográfiai kulcsok kezelésének elvárásait és dokumentációit, interfészek leírását, az ellátási lánc védelmére vonatkozó eljárásokat, az ellátási lánc biztonságával kapcsolatos dokumentációkat, titoktartási megállapodásokat, képzésekkel kapcsolatos nyilvántartásokat, fizikai biztonsági intézkedéseket, oktatással kapcsolatos dokumentációkat,
1.2.1.2.4. változáskezeléssel kapcsolatos dokumentációk, ideértve a tervezési, hatásvizsgálati, tesztelési, átvételi és engedélyezési eljárásokat, a rendszerfejlesztés életciklus folyamatában alkalmazandó minőségellenőrzési eljárásokat, megvalósított átvételi eljárások dokumentációit,
1.2.1.2.5. vészhelyzeti tervezéssel, incidenskezeléssel, ellenőrzéssel, mentéssel, naplózással kapcsolatos dokumentációk, ideértve az incidensekre való reagálási tevékenységek dokumentumait, ellenőrzési terveket, végrehajtott ellenőrzési dokumentációkat, korábbi sérülékenységvizsgálatok eredményeit, mentések szabályozását, mentett információk védelmét, naplózás szabályozását, naplók védelmét.

1.2.2. Interjú

1.2.2.1. Az interjúk során az elektronikus információs rendszerek biztonsági osztályától, a szervezet sajátosságaitól, az adott követelménycsoporttól függően az auditor a szervezet által rendelkezésre bocsátott dokumentumok alapján írásban feltett interjúkérdésekkel, továbbá személyes interjúk során a dokumentumvizsgálathoz képest további bizonyítékok begyűjtését, a felmerült kérdések tisztázását végzi a folyamatok, eljárások gyakorlati megvalósításának megismerése érdekében.

1.2.2.2. A személyes interjúknál az auditor – az elektronikus információs rendszerek biztonságáért felelős személy jelenlétében – helyszíni vagy – elektronikus hírközlő eszköz igénybevételével – távoli interjúkat folytat le a vizsgált követelménycsoporttal kapcsolatos releváns feladatokat ellátó vezetőkkel, munkatársakkal, ideértve a rendszertervezéssel, beszerzéssel, jóváhagyással, engedélyezéssel, működtetéssel, karbantartással, ellenőrzéssel, incidenskezeléssel kapcsolatosan felelősséggel rendelkező személyeket, illetve technikai kérdésekben a rendszergazdákat, hálózati rendszergazdákat.

1.2.3. Teszt

1.2.3.1. Az auditor a tesztelések során az elektronikus információs rendszerek biztonsági osztályától, a szervezet sajátosságaitól, illetve az adott követelménycsoporttól függően automatizált ellenőrző programokkal, vagy – a szervezet munkatársainak közreműködésével végrehajtott – céltesztekkel, a szervezeti tevékenységek és céltesztek naplózási nyomainak lekérdezésével a szervezetnek azokat az informatikai mechanizmusait és tevékenységeit ellenőrzi, amelyek megvalósítják az adott követelménycsoportra elvárt intézkedéseket.

1.2.3.2. A tesztelési folyamat során az auditor a tényleges és az elvárt működés összehasonlítása érdekében a tesztelendő követelménycsoport elemi követelményei teljesülését ellenőrzi.

2. Az auditálási eljárás

2.1. Biztonsági osztályba sorolás vizsgálata

2.1.1. Az auditor az 1. § (2) bekezdés a) pontja szerinti vizsgálat során ellenőrzi a 3. § (3) bekezdése szerint átadott, a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását tartalmazó nyilvántartásban foglalt valamennyi elektronikus információs rendszer biztonsági osztályba sorolásának megfelelőségét.

2.1.2. Az auditor ellenőrzi a besorolási döntéseket megalapozó bizonyítékokat az MKr. 1. melléklet 2.2.2–2.2.4.7. pontjában meghatározott feltételek fennállása szempontjából.

2.1.3. Az auditor ellenőrzi, hogy a biztonsági osztályba sorolásra vonatkozó döntések az MKr. 1. melléklet 2.1.2. pontjával összhangban a szervezet vezetője által jóváhagyásra kerültek-e.

2.1.4. Az auditor a biztonsági osztályba sorolás értékelésénél dokumentumvizsgálat és interjú általános vizsgálati módszereket alkalmaz.

2.1.5. Az egyes elektronikus információs rendszerek biztonsági osztályba sorolásának megalapozottságát vizsgáló ellenőrzés eredménye lehet

2.1.5.1. „megfelelő”, ha a biztonsági osztályba sorolást megalapozó bizonyítékok az elektronikus információs rendszer nyilvántartásban szereplő biztonsági osztályát alátámasztják,

2.1.5.2. „nem megfelelő”, ha a biztonsági osztályba sorolást megalapozó bizonyítékok az elektronikus információs rendszer nyilvántartásban szereplő biztonsági osztályát nem támasztják alá.

2.1.6. A biztonsági osztály „nem megfelelő” értékelése esetén az auditor az MKr. rendelkezéseinek megfelelő biztonsági osztályba sorolásra tesz javaslatot, de a 2.2. és 2.3. pont szerinti értékelést a szervezet által megállapított biztonsági osztályra figyelemmel végzi el.

2.1.7. A biztonsági osztályba sorolás vizsgálatának eredményét az auditjelentés tartalmazza.

2.2. Az elektronikus információs rendszer követelménycsoportok szerinti értékelése

2.2.1. A 6. mellékletben foglalt táblázat B oszlopában

2.2.1.1. „SZ” értékkel jelölt követelménycsoport szervezeti szinten, azaz valamennyi EIR-re egységesen vonatkoztatva vizsgálandó,

2.2.1.2. „EIR” értékkel jelölt követelménycsoport EIR-enként vizsgálandó.

2.2.2. Alkalmazhatósági értékelés

2.2.2.1. Az auditor az egyes követelménycsoportok alkalmazhatóságát a 2.2.1.1. és 2.2.1.2. pont szerint vizsgálja, és ennek során az auditálási tervben foglalt, az audittal érintett elektronikus információs rendszerekhez tartozó eltéréseket és helyettesítő intézkedéseket is értékeli.

2.2.2.2. Az auditor értékeli az eltérést alátámasztó dokumentumokat, indokolásokat a megállapított biztonsági osztálynak megfelelően, valamint az MKr. 1. melléklet 3.1–4.2.4. pontjában meghatározott feltételrendszernek való megfelelés alapján.

2.2.2.3. A követelménycsoport „nem alkalmazható” minősítést kap, ha a szervezet által átadott, 4. melléklet szerinti eltérések és helyettesítő intézkedések katalógusában a követelménycsoport eltérésként szerepel, az indokolás az auditor értékelése alapján megfelelően alátámasztott és az eltéréseket bemutató dokumentumok a szervezet vezetője vagy a kockázatok felvállalására jogosult szerepkört betöltő személy részéről jóváhagyásra kerültek.

2.2.2.4. Az auditor – a 2.2.2.3. pontban foglaltakon túl – indokolás mellett a vizsgált szervezeti vagy EIR-szintű követelménycsoportot a vizsgálatból kizárhatja, kivéve, ha a követelménycsoport a 6. mellékletben foglalt táblázat G oszlopában „Értékelésből nem kizárható”-ként került megjelölésre. A követelménycsoport ebben az esetben „nem alkalmazható” minősítést kap.

2.2.2.5. Ha a 2.2.2.3. vagy a 2.2.2.4. pont szerinti eset nem áll fenn, a követelménycsoport értékelése „alkalmazható”.

2.2.2.6. A „nem alkalmazható” követelménycsoport nem képezi az audit tárgyát.

2.2.3. Követelménycsoportok vizsgálata

2.2.3.1. A szervezeti szintű követelménycsoportok az audit eljárás során a szervezet valamennyi vizsgálatba bevont EIR-jére egységesen vonatkoztatva legalább egyszer vizsgálandóak.

2.2.3.2. Szervezeti szintű követelménycsoport esetén az auditor a szervezet EIR-jei közül a legmagasabb biztonsági osztályát veszi figyelembe.

2.2.3.3. A 2.2.2. pont szerinti értékelés során „alkalmazható” minősítést kapott követelménycsoportokat az auditor a 6. melléklet szerinti vizsgálati módszerekkel vizsgálja.

2.2.3.4. A 7. mellékletben foglalt táblázat követelménycsoportonként tartalmazza az elemi követelményeket, amelyek értékelésének eredménye, azaz az auditori döntés (AD) a következő lehet:

2.2.3.4.1. „nem alkalmazható” („NA”), ha a követelménycsoport a 2.2.2.3. vagy a 2.2.2.4. pont alapján nem került kizárásra, azonban a biztonsági cél, illetve az elemi követelmény nem értelmezhető;

2.2.3.4.2. „nem megfelelt” („NM”), ha az elemi követelmény teljesülésére nincs bizonyíték vagy a szervezet nem vállalja az intézkedés megvalósítását;

2.2.3.4.3. „megfelelt” (M), ha az auditor rendelkezésére állnak a kötelező vizsgálati módszerek alapján az elemi követelmény teljesülésére vonatkozó bizonyítékok.

2.2.4. Követelménycsoport értékelése

2.2.4.1. A követelménycsoport értékelése az elemi követelmények értékelése alapján történik a következők szerint:

2.2.4.1.1. „megfelelt”, ha a 7. melléklet szerinti elemi követelmények mindegyike „megfelelt” vagy „nem alkalmazható” értékelést kapott,

2.2.4.1.2. ha a vizsgált követelménycsoportra van egy vagy több olyan elemi követelmény, amelyre vonatkozóan az auditor „nem megfelelt” döntést hozott, akkor az auditor az eltérést minősíti. A minősítés során az auditor különösen a következő szempontokat veszi figyelembe:

2.2.4.1.2.1. a „nem megfelelt” döntések száma,

2.2.4.1.2.2. az auditornak a komplex rendszerre, más intézkedésekre vonatkozó ismeretei, figyelembe véve a nem megfelelőségek támadó oldali kihasználási lehetőségeit, amelyeket befolyásol,

2.2.4.1.2.2.1. az esetleges támadásokhoz a támadó részéről szükséges rendszerismeret szintje,

2.2.4.1.2.2.2. a rendszerhez való hozzáférés-igény szintje,

2.2.4.1.2.2.3. a támadáshoz szükséges kvalifikált ismeretek szintje,

2.2.4.1.2.2.4. a speciális eszközpark használati igénye,

2.2.4.1.2.2.5. támadási időszükséglet korlátai.

2.2.4.1.3. A 2.2.4.1.2–2.2.4.1.2.2.5. pont szerinti szempontok alapján az eltérés minősítése:

2.2.4.1.3.1. „elhanyagolható mértékű eltérés”: ha a vonatkozó biztonsági elvárások nem teljesülnek hiánytalanul, de ez az EIR biztonságát az auditor megítélése szerint nem érinti;

2.2.4.1.3.2. „kis mértékű eltérés”: ha a vonatkozó biztonsági elvárások kisebb hiányosságokkal, de alapvetően céljuknak megfelelően működnek;

2.2.4.1.3.3. „kiemelt mértékű eltérés”: ha az elvárt intézkedés fő céljai nem teljesülnek;

2.2.4.1.3.4. „kritikus mértékű eltérés”: ha az intézkedés nem megfelelése olyan súlyú, hogy a következő kockázatok bekövetkezési valószínűségét növeli:

2.2.4.1.3.4.1. személyes adatok bizalmasságának sérülése;

2.2.4.1.3.4.2. személyi sérülés bekövetkezése;

2.2.4.1.3.4.3. nemzeti adatvagyon sérülése;

2.2.4.1.3.4.4. létfontosságú rendszer rendelkezésre állása nem biztosított;

2.2.4.1.3.4.5. a szervezet üzlet- vagy ügymenete szempontjából nagy értékű, üzleti titkot vagy különösen érzékeny folyamatokat kezelő rendszer, vagy információt képező adat sérülése;

2.2.4.1.3.4.6. súlyos bizalomvesztés a szervezettel szemben, vagy kiemelt jogok sérülése;
2.2.4.1.3.4.7. jelentős közvetett vagy közvetlen anyagi kár.

2.2.5. Az EIR értékelése

2.2.5.1. Az EIR értékelésére összehasonlíthatóságot biztosító, kvantitatív számítási módszer alkalmazandó a követelménycsoportok értékelése alapján.

2.2.5.2. Az egyes követelménycsoportok értékelése alapján a következő számszerű értékek alkalmazandóak:
2.2.5.2.1. „megfelelt" esetén 0,
2.2.5.2.2. „elhanyagolható mértékű eltérés" esetén 1,
2.2.5.2.3. „kis mértékű eltérés" esetén 4,
2.2.5.2.4. „kiemelt mértékű eltérés" esetén 10,
2.2.5.2.5. „kritikus mértékű eltérés" esetén 1000.

2.2.5.3. A vizsgált EIR értékelésénél az auditor figyelembe veszi az adott követelménycsoportnak a 6. mellékletben foglalt táblázat F oszlopa szerinti típusát.

2.2.5.4. Az EIR értékelésének meghatározására a védelmi megfelelési index (a továbbiakban: VMI) szolgál, amelynek értékét az auditor a következő képlettel határozza meg:

$$\text{VMI} = 100 - 100 * \frac{2*\sum_{i=1}^{n} b_i + \sum_{j=1}^{m} t_j}{20n+10m}$$

2.2.5.5. A 2.2.5.4. pont szerinti képletben alkalmazott jelölések:
2.2.5.5.1. b_i: a 6. melléklet szerint „Biztosító" típusú követelménycsoport 2.2.5.2. pont szerinti számszerű értéke;
2.2.5.5.2. t_j: a 6. melléklet szerint „Támogató" típusú követelménycsoport 2.2.5.2. pont szerinti számszerű értéke;
2.2.5.5.3. n: a 6. melléklet szerinti „Biztosító" típusú követelménycsoportok számossága;
2.2.5.5.4. m: a 6. melléklet szerinti „Támogató" típusú követelménycsoportok számossága.

2.2.5.6. A VMI alapján az EIR-t az elvárásoktól való eltérés alapján az auditor szövegesen értékeli a következők szerint:

	A	B
1.	Eltérés mértéke	Az EIR-nek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő értékelése
2.	VMI ≥ 95	megfelel
3.	90 ≤ VMI < 95	alacsony kockázattal megfelel
4.	80 ≤ VMI < 90	jelentős kockázattal megfelel
5.	70 ≤ VMI < 80	magas kockázattal megfelel
6.	VMI < 70	nem felel meg

2.2.5.7. Az auditor a VMI 2.2.5.4. pont szerinti kiszámításakor minden EIR esetén beszámolja a szervezeti szintű követelménycsoportokat is.

2.3. A szervezet értékelése

2.3.1. Az auditor a szervezet ellenálló-képességi indexét (a továbbiakban: SZEKI) a következő képlettel határozza meg:

$$szervezet\ ellenálló - képességi\ indexe = \frac{\sum_{i=1}^{n} VMI_i}{n}$$

2.3.2. Az auditor a SZEKI szövegszerű értékelését a következő táblázatban foglaltak szerint végzi el:

	A	B	C
1.	Szervezet értékelése	A szervezetnek a védelmi intézkedések katalógusa elvárásainak való megfelelés szempontjából történő minősítése	Értékelés eredménye
2.	SZEKI ≥ 95	elhanyagolható kockázattal megfelel	megfelelt
3.	90 ≤ SZEKI < 95	alacsony kockázattal megfelel	auditált
4.	80 ≤ SZEKI < 90	közepes kockázattal megfelel	
5.	70 ≤ SZEKI < 80	magas kockázattal megfelel	
6.	SZEKI < 70	kritikus kockázattal nem felel meg	nem megfelelt

Az MKr. szerinti követelménycsoportok esetében a kiberbiztonsági audit során alkalmazandó vizsgálati módszerek, valamint a követelménycsoportok audit eljárás szempontjából lényeges jellemzői

	A	B	C	D	E	F	G
1.	MKr. 2. melléklete szerinti követelménycsoport	Jellege	Kötelezően alkalmazandó dokumentumvizsgálat	Kötelezően alkalmazandó interjú	Kötelezően alkalmazandó teszt	Típusa	Értékelésből nem kizárható
2.	1.1. Információbiztonsági szabályzat	SZ	X	X	-	Biztosító	X
3.	1.2. Elektronikus információs rendszerek biztonságáért felelős személy	SZ	X	X	-	Biztosító	X
4.	1.3. Információbiztonságot érintő erőforrások	SZ	X	X	-	Biztosító	-
5.	1.4. Intézkedési terv és mérföldkövei	SZ	X	X	-	Támogató	X
6.	1.5. Elektronikus információs rendszerek nyilvántartása	SZ	X	X	-	Biztosító	X
7.	1.6. Biztonsági teljesítmény mérése	SZ	X	X	-	Támogató	-
8.	1.7. Szervezeti architektúra	SZ	X	X	-	Támogató	-
9.	1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve	SZ	X	X	-	Biztosító	-
10.	1.10. Kockázatmenedzsment stratégia	SZ	X	X	-	Támogató	-
11.	1.11. Engedélyezési folyamatok meghatározása	SZ	X	X	-	Biztosító	-
12.	1.12. Szervezeti működés és üzleti folyamatok meghatározása	SZ	X	X	-	Támogató	-
13.	1.14. Biztonsági személyzet képzése	SZ	X	X	-	Támogató	-
14.	1.15. Tesztelés, képzés és felügyelet	SZ	X	X	-	Támogató	-
15.	1.16. Szakmai csoportokkal és közösségekkel való kapcsolattartás	SZ	X	X	-	Támogató	-
16.	1.17. Fenyegetettség tudatosító program	SZ	X	X	-	Támogató	-
17.	1.19. Kockázatmenedzsment keretrendszer	SZ	X	X	-	Támogató	-
18.	1.20. Kockázatkezelésért felelős szerepkörök	SZ	X	X	-	Támogató	-
19.	1.21. Ellátási lánc kockázatmenedzsment stratégiája	SZ	X	X	-	Támogató	X

20.	1.22. Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói	SZ	X	X	-	Támogató	-
21.	1.23. Folyamatos felügyeleti stratégia	SZ	X	X	-	Támogató	-
22.	2.1. Szabályzat és eljárásrendek	EIR	X	X	-	Biztosító	X
23.	2.2. Fiókkezelés	EIR	X	-	X	Biztosító	X
24.	2.3. Fiókkezelés – Automatizált fiókkezelés	EIR	X	-	-	Támogató	-
25.	2.4. Fiókkezelés – Automatizált ideiglenes és vészhelyzeti fiók kezelés	EIR	X	-	-	Biztosító	-
26.	2.5. Fiókkezelés – Fiókok letiltása	EIR	X	-	X	Támogató	-
27.	2.6. Fiókkezelés – Automatikus naplózási műveletek	EIR	X	-	X	Biztosító	X
28.	2.7. Fiókkezelés – Inaktivitásból fakadó kijelentkeztetés	EIR	X	-	-	Biztosító	-
29.	2.12. Fiókkezelés – Használati feltételek	EIR	X	-	-	Támogató	-
30.	2.13. Fiókkezelés – Fiókok szokatlan használatának felügyelete	EIR	X	X	-	Biztosító	-
31.	2.14. Fiókkezelés – Magas kockázatú személyek fiókjának letiltása	EIR	X	X	-	Támogató	-
32.	2.15. Hozzáférési szabályok érvényesítése	EIR	X	-	X	Biztosító	X
33.	2.28. Információáramlási szabályok érvényesítése	EIR	X	-	-	Támogató	-
34.	2.32. Információáramlási szabályok érvényesítése – Titkosított információk áramlásának irányítása	EIR	X	X	-	Biztosító	-
35.	2.59. Felelősségek szétválasztása	EIR	X	X	-	Biztosító	-
36.	2.60. Legkisebb jogosultság elve	EIR	X	-	-	Biztosító	X
37.	2.61. Legkisebb jogosultság elve – Hozzáférés biztosítása a biztonsági funkciókhoz	EIR	X	-	X	Biztosító	-
38.	2.62. Legkisebb jogosultság elve – Nem privilegizált hozzáférés biztosítása a nem biztonsági funkciókhoz	EIR	X	-	-	Támogató	-
39.	2.63. Legkisebb jogosultság elve – Hálózati hozzáférés a privilegizált parancsokhoz	EIR	X	-	-	Támogató	-
40.	2.65. Legkisebb jogosultság elve – Privilegizált fiókok	EIR	X	X	-	Támogató	-

41.	2.67. Legkisebb jogosultság elve – Felhasználói jogosultságok felülvizsgálata	EIR	X	X	-	Támogató	-
42.	2.69. Legkisebb jogosultság elve – Privilegizált funkciók használatának naplózása	EIR	X	-	X	Támogató	-
43.	2.70. Legkisebb jogosultság elve – Nem-privilegizált felhasználók korlátozása	EIR	X	-	-	Támogató	-
44.	2.71. Sikertelen bejelentkezési kísérletek	EIR	X	-	X	Biztosító	X
45.	2.75. A rendszerhasználat jelzése	EIR	X	-	X	Támogató	-
46.	2.81. Egyidejű munkaszakasz kezelés	EIR	X	-	-	Támogató	-
47.	2.82. Eszköz zárolása	EIR	X	-	X	Támogató	-
48.	2.83. Eszköz zárolása – Képernyőtakarás	EIR	X	-	X	Támogató	-
49.	2.84. A munkaszakasz lezárása	EIR	X	-	X	Támogató	-
50.	2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	EIR	X	-	X	Támogató	-
51.	2.100. Távoli hozzáférés	EIR	X	X	X	Biztosító	-
52.	2.101. Távoli hozzáférés – Felügyelet és irányítás	EIR	X	-	-	Biztosító	-
53.	2.102. Távoli hozzáférés – Bizalmasság és sértetlenség védelme titkosítás által	EIR	X	-	X	Biztosító	-
54.	2.103. Távoli hozzáférés – Menedzselt hozzáférés-felügyeleti pontok	EIR	X	X	-	Támogató	-
55.	2.104. Távoli hozzáférés – Privilegizált parancsok és hozzáférés	EIR	X	-	-	Támogató	-
56.	2.108. Vezeték nélküli hozzáférés	EIR	X	X	-	Biztosító	-
57.	2.109. Vezeték nélküli hozzáférés – Hitelesítés és titkosítás	EIR	X	-	-	Biztosító	-
58.	2.110. Vezeték nélküli hozzáférés – Vezeték nélküli hálózat letiltása	EIR	X	-	X	Támogató	-
59.	2.111. Vezeték nélküli hozzáférés – Felhasználók általi konfiguráció korlátozása	EIR	X	-	-	Támogató	-
60.	2.112. Vezeték nélküli hozzáférés – Antennák és átviteli teljesítmény	EIR	X	-	-	Támogató	-
61.	2.113. Mobil eszközök hozzáférés-ellenőrzése	EIR	X	X	-	Biztosító	-

62.	2.114. Mobil eszközök hozzáférés-ellenőrzése – Teljes eszköz vagy konténer-alapú titkosítás	EIR	X	-	X	Biztosító	-
63.	2.115. Külső elektronikus információs rendszerek használata	EIR	X	-	-	Támogató	-
64.	2.116. Külső rendszerek használata – Engedélyezett használat korlátozásai	EIR	X	-	-	Támogató	-
65.	2.117. Külső rendszerek használata – Hordozható adattárolók használatának korlátozása	EIR	X	-	-	Támogató	-
66.	2.121. Információmegosztás	EIR	X	X	-	Támogató	-
67.	2.124. Nyilvánosan elérhető tartalom	EIR	X	X	-	Támogató	-
68.	3.1. Szabályzat és eljárásrendek	SZ	X	X	-	Támogató	-
69.	3.2. Biztonságtudatossági képzés	SZ	X	X	-	Biztosító	X
70.	3.4. Biztonságtudatossági képzés – Belső fenyegetés	SZ	X	-	-	Támogató	-
71.	3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés	SZ	X	-	-	Támogató	-
72.	3.9. Szerepkör alapú biztonsági képzés	SZ	X	-	-	Támogató	-
73.	3.13. A biztonsági képzésre vonatkozó dokumentációk	SZ	X	-	X	Támogató	-
74.	4.1. Szabályzat és eljárásrendek	EIR	X	X	-	Biztosító	X
75.	4.2. Naplózható események	EIR	X	X	-	Biztosító	X
76.	4.3. Naplóbejegyzések tartalma	EIR	X	-	X	Biztosító	-
77.	4.4. Naplóbejegyzések tartalma – Kiegészítő naplóinformációk	EIR	X	-	-	Támogató	-
78.	4.5. Naplózás tárkapacitása	EIR	X	-	X	Támogató	-
79.	4.7. Naplózási hiba kezelése	EIR	X	X	-	Biztosító	-
80.	4.8. Naplózási hiba kezelése – Tárhelykapacitás figyelmeztetés	EIR	X	-	-	Támogató	-
81.	4.9. Naplózási hiba kezelése – Valós idejű riasztások	EIR	X	-	-	Biztosító	-
82.	4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel	EIR	X	X	X	Biztosító	-
83.	4.14. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Automatizált folyamatintegráció	EIR	X	-	-	Biztosító	-

84.	4.15. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Naplózási tárhelyek összekapcsolása	EIR	X	-	-	Támogató	-
85.	4.17. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Felügyeleti képességek integrálása	EIR	X	X	-	Támogató	-
86.	4.18. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Összevetés a fizikai felügyelettel	EIR	X	-	-	Támogató	-
87.	4.22. Naplóbejegyzések csökkentése és jelentéskészítés	EIR	X	-	-	Biztosító	-
88.	4.23. Naplóbejegyzések csökkentése és jelentéskészítés – Automatikus feldolgozás	EIR	X	-	-	Támogató	-
89.	4.24. Időbélyegek	EIR	X	-	X	Támogató	-
90.	4.25. Naplóinformációk védelme	EIR	X	X	-	Biztosító	-
91.	4.27. A naplóinformációk védelme – Tárolás fizikailag különálló rendszereken vagy rendszerelemeken	EIR	X	-	-	Támogató	-
92.	4.28. A naplóinformációk védelme – Kriptográfiai védelem	EIR	X	-	-	Támogató	-
93.	4.29. A naplóinformációk védelme – Privilegizált felhasználók hozzáférése	EIR	X	-	-	Biztosító	-
94.	4.33. Letagadhatatlanság	EIR	X	-	X	Biztosító	-
95.	4.38. A naplóbejegyzések megőrzése	EIR	X	-	-	Támogató	-
96.	4.40. Naplóbejegyzések létrehozása	EIR	X	-	X	Biztosító	X
97.	4.41. Naplóbejegyzések létrehozása – Az egész rendszerre kiterjedő és időbeli naplózási nyomvonal.	EIR	X	X	-	Támogató	-
98.	4.43. Naplóbejegyzések létrehozása – Felhatalmazott személyek változtatásai	EIR	X	-	-	Támogató	-
99.	5.1. Szabályzat és eljárásrendek	EIR	X	X	-	Támogató	-
100.	5.2. Biztonsági értékelések	EIR	X	-	X	Biztosító	X
101.	5.3. Biztonsági értékelések – Független értékelők	EIR	X	-	-	Biztosító	-
102.	5.4. Biztonsági értékelések – Kiberbiztonsági audit	EIR	X	-	-	Biztosító	X

103.	5.5. Biztonsági értékelések – Speciális értékelések	EIR	X	-	-	Támogató	-
104.	5.7. Információcsere	EIR	X	X	-	Támogató	-
105.	5.8. Információcsere – Átviteli engedélyek	EIR	X	-	-	Támogató	-
106.	5.10. Az intézkedési terv és mérföldkövei	EIR	X	-	-	Támogató	-
107.	5.12. Engedélyezés	EIR	X	X	X	Támogató	-
108.	5.15. Folyamatos felügyelet	EIR	X	X	-	Támogató	-
109.	5.16. Folyamatos felügyelet – Független értékelés	EIR	X	-	-	Támogató	-
110.	5.18. Folyamatos felügyelet – Kockázatmonitorozás	EIR	X	-	-	Támogató	-
111.	5.22. Behatolásvizsgálat – Független szakértő vagy csapat	EIR	X	-	-	Támogató	-
112.	5.25. Belső rendszerkapcsolatok	EIR	X	X	X	Támogató	-
113.	6.1. Szabályzat és eljárásrendek	EIR	X	X	-	Biztosító	X
114.	6.2. Alapkonfiguráció	EIR	X	X	X	Biztosító	X
115.	6.3. Alapkonfiguráció – Automatikus támogatás a pontosság és a naprakészség érdekében	EIR	X	-	-	Támogató	-
116.	6.4. Alapkonfiguráció – Korábbi konfigurációk megőrzése	EIR	X	-	-	Támogató	-
117.	6.6. Alapkonfiguráció – Rendszerek és rendszerelemek konfigurálása magas kockázatú területekre	EIR	X	X	-	Biztosító	-
118.	6.7. A konfigurációváltozások felügyelete (változáskezelés)	EIR	X	-	X	Támogató	-
119.	6.8. A konfigurációváltozások felügyelete – Automatizált dokumentáció, értesítés és változtatási tilalom	EIR	X	-	-	Támogató	-
120.	6.9. A konfigurációváltozások felügyelete – Változások tesztelése, jóváhagyása és dokumentálása	EIR	X	-	X	Támogató	-
121.	6.12. A konfigurációváltozások felügyelete – Kriptográfia kezelése	EIR	X	X	-	Támogató	-
122.	6.15. Biztonsági hatásvizsgálatok	EIR	X	-	-	Támogató	-
123.	6.16. Biztonsági hatásvizsgálatok – Különálló tesztkörnyezetek	EIR	X	-	-	Támogató	-

124.	6.17. Biztonsági hatásvizsgálatok – Követelmények ellenőrzése	EIR	X	-	-	Támogató	-
125.	6.18. A változtatásokra vonatkozó hozzáférés korlátozások	EIR	X	-	-	Támogató	-
126.	6.19. A változtatásokra vonatkozó hozzáférés korlátozások – Automatizált hozzáférés-érvényesítés és naplóbejegyzések	EIR	X	-	-	Támogató	-
127.	6.23. Konfigurációs beállítások	EIR	X	-	X	Biztosító	X
128.	6.24. Konfigurációs beállítások – Automatizált kezelés, alkalmazás és ellenőrzés	EIR	X	-	-	Támogató	-
129.	6.25. Konfigurációs beállítások – Reagálás a jogosulatlan változtatásokra	EIR	X	X	-	Támogató	-
130.	6.26. Legszűkebb funkcionalitás	EIR	X	-	X	Biztosító	X
131.	6.27. Legszűkebb funkcionalitás – Rendszeres felülvizsgálat	EIR	X	-	-	Biztosító	-
132.	6.28. Legszűkebb funkcionalitás – Program futtatásának megakadályozása	EIR	X	-	X	Támogató	-
133.	6.31. Legszűkebb funkcionalitás – Engedélyezett Szoftverek – Kivételes Engedélyezés	EIR	X	X	-	Biztosító	-
134.	6.36. Rendszerelem leltár	EIR	X	X	-	Biztosító	X
135.	6.37. Rendszerelem leltár – Frissítések a telepítés és eltávolítás során	EIR	X	-	-	Biztosító	-
136.	6.38. Rendszerelem leltár – Automatizált karbantartás	EIR	X	-	-	Támogató	-
137.	6.39. Rendszerelem leltár – Jogosulatlan elemek automatikus észlelése	EIR	X	X	-	Támogató	-
138.	6.40. Rendszerelem leltár – Elszámoltathatósággal kapcsolatos információk	EIR	X	-	-	Támogató	-
139.	6.45. Konfigurációkezelési terv	EIR	X	-	-	Támogató	-
140.	6.47. A szoftverhasználat korlátozásai	EIR	X	-	-	Támogató	-
141.	6.49. Felhasználó által telepített szoftver	EIR	X	-	X	Támogató	-
142.	6.52. Információ helyének azonosítása és dokumentálása	EIR	X	X	-	Biztosító	-
143.	7.1. Szabályzat és eljárásrendek	EIR	X	X	-	Támogató	-
144.	7.2. Üzletmenet-folytonossági terv	EIR	X	X	-	Biztosító	X

145.	7.3. Üzletmenet-folytonossági terv – Összehangolás a kapcsolódó tervekkel	EIR	X	-	-	Támogató	-
146.	7.4. Üzletmenet-folytonossági terv – Kapacitás tervezése	EIR	X	-	-	Támogató	-
147.	7.5. Üzletmenet-folytonossági terv – Üzleti (ügymeneti) funkciók visszaállítása	EIR	X	-	-	Biztosító	-
148.	7.6. Üzletmenet-folytonossági terv – Alapfeladatok és alapfunkciók folyamatossága	EIR	X	-	-	Támogató	-
149.	7.9. Üzletmenet-folytonossági terv – Kritikus erőforrások meghatározása	EIR	X	-	-	Biztosító	-
150.	7.10. A folyamatos működésre felkészítő képzés	EIR	X	-	-	Támogató	-
151.	7.11. A folyamatos működésre felkészítő képzés – Szimulált események	EIR	X	-	-	Támogató	-
152.	7.13. Üzletmenet-folytonossági terv tesztelése	EIR	X	-	X	Biztosító	X
153.	7.14. Üzletmenet-folytonossági terv tesztelése – Összehangolás a kapcsolódó tervekkel	EIR	X	-	-	Támogató	-
154.	7.15. Üzletmenet-folytonossági terv tesztelése – Alternatív feldolgozási helyszín	EIR	X	-	-	Támogató	-
155.	7.19. Biztonsági tárolási helyszín	EIR	X	X	-	Biztosító	-
156.	7.20. Biztonsági tárolási helyszín – Elkülönítés az elsődleges tárolási helyszíntől	EIR	X	-	-	Biztosító	-
157.	7.21. Biztonsági tárolási helyszín – Helyreállítási idő és helyreállítási pont céljai	EIR	X	-	-	Biztosító	-
158.	7.22. Biztonsági tárolási helyszín – Hozzáférhetőség	EIR	X	-	-	Támogató	-
159.	7.23. Alternatív feldolgozási helyszín	EIR	X	X	-	Támogató	-
160.	7.24. Alternatív feldolgozási helyszín – Elkülönítés az elsődleges helyszíntől	EIR	X	-	-	Támogató	-
161.	7.25. Alternatív feldolgozási helyszín – Hozzáférhetőség	EIR	X	-	-	Támogató	-
162.	7.26. Alternatív feldolgozási helyszín – Szolgáltatás prioritása	EIR	X	-	-	Támogató	-
163.	7.27. Alternatív feldolgozási helyszín – Használatra való felkészítés	EIR	X	-	-	Támogató	-
164.	7.29. Telekommunikációs szolgáltatások	EIR	X	-	-	Támogató	-

165.	7.30. Telekommunikációs szolgáltatások – Szolgáltatásprioritási rendelkezések	EIR	X	-	-	Támogató	-
166.	7.31. Telekommunikációs szolgáltatások – Kritikus meghibásodási pont	EIR	X	-	-	Támogató	-
167.	7.32. Telekommunikációs szolgáltatások – Elsődleges és másodlagos szolgáltatók különválasztása	EIR	X	-	-	Támogató	-
168.	7.33. Telekommunikációs szolgáltatások – Szolgáltatói üzletmenet-folytonossági terv	EIR	X	-	-	Támogató	-
169.	7.35. Az elektronikus információs rendszer mentései	EIR	X	-	X	Biztosító	X
170.	7.36. Az elektronikus információs rendszer mentései – Megbízhatóság és sértetlenség tesztelése	EIR	X	-	X	Biztosító	-
171.	7.37. Az elektronikus információs rendszer mentései – Visszaállítás tesztelése mintavétellel	EIR	X	-	X	Biztosító	-
172.	7.38. Az elektronikus információs rendszer mentései – Kritikus információk elkülönített tárhelye	EIR	X	-	X	Támogató	-
173.	7.39. Az elektronikus információs rendszer mentései – Átvitel másodlagos tárolási helyszínre	EIR	X	-	-	Támogató	-
174.	7.42. Az elektronikus információs rendszer mentései – Kriptográfiai védelem	EIR	X	-	X	Biztosító	-
175.	7.43. Az elektronikus információs rendszer helyreállítása és újraindítása	EIR	X	-	X	Biztosító	X
176.	7.44. Az elektronikus információs rendszer helyreállítása és újraindítása – Tranzakciók helyreállítása	EIR	X	-	-	Támogató	-
177.	7.45. Az elektronikus információs rendszer helyreállítása és újraindítása – Meghatározott időn belüli visszaállítás	EIR	X	-	-	Támogató	-
178.	8.1. Szabályzat és eljárásrendek	EIR	X	X	-	Biztosító	X
179.	8.2. Azonosítás és hitelesítés	EIR	X	X	X	Biztosító	X
180.	8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése	EIR	X	-	X	Támogató	-
181.	8.4. Azonosítás és hitelesítés (felhasználók) – Nem-privilegizált fiókok többtényezős hitelesítése	EIR	X	-	X	Támogató	-

182.	8.5. Azonosítás és hitelesítés (felhasználók) – Egyéni azonosítás csoportos hitelesítéssel	EIR	X	-	-	Támogató	-
183.	8.7. Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem	EIR	X	-	-	Biztosító	-
184.	8.10. Eszközök azonosítása és hitelesítése	EIR	X	-	X	Biztosító	X
185.	8.14. Azonosító kezelés	EIR	X	X	-	Biztosító	X
186.	8.16. Azonosító kezelés – Felhasználói státusz azonosítása	EIR	X	-	-	Támogató	-
187.	8.21. A hitelesítésre szolgáló eszközök kezelése	EIR	X	X	X	Biztosító	X
188.	8.22. A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés	EIR	X	-	X	Támogató	-
189.	8.23. A hitelesítésre szolgáló eszközök kezelése – Nyilvános kulcs alapú hitelesítés	EIR	X	-	X	Támogató	-
190.	8.25. A hitelesítésre szolgáló eszközök kezelése – A hitelesítő eszközök védelme	EIR	X	-	-	Támogató	-
191.	8.36. Hitelesítési információk visszajelzésének elrejtése	EIR	X	-	X	Támogató	-
192.	8.37. Hitelesítés kriptográfiai modul esetén	EIR	X	X	-	Támogató	-
193.	8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	EIR	X	X	-	Biztosító	-
194.	8.39. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata	EIR	X	-	-	Támogató	-
195.	8.43. Újrahitelesítés	EIR	X	-	X	Biztosító	X
196.	8.44. Személyazonosság igazolása	EIR	X	X	-	Biztosító	X
197.	8.46. Személyazonosság igazolása – Személyazonosság bizonyítéka	EIR	X	-	-	Biztosító	-
198.	8.47. Személyazonosság igazolása – Személyazonossági bizonyítékok hitelesítése és ellenőrzése	EIR	X	-	-	Biztosító	-
199.	8.48. Személyazonosság igazolása – Személyes jelenlét melletti hitelesítés és ellenőrzés	EIR	X	-	-	Biztosító	-
200.	8.49. Személyazonosság igazolása – Cím megerősítése	EIR	X	-	-	Támogató	-

201.	9.1. Szabályzat és eljárásrendek	SZ	X	X	-	Támogató	-
202.	9.2. Képzés a biztonsági események kezelésére	SZ	X	-	X	Támogató	X
203.	9.3. Képzés a biztonsági események kezelésére – Szimulált események	SZ	X	X	-	Támogató	-
204.	9.4. Képzés a biztonsági események kezelésére – Automatizált képzési környezet	SZ	X	-	-	Támogató	-
205.	9.5. Biztonsági események kezelésének tesztelése	SZ	X	-	-	Támogató	-
206.	9.7. Biztonsági események kezelésének tesztelése – Összehangolás a kapcsolódó tervekkel	SZ	X	-	-	Támogató	-
207.	9.9. Biztonsági események kezelése	SZ	X	X	X	Biztosító	X
208.	9.10. Biztonsági események kezelése – Automatizált eseménykezelő folyamatok	SZ	X	-	-	Támogató	-
209.	9.13. Biztonsági események kezelése – Információk korrelációja	SZ	X	-	-	Támogató	-
210.	9.20. Biztonsági események kezelése – Integrált eseménykezelő csoport	SZ	X	-	-	Támogató	-
211.	9.25. A biztonsági események nyomonkövetése	SZ	X	-	X	Biztosító	-
212.	9.26. A biztonsági események nyomonkövetése – Automatizált nyomon követés, adatgyűjtés és elemzés	SZ	X	-	-	Támogató	-
213.	9.27. A biztonsági események jelentése	SZ	X	-	X	Biztosító	-
214.	9.28. A biztonsági események jelentése – Automatizált jelentés	SZ	X	-	-	Támogató	-
215.	9.30. A biztonsági események jelentése – Ellátási lánc koordinációja	SZ	X	-	-	Támogató	-
216.	9.31. Segítségnyújtás a biztonsági események kezeléséhez	SZ	X	-	-	Támogató	-
217.	9.32. Segítségnyújtás biztonsági események kezeléséhez – Automatizált támogatás az információk és a támogatás elérhetőségéhez	SZ	X	-	-	Támogató	-
218.	9.34. Biztonsági eseménykezelési terv	SZ	X	-	-	Biztosító	-
219.	10.1. Szabályzat és eljárásrendek	SZ	X	X	-	Támogató	-
220.	10.2. Szabályozott karbantartás	SZ	X	-	X	Biztosító	X
221.	10.3. Rendszeres karbantartás – Automatizált karbantartási tevékenységek	SZ	X	-	-	Támogató	-

222.	10.4. Karbantartási eszközök	SZ	X	-	-	Támogató	-
223.	10.5. Karbantartási eszközök – Eszközök vizsgálata	SZ	X	-	-	Támogató	-
224.	10.6. Karbantartási eszközök – Adathordozók vizsgálata	SZ	X	-	-	Támogató	-
225.	10.7. Karbantartási eszközök – Jogosulatlan elszállítás megakadályozása	SZ	X	-	-	Támogató	-
226.	10.11. Távoli karbantartás	SZ	X	-	X	Támogató	-
227.	10.13. Távoli karbantartás – Azonos szintű biztonság és adattörlés	SZ	X	-	-	Támogató	-
228.	10.18. Karbantartó személyek	SZ	X	-	-	Támogató	-
229.	10.19. Karbantartó személyek – Nem megfelelő ellenőrzöttségű személyek	SZ	X	-	-	Támogató	-
230.	10.21. Kellő időben történő karbantartás	SZ	X	-	-	Támogató	-
231.	11.1. Szabályzat és eljárásrendek	SZ	X	X	-	Támogató	-
232.	11.2. Hozzáférés az adathordozókhoz	SZ	X	-	X	Biztosító	X
233.	11.3. Adathordozók címkézése	SZ	X	-	-	Támogató	-
234.	11.4. Adathordozók tárolása	SZ	X	-	-	Biztosító	-
235.	11.6. Adathordozók szállítása	SZ	X	-	-	Biztosító	-
236.	11.8. Adathordozók törlése	SZ	X	-	X	Biztosító	-
237.	11.9. Adathordozók törlése – Felülvizsgálat, jóváhagyás, nyomon követés, dokumentálás és ellenőrzés	SZ	X	-	X	Biztosító	-
238.	11.10. Adathordozók törlése – Berendezés tesztelése	SZ	X	-	-	Támogató	-
239.	11.11. Adathordozók törlése – Roncsolásmentes technikák	SZ	X	-	-	Támogató	-
240.	11.14. Adathordozók használata	SZ	X	X	X	Támogató	-
241.	12.1. Szabályzat és eljárásrendek	SZ	X	X	-	Biztosító	X
242.	12.2. A fizikai belépési engedélyek	SZ	X	X	-	Biztosító	-
243.	12.6. A fizikai belépés ellenőrzése	SZ	X	-	X	Biztosító	X
244.	12.7. A fizikai belépés ellenőrzése – Rendszer hozzáférés	SZ	X	-	X	Támogató	-
245.	12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz	SZ	X	-	X	Támogató	-

246.	12.15. A kimeneti eszközök hozzáférés-ellenőrzése	SZ	X	-	X	Támogató	-
247.	12.17. A fizikai hozzáférések felügyelete	SZ	X	-	X	Biztosító	X
248.	12.18. A fizikai hozzáférések felügyelete – Behatolásjelző és megfigyelő berendezések	SZ	X	-	X	Támogató	-
249.	12.21. A fizikai hozzáférések felügyelete – Rendszerekhez való fizikai hozzáférés-ellenőrzése	SZ	X	-	-	Támogató	-
250.	12.22. Látogatói hozzáférési naplók	SZ	X	-	-	Támogató	-
251.	12.23. Látogatói hozzáférési naplók – Nyilvántartások automatizált karbantartása és felülvizsgálata	SZ	X	-	-	Támogató	-
252.	12.24. Áramellátó berendezések és kábelezés	SZ	X	-	-	Támogató	-
253.	12.27. Vészkikapcsolás	SZ	X	-	X	Támogató	-
254.	12.28. Vészhelyzeti tápellátás	SZ	X	-	X	Támogató	-
255.	12.29. Vészhelyzeti tápellátás – Tartalék áramellátás – Minimális működési képesség	SZ	X	-	-	Támogató	-
256.	12.31. Vészvilágítás	SZ	X	-	X	Támogató	-
257.	12.33. Tűzvédelem	SZ	X	-	X	Biztosító	-
258.	12.34. Tűzvédelem – Érzékelőrendszerek – Automatikus élesítés és értesítés	SZ	X	-	X	Támogató	-
259.	12.35. Tűzvédelem – Tűzoltó berendezések – Automatikus élesítés és értesítés	SZ	X	-	X	Támogató	-
260.	12.37. Környezeti védelmi intézkedések	SZ	X	X	X	Biztosító	-
261.	12.40. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	SZ	X	-	X	Biztosító	-
262.	12.41. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem – Automatizálás támogatása	SZ	X	-	-	Támogató	-
263.	12.42. Be- és kiszállítás	SZ	X	-	-	Támogató	-
264.	12.43. Munkavégzésre kijelölt alternatív helyszín	SZ	X	-	-	Biztosító	-
265.	12.44. Az információs rendszer elemeinek elhelyezése	SZ	X	-	-	Támogató	-
266.	13.1. Szabályzat és eljárásrendek	SZ	X	X	-	Támogató	-
267.	13.2. Rendszerbiztonsági terv	EIR	X	-	X	Biztosító	X

268.	13.3. Viselkedési szabályok	SZ	X	-	-	Támogató	-
269.	13.4. Viselkedési szabályok – Közösségi média és külső webhelyek, alkalmazások használatára vonatkozó korlátozások	SZ	X	-	-	Támogató	-
270.	13.6. Információbiztonsági architektúra leírás	EIR	X	-	-	Támogató	-
271.	13.10. Biztonsági követelmények kiválasztása	EIR	X	-	-	Támogató	-
272.	13.11. Biztonsági követelmények testre szabása	EIR	X	-	-	Támogató	-
273.	14.1. Szabályzat és eljárásrendek	SZ	X	X	-	Biztosító	X
274.	14.2. Munkakörök biztonsági szempontú besorolása	SZ	X	-	X	Támogató	-
275.	14.3. Személyek háttérellenőrzése	SZ	X	-	-	Támogató	-
276.	14.5. Személyek munkaviszonyának megszűnése	SZ	X	-	X	Biztosító	X
277.	14.7. Személyek munkaviszonyának megszűnése – Automatizált intézkedések	SZ	X	-	-	Biztosító	-
278.	14.8. Az áthelyezések, átirányítások és kirendelések kezelése	SZ	X	-	-	Támogató	-
279.	14.9. Hozzáférési megállapodások	SZ	X	-	-	Támogató	-
280.	14.11. Külső személyekhez kapcsolódó biztonsági követelmények	SZ	X	-	-	Támogató	-
281.	14.12. Fegyelmi intézkedések	SZ	X	-	-	Támogató	-
282.	14.13. Munkaköri leírások	SZ	X	X	-	Támogató	-
283.	15.1. Szabályzat és eljárásrendek	SZ	X	X	-	Támogató	-
284.	15.2. Biztonsági osztályba sorolás	SZ	X	-	X	Támogató	-
285.	15.4. Kockázatelemzés	SZ	X	-	X	Biztosító	X
286.	15.5. Kockázatelemzés – Ellátási lánc	SZ	X	-	-	Támogató	-
287.	15.9. Sérülékenységek ellenőrzése	EIR	X	-	X	Támogató	-
288.	15.10. Sérülékenységmenedzsment	EIR	X	-	X	Biztosító	-
289.	15.11. Sérülékenységmenedzsment – Sérülékenységi adatbázis frissítése	EIR	X	-	-	Támogató	-
290.	15.13. Sérülékenységmenedzsment – Felfedezhető információk	EIR	X	-	-	Támogató	-

291.	15.14. Sérülékenységmenedzsment – Privilegizált hozzáférés	EIR	X	-	-	Támogató	-
292.	15.18. Sérülékenységmenedzsment – Sérülékenységi információk fogadása	EIR	X	-	-	Támogató	-
293.	15.20. Kockázatokra adott válasz	EIR	X	-	-	Biztosító	-
294.	15.21. Rendszerelemek kritikusságának elemzése	EIR	X	-	-	Biztosító	-
295.	16.1. Szabályzat és eljárásrendek	SZ	X	X	-	Támogató	-
296.	16.2. Erőforrások rendelkezésre állása	SZ	X	X	-	Támogató	-
297.	16.3. A rendszer fejlesztési életciklusa	SZ	X	-	-	Támogató	-
298.	16.7. Beszerzések	EIR	X	X	-	Támogató	-
299.	16.8. Beszerzések – Alkalmazandó védelmi intézkedések funkcionális tulajdonságai	EIR	X	-	-	Támogató	-
300.	16.9. Beszerzések – Tervezési és megvalósítási információk a védelmi intézkedések teljesüléséhez	EIR	X	-	-	Támogató	-
301.	16.11. Beszerzések - Rendszer, rendszerelem és szolgáltatás konfigurációk – Rendszer, rendszerelem és szolgáltatás konfigurációk	EIR	X	-	-	Támogató	-
302.	16.13. Beszerzések – Használatban lévő funkciók, portok, protokollok és szolgáltatások	EIR	X	-	-	Támogató	-
303.	16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció	EIR	X	-	X	Támogató	-
304.	16.16. Biztonságtervezési elvek	SZ	X	-	-	Támogató	-
305.	16.49. Külső elektronikus információs rendszerek szolgáltatásai	SZ	X	-	-	Támogató	-
306.	16.51. Külső információs rendszerek szolgáltatásai – Funkciók, portok, protokollok és szolgáltatások azonosítása	EIR	X	-	-	Támogató	-
307.	16.58. Fejlesztői változáskövetés	EIR	X	-	-	Biztosító	-
308.	16.66. Fejlesztői biztonsági tesztelés	EIR	X	-	X	Biztosító	-
309.	16.76. Fejlesztési folyamat, szabványok és eszközök	SZ	X	-	-	Támogató	-
310.	16.79. Fejlesztési folyamat, szabványok és eszközök – Kritikussági elemzés	SZ	X	-	-	Támogató	-

311.	16.86. Szoftverfejlesztők oktatása	SZ	X	-	-	Támogató	-
312.	16.87. Fejlesztői biztonsági architektúra és tervezés	SZ	X	-	-	Biztosító	X
313.	16.98. Külső fejlesztők háttérellenőrzése	SZ	X	-	-	Támogató	-
314.	16.99. Támogatással nem rendelkező rendszerelemek	EIR	X	-	X	Biztosító	X
315.	17.1. Szabályzat és eljárásrendek	EIR	X	X	-	Biztosító	X
316.	17.2. Rendszer és felhasználói funkciók szétválasztása	EIR	X	-	-	Támogató	-
317.	17.4. Biztonsági funkciók elkülönítése	EIR	X	-	-	Támogató	-
318.	17.10. Információk az osztott használatú rendszererőforrásokban	EIR	X	-	X	Támogató	-
319.	17.12. Szolgáltatásmegtagadással járó támadások elleni védelem	EIR	X	-	X	Biztosító	X
320.	17.17. A határok védelme	EIR	X	-	X	Biztosító	X
321.	17.18. A határok védelme – Hozzáférési pontok	EIR	X	-	X	Támogató	-
322.	17.19. A határok védelme – Külső infokommunikációs szolgáltatások	EIR	X	-	X	Biztosító	-
323.	17.20. A határok védelme – Alapértelmezés szerinti elutasítás és kivétel alapú engedélyezés	EIR	X	-	X	Biztosító	-
324.	17.21. A határok védelme – Megosztott csatornahasználat távoli eszközök esetén	EIR	X	-	X	Támogató	-
325.	17.22. A határok védelme – A forgalom átirányítása hitelesített proxykiszolgálókra	EIR	X	-	-	Támogató	-
326.	17.32. A határok védelme – Biztonságos állapot fenntartása	EIR	X	-	-	Támogató	-
327.	17.35. A határok védelme – Rendszerelemek elkülönítése	EIR	X	-	X	Támogató	-
328.	17.40. Az adatátvitel bizalmassága és sértetlensége	EIR	X	-	X	Biztosító	-
329.	17.41. Az adatátvitel bizalmassága és sértetlensége – Kriptográfiai védelem	EIR	X	-	-	Támogató	-
330.	17.46. A hálózati kapcsolat megszakítása	EIR	X	-	-	Támogató	-
331.	17.49. Kriptográfiai kulcs előállítása és kezelése	EIR	X	-	X	Biztosító	X
332.	17.50. Kriptográfiai kulcs előállítása és kezelése – Rendelkezésre állás	EIR	X	-	-	Támogató	-

333.	17.53. Kriptográfiai védelem	EIR	X	-	X	Biztosító	X
334.	17.54. Együttműködésen alapuló informatikai eszközök	EIR	X	-	-	Támogató	-
335.	17.62. Nyilvános kulcsú infrastruktúra tanúsítványok	EIR	X	-	X	Támogató	-
336.	17.63. Mobilkód korlátozása	EIR	X	-	-	Támogató	-
337.	17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)	EIR	X	-	X	Támogató	-
338.	17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)	EIR	X	-	-	Támogató	-
339.	17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	EIR	X	-	-	Támogató	-
340.	17.73. Munkaszakasz hitelessége	EIR	X	-	X	Biztosító	-
341.	17.77. Ismert állapotba való visszatérés	EIR	X	-	-	Biztosító	-
342.	17.81. Tárolt (at rest) adatok védelme	EIR	X	X	-	Biztosító	X
343.	17.82. Tárolt (at rest) adatok védelme – Kriptográfiai védelem	EIR	X	-	-	Támogató	-
344.	17.108. A folyamatok elkülönítése	EIR	X	-	-	Támogató	-
345.	18.1. Szabályzat és eljárásrendek	EIR	X	X	-	Biztosító	X
346.	18.2. Hibajavítás	EIR	X	-	X	Biztosító	X
347.	18.3. Hibajavítás – Automatizált hibaelhárítás állapota	EIR	X	-	-	Támogató	-
348.	18.8. Kártékony kódok elleni védelem	EIR	X	-	X	Biztosító	X
349.	18.13. Az EIR monitorozása	EIR	X	-	X	Biztosító	X
350.	18.15. Az EIR monitorozása – Automatizált eszközök és mechanizmusok valós idejű elemzéshez	EIR	X	-	-	Biztosító	-
351.	18.17. Az EIR monitorozása – Bejövő és kimenő kommunikációs forgalom	EIR	X	-	-	Biztosító	-
352.	18.18. Az EIR monitorozása – Rendszer által generált riasztások	EIR	X	-	X	Támogató	-
353.	18.21. Az EIR monitorozása – A titkosított kommunikáció láthatósága	EIR	X	-	-	Támogató	-

354.	18.23. Az EIR monitorozása – Automatikusan generált szervezeti riasztások	EIR	X	-	-	Támogató	-
355.	18.25. Az EIR monitorozása – Vezeték nélküli behatolást érzékelő rendszer	EIR	X	-	-	Támogató	-
356.	18.31. Az EIR monitorozása – Privilegizált felhasználók	EIR	X	-	-	Támogató	-
357.	18.33. Az EIR monitorozása – Engedély nélküli hálózati szolgáltatások	EIR	X	-	-	Támogató	-
358.	18.37. Biztonsági riasztások és tájékoztatások	EIR	X	X	-	Támogató	-
359.	18.38. Biztonsági riasztások és tájékoztatások – Automatizált figyelmeztetések és tanácsok	EIR	X	-	-	Támogató	-
360.	18.39. Biztonsági funkciók ellenőrzése	EIR	X	X	-	Biztosító	-
361.	18.42. Szoftver- és információsértetlenség	EIR	X	-	-	Támogató	-
362.	18.43. Szoftver-, firmware- és információsértetlenség – Sértetlenség ellenőrzése	EIR	X	-	-	Támogató	-
363.	18.44. Szoftver-, firmware- és információsértetlenség – Automatikus értesítések az sértetlenség megszűnéséről	EIR	X	-	-	Támogató	-
364.	18.46. Szoftver- és információsértetlenség – Automatikus reagálás	EIR	X	-	-	Támogató	-
365.	18.48. Szoftver- és információsértetlenség – Észlelés és a válaszadás integrálása	EIR	X	-	-	Támogató	-
366.	18.53. Szoftver-, firmware- és információsértetlenség – Kódok hitelesítése	EIR	X	-	-	Támogató	-
367.	18.56. Kéretlen üzenetek elleni védelem	EIR	X	-	X	Biztosító	-
368.	18.57. Kéretlen üzenetek elleni védelem – Automatikus frissítések	EIR	X	-	X	Biztosító	-
369.	18.59. Bemeneti információ ellenőrzés	EIR	X	-	X	Biztosító	-
370.	18.66. Hibakezelés	EIR	X	-	-	Támogató	-
371.	18.67. Információ kezelése és megőrzése	EIR	X	-	-	Támogató	-
372.	18.78. Memóriavédelem	EIR	X	-	-	Biztosító	-
373.	19.1. Szabályzat és eljárásrendek	SZ	X	X	-	Biztosító	X
374.	19.2. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat	SZ	X	-	-	Biztosító	X

375.	19.4. Ellátási láncra vonatkozó követelmények és folyamatok	SZ	X	-	-	Támogató	-
376.	19.7. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók	SZ	X	-	-	Támogató	-
377.	19.13. Beszerzési stratégiák, eszközök és módszerek	SZ	X	-	-	Támogató	-
378.	19.16. Beszállítók értékelése és felülvizsgálata	SZ	X	-	-	Biztosító	-
379.	19.19. Értesítési megállapodások	SZ	X	-	-	Támogató	-
380.	19.20. Hamisítás elleni védelem	SZ	X	-	-	Biztosító	X
381.	19.21. Hamisítás elleni védelem - Rendszerfejlesztési életciklus	SZ	X	-	-	Támogató	-
382.	19.22. Rendszerek vagy rendszerelemek vizsgálata	SZ	X	-	-	Biztosító	-
383.	19.23. Rendszerelem hitelessége	SZ	X	-	-	Biztosító	-
384.	19.24. Rendszerelem hitelessége – Hamisítás elleni képzés	SZ	X	-	-	Támogató	-
385.	19.25. Rendszerelem hitelessége – Konfigurációfelügyelet	SZ	X	-	-	Támogató	-
386.	19.27. Rendszerelem selejtezése, megsemmisítése	SZ	X	-	-	Támogató	-

Az MKr. szerinti követelménycsoportok értékelése

1. Programmenedzsment

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	1.1. Információbiztonsági szabályzat	K01.001_P[1]	meghatározott a szervezet egészére kiterjedő információbiztonsági szabályzat felülvizsgálatának és frissítésének gyakorisága
3.		K01.001_P[2]	meghatározásra kerültek azok az események, amelyek kiváltják az egész szervezetre kiterjedő információbiztonsági szabályzat felülvizsgálatát és frissítését
4.		K01.001_O.1.1.1.1.(a)	az információbiztonsági szabályzat áttekintést nyújt a biztonsággal kapcsolatos követelményekről
5.		K01.001_O.1.1.1.1.(b)	az információbiztonsági szabályzat áttekintést nyújt a védelmi intézkedésekről, amelyeket az MKr. szerinti követelmények teljesítése érdekében alkalmaznak vagy terveznek bevezetni
6.		K01.001_O.1.1.1.2.(a)	az információbiztonsági szabályzat meghatározza a célkitűzéseket
7.		K01.001_O.1.1.1.2.(b)	az információbiztonsági szabályzat meghatározza a szerepkörök azonosítását és kijelölését
8.		K01.001_O.1.1.1.2.(c)	az információbiztonsági szabályzat meghatározza a felelősségek azonosítását és kijelölését
9.		K01.001_O.1.1.1.2.(d)	az információbiztonsági szabályzat rögzíti a vezetői elkötelezettséget a biztonsággal kapcsolatos követelményeknek való megfelelés iránt
10.		K01.001_O.1.1.1.2.(e)	az információbiztonsági szabályzat szabályozza a szervezeti egységek közötti együttműködést
11.		K01.001_O.1.1.1.2.(f)	az információbiztonsági szabályzat rendelkezik a megfelelőségről
12.		K01.001_O.1.1.1.3	az információbiztonsági szabályzat leírja az információbiztonságért felelős szervezeti egységek közötti együttműködést
13.		K01.001_O.1.1.1.4	az információbiztonsági szabályzatot olyan vezető tisztviselő hagyta jóvá, aki felelős és elszámoltatható a szervezeti működésre (beleértve a célkitűzéseket, a funkciókat, az arculatot és a hírnevet), a szervezeti eszközökre, a személyekre és más szervezetekre jelentett kockázatokért
14.		K01.001_O.1.1.1.(a)	az egész szervezetre kiterjedő információbiztonsági szabályzat kidolgozásra került
15.		K01.001_O.1.1.1.(b)	az információbiztonsági szabályzat kihirdetése dokumentált módon megtörtént

16.		K01.001_O.1.1.2.(a)	az információbiztonsági szabályzatot felülvizsgálják és frissítik a K01.001_P[1] szerint meghatározott gyakorisággal
17.		K01.001_O.1.1.2.(b)	az információbiztonsági szabályzatot a K01.001_P[2] által meghatározott eseményeket követően felülvizsgálják és frissítik
18.		K01.001_O.1.1.3.(a)	az információbiztonsági szabályzat védett a jogosulatlan megismeréssel szemben
19.		K01.001_O.1.1.3.(b)	az információbiztonsági szabályzat védett a jogosulatlan módosítással szemben
20.	1.2. Elektronikus információs rendszerek biztonságáért felelős személy	K01.002_O.1.2.(a)	a biztonságért felelős személy kinevezése megtörtént
21.		K01.002_O.1.2.(b)	a biztonságért felelős személy rendelkezik a szervezet egészére kiterjedő információbiztonsági szabályzat koordinálásához szükséges feladatkörrel és erőforrásokkal
22.		K01.002_O.1.2.(c)	a biztonságért felelős személy rendelkezik a szervezet egészére kiterjedő információbiztonsági szabályzat fejlesztéséhez szükséges hatáskörrel és erőforrásokkal
23.		K01.002_O.1.2.(d)	a biztonságért felelős személy rendelkezik a szervezet egészére kiterjedő információbiztonsági szabályzat bevezetéséhez szükséges hatáskörrel és erőforrásokkal
24.		K01.002_O.1.2.(e)	a biztonságért felelős személy rendelkezik a szervezet egészére kiterjedő információbiztonsági szabályzat fenntartásához szükséges hatáskörrel és a célok eléréséhez szükséges erőforrásokkal
25.	1.3. Információbiztonságot érintő erőforrások	K01.003_O.1.3.1	az információbiztonsági szabályzat végrehajtásához szükséges erőforrások szerepelnek az éves költségvetés tervezésében és a szervezet beruházási terveiben, valamint minden, a követelmény alóli kivétel dokumentálásra került
26.		K01.003_O.1.3.2	az információbiztonsági szabályzat végrehajtásához szükséges erőforrások szerepelnek az éves költségvetés tervezésében és a szervezet beruházási terveiben, és az ahhoz szükséges dokumentáció összhangban van a hatályos jogszabályi rendelkezésekkel, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal
27.		K01.003_O.1.3.3	az információbiztonsági forrásokat a tervezett kiadásokra rendelkezésre bocsátották és bocsátják
28.	1.4. Intézkedési terv és mérföldkövei	K01.004_P[1]	a szervezet a cselekvési tervek és mérföldköveik jelentési követelményeit meghatározta
29.		K01.004_O.1.4.1.1.(a)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az információbiztonsági szabályzatra és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési terveket és mérföldköveket dolgozzanak ki
30.		K01.004_O.1.4.1.1.(b)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az információbiztonsági szabályzatra és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési terveket és mérföldköveket karban tartják
31.		K01.004_O.1.4.1.1.(c)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az ellátási lánc kockázatkezelésére és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési terveket és mérföldköveket dolgozzanak ki
32.		K01.004_O.1.4.1.1.(d)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az ellátási lánc kockázatkezelésére és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési terveket és mérföldköveket karban tartják

33.		K01.004_O.1.4.1.2.(a)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az információbiztonsági szabályzatra és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési tervek és mérföldkövek dokumentálják az információbiztonsági kockázatkezeléssel kapcsolatos helyreállító intézkedéseket
34.		K01.004_O.1.4.1.2.(b)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az ellátási lánc kockázatkezelésére és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési tervek és mérföldkövek dokumentálják az ellátási lánc kockázatkezelésével kapcsolatos helyreállító intézkedéseket
35.		K01.004_O.1.4.1.3.(a)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az információbiztonsági kockázatkezelési szabályzatra és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési tervek és mérföldkövek a K01.004_P[1]-nek megfelelően bemutatásra kerüljenek
36.		K01.004_O.1.4.1.3.(b)	a szervezet fenntart olyan folyamatot, amely biztosítja, hogy az ellátási lánc kockázatkezelési szabályzatra és a kapcsolódó szervezeti rendszerekre vonatkozó cselekvési tervek és mérföldkövek a K01.004_P[1]-nek megfelelően bemutatásra kerüljenek
37.		K01.004_O.1.4.2.(a)	az intézkedési terveket és a mérföldköveket a szervezeti kockázatkezelési stratégiával való összhang szempontjából felülvizsgálják
38.		K01.004_O.1.4.2.(b)	a cselekvési terveket és a mérföldköveket felülvizsgálják a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal való összhang szempontjából
39.	1.5. Elektronikus információs rendszerek nyilvántartása	K01.005_P[1]	meghatározott, hogy milyen gyakorisággal kell felülvizsgálni az EIR-ek nyilvántartását
40.		K01.005_O.1.5.(a)	az elektronikus információs rendszerek nyilvántartását létrehozták
41.		K01.005_O.1.5.(b)	az elektronikus információs rendszerek nyilvántartását frissítik a szervezet EIR-jeiben bekövetkezett változások esetén
42.		K01.005_O.1.5.(c)	a szervezeti rendszerek nyilvántartását felülvizsgálják a K01.005_P[1] által meghatározott gyakorisággal
43.	1.6. Biztonsági teljesítmény mérése	K01.006_O.1.6.(a)	az információbiztonsági teljesítménymutatókat kidolgozták
44.		K01.006_O.1.6.(b)	az információbiztonsági teljesítménymutatók nyomon követése biztosított
45.		K01.006_O.1.6.(c)	az információbiztonsági teljesítménymutatók eredményei jelentésre kerülnek
46.	1.7. Szervezeti architektúra	K01.007_O.1.7.(a)	a szervezetrendszert a szervezeti működésre és eszközökre, az egyénekre és más szervezetekre jelentett kockázatok figyelembevételével alakítják ki
47.		K01.007_O.1.7.(b)	a szervezetrendszert a szervezeti működésre és eszközökre, az egyénekre és más szervezetekre jelentett kockázatok figyelembevételével tartják fenn
48.		K01.009_O.1.9.(a)	az információbiztonsági kérdésekkel a kritikus infrastruktúrák és kulcsfontosságú erőforrások védelmére vonatkozó terv kidolgozása során foglalkoznak

49.	1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve	K01.009_O.1.9.(b)	az információbiztonsági kérdésekkel a kritikus infrastruktúrák és kulcsfontosságú erőforrások védelmére vonatkozó terv dokumentálása során foglalkoznak
50.		K01.009_O.1.9.(c)	az információbiztonsági kérdésekkel a kritikus infrastruktúrák és kulcsfontosságú erőforrások védelmére vonatkozó terv frissítése során foglalkoznak
51.	1.10. Kockázatmenedzsment stratégia	K01.010_P[1]	meghatározott a kockázatmenedzsment stratégia felülvizsgálatának és frissítésének gyakorisága annak érdekében, hogy a szervezeti változásoknak megfeleljen
52.		K01.010_P[2]	meghatározottak azok az esetek, amelyek indokolják a kockázatmenedzsment stratégia felülvizsgálatát és frissítését annak érdekében, hogy az a szervezeti változásoknak megfeleljen
53.		K01.010_O.1.10.1.1	átfogó stratégia került kidolgozásra a szervezeti működés és vagyonelemek, a személyek és más szervezetekhez kapcsolódó, illetve a szervezeti rendszerek működéséhez és használatához kapcsolódó biztonsági kockázatok kezelésére
54.		K01.010_O.1.10.1.2	átfogó stratégia került kidolgozásra a személyazonosításra alkalmas információk engedélyezett feldolgozásából eredő, az egyéneket érintő adatvédelmi kockázatok kezelésére
55.		K01.010_O.1.10.2	a kockázatmenedzsment stratégiát egységesen hajtják végre a szervezeten belül
56.		K01.010_O.1.10.3.(a)	a kockázatmenedzsment stratégiát felülvizsgálják és frissítik a K01.010_P[1] által meghatározott gyakorisággal
57.		K01.010_O.1.10.3.(b)	a kockázatmenedzsment stratégiát felülvizsgálják és frissítik a K01.010_P[2] szerinti esetekben
58.	1.11. Engedélyezési folyamatok meghatározása	K01.011_O.1.11.1	az EIR-ek biztonsági állapotát és a környezetet, amelyben ezek a rendszerek működnek, engedélyezési folyamatok segítségével kezelik
59.		K01.011_O.1.11.2	a szervezeti kockázatmenedzsment folyamaton belül meghatározottak szerepek és felelősségi körök betöltésére kijelölt személyek
60.		K01.011_O.1.11.3	az engedélyezési folyamatokat a szervezet egészére kiterjedő kockázatmenedzsment programba illesztették és működtetik
61.	1.12. Szervezeti működés és üzleti folyamatok meghatározása	K01.012_P[1]	meghatározott a szervezeti célok és az üzleti folyamatok felülvizsgálatának és frissítésének gyakorisága
62.		K01.012_O.1.12.1.(a)	a szervezeti célok és az üzleti folyamatok meghatározása az információbiztonság figyelembevételével történt
63.		K01.012_O.1.12.1.(b)	a szervezeti célokat és az üzleti folyamatokat a szervezeti működésre, a szervezeti eszközökre, a személyekre és más szervezetekre vonatkozó kockázatok figyelembevételével határozták meg
64.		K01.012_O.1.12.2	a meghatározott célokból és üzleti folyamatokból eredő információvédelmi igények meghatározásra kerültek
65.		K01.012_O.1.12.3	a szervezeti célok és az üzleti folyamatok felülvizsgálata és módosítása a K01.012_P[1] által meghatározott gyakorisággal történik

66.	1.14. Biztonsági személyzet képzése	K01.014_O.1.14 (a)	létrehozásra került egy, a biztonsági személyzet képzését elősegítő program
67.		K01.014_O.1.14 (b)	létrehozásra került egy, a biztonsági személyzet fejlesztését elősegítő program
68.	1.15. Tesztelés, képzés és felügyelet	K01.015_O.1.15.1.(a)	a szervezet folyamatot tart fenn annak biztosítására, hogy az EIR-ekhez kapcsolódó biztonsági tesztelésre, képzésre és felügyeleti tevékenységekre vonatkozó szervezeti terveket dolgozzanak ki
69.		K01.015_O.1.15.1.(b)	a szervezet folyamatot tart fenn annak biztosítására, hogy az EIR-ekhez kapcsolódó biztonsági tesztelésre, képzésre és felügyeleti tevékenységekre vonatkozó szervezeti terveket karbantartsák
70.		K01.015_O.1.15.1.(c)	a szervezet folyamatot tart fenn annak biztosítására, hogy az EIR-ekhez kapcsolódó biztonsági tesztelésre, képzésre és felügyeleti tevékenységekre vonatkozó szervezeti terveket folyamatosan végrehajtsák
71.		K01.015_O.1.15.2.(a)	a tesztelési terveket felülvizsgálják a szervezeti kockázatmenedzsment stratégiával való összhang szempontjából
72.		K01.015_O.1.15.2.(b)	a képzési terveket felülvizsgálják a szervezeti kockázatmenedzsment stratégiával való összhang szempontjából
73.		K01.015_O.1.15.2.(c)	a felügyeleti terveket felülvizsgálják a szervezeti kockázatmenedzsment stratégiával való összhang szempontjából
74.		K01.015_O.1.15.2.(d)	a tesztelési terveket felülvizsgálják a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal való összhang szempontjából
75.		K01.015_O.1.15.2.(e)	a képzési terveket felülvizsgálják a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal való összhang szempontjából
76.		K01.015_O.1.15.2.(f)	a felügyeleti terveket felülvizsgálják a kockázatkezelési intézkedésekre vonatkozó, az egész szervezetre kiterjedő prioritásokkal való összhang szempontjából
77.	1.16. Szakmai csoportokkal és közösségekkel való kapcsolattartás	K01.016_ O.1.16	a szervezet kapcsolatot tart szakmai csoportokkal és közösségekkel az MKr. szerinti követelmények teljesítése érdekében
78.	1.17. Fenyegetettség tudatosító program	K01.017_O.1.17	olyan fenyegetettség tudatosító programot hajtanak végre, amely magában foglalja a fenyegetések felismerését szolgáló szervezeten belüli és szervezetek közötti információmegosztási képességet
79.	1.19. Kockázatmenedzsment keretrendszer	K01.019_P[1]	a kockázatmenedzsment tevékenységek eredményeit megismerő személyek meghatározásra kerültek
80.		K01.019_P[2]	meghatározták a kockázatmenedzsment keretrendszer felülvizsgálatának és frissítésének gyakoriságát
81.		K01.019_O.1.19.1.1.(a)	a kockázatelemzést befolyásoló feltételezések azonosítása és dokumentálása megtörtént
82.		K01.019_O.1.19.1.1.(b)	a kockázatkezelést befolyásoló feltételezések azonosítása és dokumentálása megtörtént
83.		K01.019_O.1.19.1.1.(c)	a kockázatok felügyeletét befolyásoló feltételezések azonosítása és dokumentálása megtörtént
84.		K01.019_O.1.19.1.2.(a)	a kockázatelemzést befolyásoló megkötések azonosítása és dokumentálása megtörtént
85.		K01.019_O.1.19.1.2.(b)	a kockázatkezelést befolyásoló megkötések azonosítása és dokumentálása megtörtént

86.		K01.019_O.1.19.1.2.(c)	a kockázatok felügyeletét befolyásoló megkötések azonosítása és dokumentálása megtörtént
87.		K01.019_O.1.19.1.3.(a)	a szervezet által a kockázatmenedzsment során figyelembe vett prioritásokat azonosították és dokumentálták
88.		K01.019_O.1.19.1.3.(b)	a szervezet által a kockázatmenedzsment során figyelembe vett kompromisszumokat azonosították és dokumentálták
89.		K01.019_O.1.19.1.4	a szervezeti kockázattűrő képességet azonosították és dokumentálták
90.		K01.019_O.1.19.2	a kockázatmenedzsment tevékenységek eredményeit a K01.019_P[1] által meghatározott személyek megismerték
91.		K01.019_O.1.19.3	a kockázatmenedzsment szempontjait felülvizsgálják és frissítik a K01.019_P[2] által meghatározott gyakorisággal
92.	1.20. Kockázatkezelésért felelős szerepkörök	K01.020_O.1.20.1.(a)	a kockázatkezelésért felelős személyt kijelölésre került
93.		K01.020_O.1.20.1.(b)	a kockázatkezelésért felelős személy összehangolja az információbiztonság irányítási folyamatait a stratégiai, működési és költségvetési tervezési folyamatokkal
94.		K01.020_O.1.20.2.(a)	a kockázati vezető kijelölésre került
95.		K01.020_O.1.20.2.(b)	a kockázati vezető az egész szervezetre kiterjedő szempontból áttekinti és elemzi a kockázatokat
96.		K01.020_O.1.20.2.(c)	a kockázati vezető biztosítja, hogy a kockázatkezelés egységes legyen a szervezeten belül
97.	1.21. Ellátási lánc kockázatmenedzsment stratégiája	K01.021_P[1]	meghatározott az ellátási lánc kockázatmenedzsment stratégiája felülvizsgálatának és frissítésének gyakorisága
98.		K01.021_O.1.21.1.(a)	az egész szervezetre kiterjedő stratégiát dolgoznak ki az ellátási lánc kockázatainak kezelésére
99.		K01.021_O.1.21.1.(b)	az ellátási lánc kockázatmenedzsment stratégiája az EIR-ek fejlesztésével kapcsolatos kockázatokkal foglalkozik
100.		K01.021_O.1.21.1.(c)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerelemek fejlesztésével kapcsolatos kockázatokkal foglalkozik
101.		K01.021_O.1.21.1.(d)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerszolgáltatások fejlesztésével kapcsolatos kockázatokkal foglalkozik
102.		K01.021_O.1.21.1.(e)	az ellátási lánc kockázatmenedzsment stratégiája az EIR-ek beszerzésével kapcsolatos kockázatokkal foglalkozik
103.		K01.021_O.1.21.1.(f)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerelemek beszerzésével kapcsolatos kockázatokkal foglalkozik
104.		K01.021_O.1.21.1.(g)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerszolgáltatások beszerzésével kapcsolatos kockázatokkal foglalkozik
105.		K01.021_O.1.21.1.(h)	az ellátási lánc kockázatmenedzsment stratégiája az EIR-ek karbantartásával kapcsolatos kockázatokkal foglalkozik
106.		K01.021_O.1.21.1.(i)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerelemek karbantartásával kapcsolatos kockázatokkal foglalkozik

107.		K01.021_O.1.21.1.(j)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerszolgáltatások karbantartásával kapcsolatos kockázatokkal foglalkozik
108.		K01.021_O.1.21.1.(k)	az ellátási lánc kockázatmenedzsment stratégiája az EIR-ek üzemeltetésével kapcsolatos kockázatokkal foglalkozik
109.		K01.021_O.1.21.1.(l)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerelemek üzemeltetésével kapcsolatos kockázatokkal foglalkozik
110.		K01.021_O.1.21.1.(m)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerszolgáltatások üzemeltetésével kapcsolatos kockázatokkal foglalkozik
111.		K01.021_O.1.21.1.(n)	az ellátási lánc kockázatmenedzsment stratégiája az EIR-ek selejtezésével kapcsolatos kockázatokkal foglalkozik
112.		K01.021_O.1.21.1.(o)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerelemek selejtezésével kapcsolatos kockázatokkal foglalkozik
113.		K01.021_O.1.21.1.(p)	az ellátási lánc kockázatmenedzsment stratégiája a rendszerszolgáltatások selejtezésével kapcsolatos kockázatokkal foglalkozik
114.		K01.021_O.1.21.2	az ellátási lánc kockázatmenedzsment stratégiáját következetesen hajtják végre a szervezeten belül
115.		K01.021_O.1.21.3	az ellátási lánc kockázatmenedzsment stratégiáját felülvizsgálják és frissítik a K01.021_P[1] által meghatározott gyakorisággal vagy a szervezeti változásoknak megfelelően
116.	1.22. Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói	K01.022_O.1.22.(a)	a kritikus technológiák, termékek és szolgáltatások beszállítóinak azonosítása megtörténik
117.		K01.022_O.1.22.(b)	a kritikus technológiák, termékek és szolgáltatások beszállítóinak rangsorolása megtörténik
118.		K01.022_O.1.22.(c)	a kritikus technológiák, termékek és szolgáltatások beszállítóinak értékelése megtörténik
119.	1.23. Folyamatos felügyeleti stratégia	K01.023_P[1]	a szervezet egészére kiterjedő folyamatos nyomonkövetés teljesítménymutatóinak meghatározása megtörtént
120.		K01.023_P[2]	a nyomonkövetés gyakoriságának meghatározása megtörtént
121.		K01.023_P[3]	a hatékonyság-értékelés gyakoriságának meghatározása megtörtént
122.		K01.023_P[4]	meghatározásra kerültek az EIR-ek biztonsági állapotáról jelentést tevő személyek vagy szerepkörök
123.		K01.023_P[5]	meghatározták, hogy milyen gyakorisággal kell jelenteni a szervezeti rendszerek biztonsági állapotát
124.		K01.023_O.1.23	az egész szervezetre kiterjedő folyamatos felügyeleti stratégiát dolgoztak ki
125.		K01.023_O.1.23.1	folyamatos felügyeleti programokat hajtanak végre, amelyek tartalmazzák a K01.023_P[1] által meghatározott teljesítménymutatók meghatározását
126.		K01.023_O.1.23.2.(a)	folyamatos felügyeleti programokat hajtanak végre, amelyek meghatározzák a felügyeletet
127.		K01.023_O.1.23.2.(b)	folyamatos felügyeleti programokat hajtanak végre K01.023_P[3] által meghatározott gyakorisággal, amelyek meghatározzák a hatékonyság-értékelést

128.		K01.023_O.1.23.3	folyamatos felügyeleti programot hajtanak végre K01.023_P[2] által meghatározott gyakorisággal, amely a K01.023_P[1] által meghatározott teljesítménymutatók folyamatos figyelemmel követését biztosítja
129.		K01.023_O.1.23.4.(a)	folyamatos felügyeleti programokat hajtanak végre, amelyek magukban foglalják a felügyeleti értékelések és a felügyelet által generált információk összefüggéseit
130.		K01.023_O.1.23.4.(b)	folyamatos felügyeleti programokat hajtanak végre, amelyek magukban foglalják a felügyeleti értékelések és a felügyelet által generált információk elemzését
131.		K01.023_O.1.23.5.(a)	folyamatos felügyeleti programokat hajtanak végre, amelyek a felügyeleti értékelési információk elemzésére irányuló válaszlépéseket tartalmaznak
132.		K01.023_O.1.23.5.(b)	folyamatos felügyeleti programokat hajtanak végre, amelyek a felügyeleti információk elemzésére irányuló válaszlépéseket tartalmaznak
133.		K01.023_O.1.23.6	folyamatos felügyeleti programokat hajtanak végre, amelyek magukban foglalják a szervezeti rendszerek biztonsági állapotának jelentését a K01.023_P[4] által meghatározott személyeknek vagy szerepköröknek a K01.023_P[5] által meghatározott gyakorisággal

2. Hozzáférés-felügyelet

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	2.1. Szabályzat és eljárásrendek	K02.001_P[1]	meghatározott azon személyek vagy szerepkörök listája, akikkel meg kell ismertetni a hozzáférés-felügyeleti szabályzatot
3.		K02.001_P[2]	meghatározott, hogy a hozzáférés-felügyeleti szabályzat szervezeti, folyamat- vagy rendszerszintű
4.		K02.001_P[3]	meghatározott azon személyek vagy szerepkörök listája, akikkel meg kell ismertetni a hozzáférés-felügyeleti eljárásrendet
5.		K02.001_P[4]	meghatározott a hozzáférés-felügyeleti szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személy
6.		K02.001_P[5]	meghatározott a hozzáférés-felügyeleti szabályzat felülvizsgálatának gyakorisága
7.		K02.001_P[6]	meghatározottak a hozzáférés-felügyeleti szabályzat felülvizsgálatát igénylő események
8.		K02.001_P[7]	meghatározott a hozzáférés-felügyeleti eljárásrend felülvizsgálatának gyakorisága
9.		K02.001_P[8]	meghatározottak a hozzáférés-felügyeleti eljárásrend felülvizsgálatát igénylő események

10.		K02.001_O.2.1.1.(a)	a K02.001_P[2] szintű hozzáférés-felügyeleti szabályzatot a szervezet kidolgozta és dokumentálta
11.		K02.001_O.2.1.1.(b)	a hozzáférés-felügyeleti szabályzatot a szervezet kiadta
12.		K02.001_O.2.1.1.(c)	a hozzáférés-felügyeleti szabályzatot a szervezet a K02.001_P[1] szerinti személyekkel vagy szerepkörökkel megismertette
13.		K02.001_O.2.1.1.1.1.(a)	a hozzáférés-felügyeleti szabályzat meghatározza a célkitűzéseket
14.		K02.001_O.2.1.1.1.1.(b)	a hozzáférés-felügyeleti szabályzat hatálya meghatározásra került
15.		K02.001_O.2.1.1.1.1.(c)	a hozzáférés-felügyeleti szabályzat meghatározza a szerepköröket
16.		K02.001_O.2.1.1.1.1.(d)	a hozzáférés-felügyeleti szabályzat meghatározza a felelősségeket
17.		K02.001_O.2.1.1.1.1.(e)	a hozzáférés-felügyeleti szabályzat rögzíti a szabályzat céljával kapcsolatos a vezetői elkötelezettséget
18.		K02.001_O.2.1.1.1.1.(f)	a hozzáférés-felügyeleti szabályzat meghatározza a szervezeten belüli együttműködés kereteit
19.		K02.001_O.2.1.1.1.1.(g)	a hozzáférés-felügyeleti szabályzat meghatározza a megfelelőségi kritériumokat
20.		K02.001_O.2.1.1.1.2	a hozzáférés-felügyeleti szabályzat összhangban van a szervezetre vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal
21.		K02.001_O.2.1.1.2.(a)	a hozzáférés-felügyeleti eljárásrendet a szervezet kidolgozta és dokumentálta
22.		K02.001_O.2.1.1.2.(b)	a hozzáférés-felügyeleti eljárásrendet a szervezet kiadta
23.		K02.001_O.2.1.1.2.(c)	a hozzáférés-felügyeleti eljárásrendet a szervezet a K02.001_P[3] szerinti személyekkel vagy szerepkörökkel megismertette
24.		K02.001_O.2.1.2	a szervezet K02.001_P[4] szerint kijelölte a hozzáférés-felügyeleti szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelős személyt
25.		K02.001_O.2.1.3.(a)	a hozzáférés-felügyeleti szabályzatot a szervezet a K02.001_P[5] szerinti rendszerességgel felülvizsgálja és frissíti
26.		K02.001_O.2.1.3.(b)	a hozzáférés-felügyeleti szabályzatot a szervezet a K02.001_P[6] szerinti esemény(ek) bekövetkezésekor felülvizsgálja és frissíti
27.		K02.001_O.2.1.3.(c)	a hozzáférés-felügyeleti eljárásrendet a szervezet K02.001_P[7] szerinti rendszerességgel felülvizsgálja és frissíti
28.		K02.001_O.2.1.3.(d)	a hozzáférés-felügyeleti eljárásrendet a szervezet K02.001_P[8] szerinti esemény(ek) bekövetkezésekor felülvizsgálja és frissíti
29.	2.2. Fiókkezelés	K02.002_P[1]	meghatározottak a fiókok létrehozására irányuló kérelmek jóváhagyásához szükséges személyek vagy szerepkörök
30.		K02.002_P[2]	meghatározottak a fiókok létrehozására, engedélyezésére, módosítására, letiltására és eltávolítására vonatkozó irányelvek, eljárások, előfeltételek és kritériumok

31.		K02.002_P[3]	meghatározott az eseményekről értesítendő személy vagy szerepkör
32.		K02.002_P[4]	meghatározott az az időintervallum, amelyen belül a felhasználói fiókok megszüntetéséről a fiókkezelőket értesíteni kell
33.		K02.002_P[5]	meghatározott az az időintervallum, amelyen belül a felhasználók jogviszony megszűnéséről a fiókkezelőket értesíteni kell
34.		K02.002_P[6]	meghatározott az az időintervallum, amelyen belül a rendszerhasználat vagy az egyén számára szükséges ismeretek változásáról a fiókkezelőket értesíteni kell
35.		K02.002_P[7]	meghatározottak a rendszerhez való hozzáférés engedélyezéséhez egyéb, a szervezet által elvárt jellemzők
36.		K02.002_P[8]	meghatározott a felhasználói fiókok felülvizsgálata rendszerességének időintervalluma
37.		K02.002_O.2.2.1.(a)	az engedélyezett fióktípusokat meghatározták és dokumentálták
38.		K02.002_O.2.2.1.(b)	a kifejezetten tiltott fióktípusokat meghatározták és dokumentálták
39.		K02.002_O.2.2.2	a fiókkezelők kijelölésre kerültek
40.		K02.002_O.2.2.3	meghatározták a csoport- és szerepkör tagsági feltételeket és kritériumokat
41.		K02.002_O.2.2.4.1	meghatározták a rendszerben engedélyezett felhasználókat
42.		K02.002_O.2.2.4.2	meghatározták a csoport- és szerepkör tagságokat
43.		K02.002_O.2.2.4.3.(a)	meghatározták a hozzáférési jogosultságokat minden egyes felhasználói fiókra
44.		K02.002_O.2.2.4.3.(b)	meghatározták a felhasználói fiókokhoz tartozó jellemzőket
45.		K02.002_O.2.2.5	a felhasználói fiókok létrehozására vonatkozó kérelmek jóváhagyását a K02.002_P[1] szerepköröket betöltő személyek végzeték el
46.		K02.002_O.2.2.6.(a)	a fiókok létrehozása a K02.002_P[2] alapján történik
47.		K02.002_O.2.2.6.(b)	a fiókok engedélyezése a K02.002_P[2] alapján történik
48.		K02.002_O.2.2.6.(c)	a fiókok módosítása a K02.002_P[2] alapján történik
49.		K02.002_O.2.2.6.(d)	a fiókok letiltása a K02.002_P[2] alapján történik
50.		K02.002_O.2.2.6.(e)	a fiókok törlése a K02.002_P[2] alapján történik
51.		K02.002_O.2.2.7	a szervezet nyomon követi a fiókok használatát
52.		K02.002_O.2.2.8.1	K02.002_P[4] időn belül értesítésre kerül a fiókkezelő, illetve a K02.002_P[3] szerinti személy vagy szerepkör abban az esetben, ha a fiókok már nem szükségesek

53.		K02.002_O.2.2.8.2	amikor a felhasználók jogviszonya megszűnik, arról a K02.002_P[5] szerinti időn belül értesítésre kerül a fiókkezelő, illetve a K02.002_P[3] szerinti személy vagy szerepkör
54.		K02.002_O.2.2.8.3	K02.002_P[6] szerinti időn belül értesítésre kerül a fiókkezelő, illetve a K02.002_P[3] szerinti személy vagy szerepkör, amikor a rendszerhasználat vagy az egyén számára szükséges ismeretek megváltoznak
55.		K02.002_O.2.2.9.1	a szervezet érvényes hozzáférési engedély alapján engedélyezi a rendszerhez való hozzáférést
56.		K02.002_O.2.2.9.2	a szervezet a tervezett rendszerhasználatnak megfelelően engedélyezi a rendszerhez való hozzáférést
57.		K02.002_O.2.2.9.3	a szervezet a K02.002_P[7] által meghatározottaknak megfelelően engedélyezi a rendszerhez való hozzáférést
58.		K02.002_O.2.2.10	K02.002_P[8] szerinti időn belül ellenőrzik a felhasználói fiókokat a fiókkezelési követelmények betartása szempontjából
59.		K02.002_O.2.2.11.(a)	létrehozott a szervezet egy folyamatot a megosztott vagy csoport felhasználói fiókok hitelesítési adatainak megváltoztatására az egyének csoportból történő eltávolításának esetére
60.		K02.002_O.2.2.11.(b)	végrehajt a szervezet egy folyamatot a megosztott vagy csoport felhasználói fiókok hitelesítési adatainak megváltoztatására az egyének csoportból történő eltávolításának esetére
61.		K02.002_O.2.2.12	a szervezet összehangolja a fiókkezelési folyamatokat a felhasználók jogviszonyának megszüntetési folyamataival
62.	2.3. Fiókkezelés – Automatizált fiókkezelés	K02.003_P[1]	a rendszerfiókok kezelésének támogatására használt automatizált mechanizmusok meghatározásra kerülnek
63.		K02.003_O.2.3	a rendszerfiókok kezelését a K02.003_P[1] által meghatározott automatizált mechanizmusok támogatják
64.	2.4. Fiókkezelés – Automatizált ideiglenes és vészhelyzeti fiók kezelés	K02.004_P[1]	a következő PARAMÉTER-ÉRTÉKEK egyike került kiválasztásra: {eltávolítás; letiltás}
65.		K02.004_P[2]	az ideiglenes vagy vészhelyzeti fiókok automatikus eltávolítására vagy letiltására szolgáló időtartam meghatározott
66.		K02.004_O.2.4	az ideiglenes vagy vészhelyzeti fiókok automatikusan eltávolításra vagy letiltásra kerülnek a K02.004_P[1] által meghatározottak szerint a K02.004_P[2] által meghatározott időtartam után
67.	2.5. Fiókkezelés – Fiókok letiltása	K02.005_P[1]	meghatározásra került az az időtartam, amelyen belül a fiókokat le kell tiltani
68.		K02.005_P[2]	az inaktivitás időtartama meghatározásra került, amelyet követően a fiókok letiltásra kerülnek
69.		K02.005_O.2.5.1	a fiókok letiltásra kerülnek a K02.005_P[1] által meghatározott időtartamot követően, ha a fiókok lejártak
70.		K02.005_O.2.5.2	a fiókok a K02.005_P[1] által meghatározott időtartamon belül letiltásra kerülnek, ha a fiókok már nem kapcsolódnak egy felhasználóhoz vagy személyhez
71.		K02.005_O.2.5.3	a fiókok a K02.005_P[1] által meghatározott időtartamon belül letiltásra kerülnek, ha a fiókok megsértik a szervezeti szabályzatot
72.		K02.005_O.2.5.4	a fiókok a K02.005_P[1] által meghatározott időtartamon belül letiltásra kerülnek, ha a K02.005_P[2] által meghatározott időtartamon belül inaktívak voltak

73.	2.6. Fiókkezelés – Automatikus naplózási műveletek	K02.006_O.2.6.1.(a)	a fiókok létrehozásával kapcsolatos tevékenységek automatikusan naplózásra kerülnek
74.		K02.006_O.2.6.1.(b)	a fiókok módosításával kapcsolatos tevékenységek automatikusan naplózásra kerülnek
75.		K02.006_O.2.6.1.(c)	a fiókok engedélyezésével kapcsolatos tevékenységek automatikusan naplózásra kerülnek
76.		K02.006_O.2.6.1.(d)	a fiókok letiltásával kapcsolatos tevékenységek automatikusan naplózásra kerülnek
77.		K02.006_O.2.6.1.(e)	a fiókok eltávolításával kapcsolatos tevékenységek automatikusan naplózásra kerülnek
78.	2.7. Fiókkezelés – Inaktivitásból fakadó kijelentkeztetés	K02.007_P[1]	meghatározásra került az az inaktivitás időtartama vagy időpont, amelyet követően a felhasználó kijelentkeztetése megtörténik
79.		K02.007_O.2.7	a K02.007_P[1] által meghatározott időtartam leteltét követően vagy az adott időpontban a felhasználók kijelentkeztetése megtörténik
80.	2.12. Fiókkezelés – Használati feltételek	K02.012_P[1]	a rendszerfiókok esetében érvényesítendő körülmények, illetve használati feltételek meghatározásra kerültek
81.		K02.012_P[2]	a körülmények, illetve a használati feltételek érvényesítésének hatálya alá tartozó rendszerfiókok meghatározásra kerültek
82.		K02.012_O.2.12	megtörténik a K02.012_P[1] által meghatározott használati feltételek kikényszerítése a K02.012_P[2] által meghatározott rendszerfiókokra
83.	2.13. Fiókkezelés – Fiókok szokatlan használatának felügyelete	K02.013_P[1]	meghatározásra került az a megszokottól eltérő használat, amelynek vonatkozásában a rendszerfiókokat felügyelni kell
84.		K02.013_P[2]	a megszokottól eltérő használatot jelentő személyek vagy szerepkörök meghatározásra kerültek
85.		K02.013_O.2.13.1	a rendszerfiókok a K02.013_P[1] által meghatározottak szerint kerülnek ellenőrzésre
86.		K02.013_O.2.13.2	a rendszerfiókok megszokottól eltérő használatát jelentik a K02.013_P[2] által meghatározott személyeknek vagy szerepköröknek
87.	2.14. Fiókkezelés – Magas kockázatú személyek fiókjának letiltása	K02.014_P[1]	meghatározottak a magas kockázatot jelentő személyek
88.		K02.014_P[2]	meghatározott az az időtartam, amelyen belül a magas kockázatot jelentő személyek fiókjait le kell tiltani
89.		K02.014_P[3]	a fiókok letiltását eredményező jelentős kockázatok meghatározásra kerülnek
90.		K02.014_O.2.14	a K02.014_P[1] szerinti személyek felhasználói fiókjai a K02.014_P[3] szerinti események esetén K02.014_P[2] által meghatározott időtartamon belül letiltásra kerülnek
91.	2.15. Hozzáférési szabályok érvényesítése	K02.015_O.2.15	az információhoz és a rendszer erőforrásaihoz való logikai hozzáférés jóváhagyott jogosultságait a szabályzatokkal összhangban érvényesítik
92.	2.28. Információáramlási szabályok érvényesítése	K02.028_P[1]	a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás-szabályozási irányelvek meghatározásra kerültek

93.		K02.028_O.2.28	a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzésére jóváhagyott engedélyek érvényesülnek a K02.028_P[1] által meghatározottak szerint
94.	2.32. Információáramlási szabályok érvényesítése – Titkosított információk áramlásának irányítása	K02.032_P[1]	meghatározásra kerültek azok az információáramlás-ellenőrzési mechanizmusok, amelyek megakadályozzák a titkosított információ megkerülését
95.		K02.032_P[2]	a szervezet a következő, a titkosított információ megkerülésére vonatkozó próbálkozástípusok valamelyikét kezeli: - az információk dekódolása, - a titkosított információáramlás blokkolása, - a titkosított információk átvitele
96.		K02.032_P[3]	a szervezet meghatározta azt az eljárást vagy módszert, amellyel megakadályozható, hogy az információáramlás-ellenőrzési mechanizmusokat kijátsszák
97.		K02.032_O.2.32	a titkosított információ a K02.028_P[1] által meghatározott információáramlás-ellenőrzési mechanizmusok megkerülésében a K02.032_P[2] által meghatározott próbálkozásokat a munkaszakasz megszakításával megakadályozza
98.	2.59. Felelősségek szétválasztása	K02.059_P[1]	meghatározásra kerültek azon személyek, akiknek K02.059_O.2.59.1 szerinti feladatellátást elkülönített módon kell ellátniuk
99.		K02.059_O.2.59.1	a K02.059_P[1] által meghatározott személyek feladatai meghatározásra és dokumentálásra kerültek
100.		K02.059_O.2.59.2	a feladatok szétválasztását támogató rendszer-hozzáférési jogosultságok meghatározásra kerültek
101.	2.60. Legkisebb jogosultság elve	K02.060_O.2.60	a legkisebb jogosultság elve érvényesül, amely csak olyan engedélyezett hozzáféréseket engedélyez a felhasználók vagy a felhasználók nevében eljáró folyamatok számára, amelyek szükségesek a kijelölt szervezeti feladatok elvégzéséhez
102.	2.61. Legkisebb jogosultság elve – Hozzáférés biztosítása a biztonsági funkciókhoz	K02.061_P[1]	a biztonsági funkciókhoz és a biztonság szempontjából fontos információkhoz való hozzáférési jogosultsággal rendelkező személyek és szerepkörök meghatározottak
103.		K02.061_P[2]	meghatározottak azok a biztonsági funkciók és a biztonság szempontjából releváns információk, amelyekhez az engedélyezett hozzáféréshez szükséges
104.		K02.061_O.2.61.2	a K02.061_P[2] által meghatározott biztonsági szempontból releváns információkhoz való hozzáférés csak a K02.061_P[1] által meghatározott személyek és szerepkörök számára engedélyezett
105.	2.62. Legkisebb jogosultság elve – Nem privilegizált hozzáférés biztosítása a nem biztonsági funkciókhoz	K02.062_P[1]	meghatározásra kerültek azok a biztonsági funkciók vagy biztonsági szempontból releváns információk, amelyekhez a K02.061_P[1] szerinti személyek hozzáférése csak privilegizált felhasználói fiókhoz kapcsoltan engedélyezett
106.		K02.062_O.2.62	a K02.062_P[1] által meghatározottak szerint a biztonsági funkciókhoz vagy a biztonság szempontjából fontos információkhoz csak privilegizált fiókon keresztül engedélyezett a hozzáférés
107.		K02.063_P[1]	meghatározásra kerültek azok a privilegizált parancsok, amelyekhez történő hozzáférés csak kényszerű üzemeltetési okból engedélyezhető

108.	2.63. Legkisebb jogosultság elve – Hálózati hozzáférés a privilegizált parancsokhoz	K02.063_P[2]	a privilegizált parancsokhoz való hálózati hozzáférést szükségessé tevő kényszerű üzemeltetési okok meghatározottak
109.		K02.063_O.2.63.1.(a)	a K02.063_P[1] által meghatározott privilegizált parancsokhoz való hálózati hozzáférés csak a K02.063_P[2] által meghatározott esetben engedélyezett
110.		K02.063_O.2.63.1.(b)	a privilegizált parancsokhoz való hálózati hozzáférés engedélyezésének indoklása dokumentálásra került a rendszerbiztonsági tervben
111.	2.65. Legkisebb jogosultság elve – Privilegizált fiókok	K02.065_P[1]	meghatározottak azok a személyek vagy szerepkörök, amelyekre az EIR privilegizált fiókjai alkalmazandóak
112.		K02.065_O.2.65	a privilegizált fiókok használata kizárólag a K02.065_P[1] által meghatározott személyek vagy szerepkörök számára engedélyezett
113.	2.67. Legkisebb jogosultság elve – Felhasználói jogosultságok felülvizsgálata	K02.067_P[1]	a szerepkörökhöz vagy felhasználói csoportokhoz rendelt jogosultságok felülvizsgálatának gyakorisága meghatározott
114.		K02.067_P[2]	a jogosultságokhoz rendelt szerepkörök vagy felhasználói csoportok meghatározásra kerültek
115.		K02.067_O.2.67.1	a K02.067_P[2] által meghatározott szerepkörökhöz és felhasználói csoportokhoz rendelt jogosultságok a K02.067_P[1] által meghatározott gyakorisággal felülvizsgálatra kerülnek a jogosultságok szükségességének igazolása érdekében
116.		K02.067_O.2.67.2	a felülvizsgálat során lehetőség van a jogosultságok újraosztására vagy megszüntetése
117.	2.69. Legkisebb jogosultság elve – Privilegizált funkciók használatának naplózása	K02.069_O.2.69	a privilegizált funkciók végrehajtása naplózott
118.	2.70. Legkisebb jogosultság elve – Nem-privilegizált felhasználók korlátozása	K02.070_O.2.70	a nem privilegizált felhasználók nem hajthatnak végre privilegizált funkciókat
119.	2.71. Sikertelen bejelentkezési kísérletek	K02.071_P[1]	meghatározott az esetszám a felhasználó meghatározott időtartamon belül engedélyezett egymást követő sikertelen bejelentkezési kísérleteire
120.		K02.071_P[2]	meghatározott az az időtartam, amelyen belül a K02.071_P[1] szerinti sikertelen bejelentkezési kísérletek engedélyezettek
121.		K02.071_P[3]	a K02.071_P[2] időtartamon belül K02.071_P[1] számot meghaladó, egymást követő sikertelen bejelentkezési kísérlet esetén a szervezet a következő intézkedések valamelyikét alkalmazza: 1. K02.071_P[4] szerint meghatározott időtartamú fiókzárolás, 2. rendszergazda feloldást igénylő fiókzárolás, vagy 3. következő bejelentkezési lehetőség késleltetése a K02.071_P[5] algoritmus szerint
122.		K02.071_P[4]	meghatározott a fiókzárolás időtartama
123.		K02.071_P[5]	meghatározott a következő bejelentkezés késleltetésének algoritmusa

124.		K02.071_O.2.71.1	korlátozás érvényesül a felhasználó által a K02.071_P[2] által meghatározott időszak alatt K02.071_P[1] számot meghaladó egymást követő érvénytelen bejelentkezési kísérletek számának elérése után
125.		K02.071_O.2.71.2.(a)	a K02.071_P[3] által meghatározottak szerint korlátozás érvényesül
126.		K02.071_O.2.71.2.(b)	a K02.071_O.2.71.1 esetén a rendszergazda értesítése megtörténik
127.		K02.071_O.2.71.2.(c)	a K02.071_P[4] szerinti időtartam alatt a fiókzárolás fennáll, amelyet rendszergazda feloldhat
128.	2.75. A rendszerhasználat jelzése	K02.075_P[1]	meghatározott az a rendszerhasználati értesítés vagy banner, amelyet a rendszer a felhasználóknak a rendszerhez való hozzáférés engedélyezése előtt megjelenít
129.		K02.075_P[2]	nyilvánosan hozzáférhető EIR-ek esetén meghatározottak a rendszerhasználat feltételei, amelyeket az EIR a további hozzáférés engedélyezése előtt megjelenít
130.		K02.075_O.2.75.1	az EIR a használata előtt megjeleníti a felhasználóknak azt a K02.075_P[1] rendszerhasználati értesítést vagy üzenetet, amely biztonsági értesítést tartalmaz a szervezetre vonatkozó, hatályos jogszabályi előírásokban, irányelvekben, szabályozásokban, eljárásrendekben, szabványokban és útmutatókban meghatározottak szerint
131.		K02.075_O.2.75.1.1	a rendszerhasználati értesítés tartalmazza, hogy a felhasználók a szervezet EIR-ét használják
132.		K02.075_O.2.75.1.2	a rendszerhasználati értesítés tartalmazza, hogy az EIR használatát megfigyelhetik, rögzíthetik, naplózhatják
133.		K02.075_O.2.75.1.3	a rendszerhasználati értesítés tartalmazza, hogy a rendszer jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár
134.		K02.075_O.2.75.1.4	a rendszerhasználati értesítés tartalmazza, hogy a rendszer használata az előbbiekben részletezett feltételek elfogadását jelenti
135.		K02.075_O.2.75.2	a rendszerhasználati értesítés a képernyőn marad, mindaddig, amíg a felhasználók nem fogadják el a használati feltételeket és nem tesznek egyértelmű lépéseket az EIR-be való bejelentkezésre vagy az EIR-hez való további hozzáférésre
136.		K02.075_O.2.75.3	nyilvánosan hozzáférhető EIR-ek esetében a nyilvánosan hozzáférhető EIR-hez való további hozzáférés engedélyezése előtt megjelenik a rendszerhasználati információ a K02.075_P[2] által meghatározottak szerint
137.		K02.075_O.2.75.3.1	nyilvánosan hozzáférhető rendszerek esetén a rendszerhasználati értesítés tartalmazza, hogy a felhasználók a szervezet EIR-ét használják
138.		K02.075_O.2.75.3.2	nyilvánosan hozzáférhető EIR-ek esetén a rendszerhasználati értesítés tartalmazza, hogy az EIR használatát megfigyelhetik, rögzíthetik, naplózhatják
139.		K02.075_O.2.75.3.3	nyilvánosan hozzáférhető EIR-ek esetén a rendszerhasználati értesítés tartalmazza, hogy az EIR jogosulatlan használata tilos és büntető- vagy polgári jogi felelősséggel jár
140.	2.81. Egyidejű munkaszakasz kezelés	K02.081_P[1]	meghatározottak azok a fiókok, illetve fióktípusok, amelyek esetében az egyidejű munkamenetek számát korlátozni kell

141.		K02.081_P[2]	az egyes fiókok, illetve fióktípusok számára engedélyezett egyidejű munkamenetek száma meghatározott
142.		K02.081_O.2.81	az egyidejű munkamenetek száma a K02.081_P[1] által meghatározott fiókok, illetve fiók típusok esetében a K02.081_P[2] által meghatározott számra korlátozódik
143.	2.82. Eszköz zárolása	K02.082_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {a K02.082_P[2] által meghatározott inaktivitás után; a felhasználó erre irányuló lépése esetén}
144.		K02.082_P[2]	meghatározott az az inaktivitási időtartam, amelyet követően az eszköz zárolása automatikusan megtörténik
145.		K02.082_O.2.82.1	az EIR-hez való további hozzáférés megakadályozásra kerül a K02.082_P[1] által meghatározottak szerint
146.		K02.082_O.2.82.2	az eszköz zárolása mindaddig fennmarad, amíg a felhasználó a meghatározott azonosítási és hitelesítési eljárásokat végre nem hajtja
147.	2.83. Eszköz zárolása – Képernyőtakarás	K02.083_O.2.83	a K02.082_P[1] szerinti eszközzárolás esetén a kijelzőn lévő információk elrejtésre kerülnek
148.	2.84. A munkaszakasz lezárása	K02.084_P[1]	a munkamenet megszakítását igénylő feltételek vagy kiváltó események meghatározásra kerültek
149.		K02.084_O.2.84	a felhasználói munkamenet automatikusan megszűnik a K02.084_P[1] által meghatározott feltételek vagy kiváltó események után
150.	2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	K02.088_P[1]	meghatározottak azok a felhasználói tevékenységek, amelyek – a szervezeti célokkal és üzleti funkciókkal összhangban – az EIR-ben azonosítás vagy hitelesítés nélkül is végrehajthatóak
151.		K02.088_O.2.88.1	az EIR-ben azonosítás és hitelesítés nélkül végrehajthatóak a K02.088_P[1] által meghatározott műveletek
152.		K02.088_O.2.88.2	az azonosítás és hitelesítés nélkül végrehajtható műveletek a rendszerbiztonsági tervben dokumentálásra kerültek
153.	2.100. Távoli hozzáférés	K02.100_O.2.100.1.(a)	az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozások kidolgozottak és dokumentáltak
154.		K02.100_O.2.100.1.(b)	a konfigurációs vagy csatlakozási követelmények az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan kidolgozottak és dokumentáltak
155.		K02.100_O.2.100.1.(c)	az alkalmazási útmutatók az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan kidolgozottak és dokumentáltak
156.		K02.100_O.2.100.2	az engedélyezett távoli hozzáférés minden egyes típusa esetén engedélyezési eljárás történik az ilyen kapcsolatok lehetővé tételét megelőzően
157.	2.101. Távoli hozzáférés – Felügyelet és irányítás	K02.101_O.2.101.1.(a)	automatizált mechanizmusokat alkalmaznak a távoli hozzáférési módszerek felügyeletére
158.		K02.101_O.2.101.1.(b)	automatizált mechanizmusokat alkalmaznak a távoli hozzáférési módszerek ellenőrzésére
159.	2.102. Távoli hozzáférés – Bizalmasság és sértetlenség védelme titkosítás által	K02.102_O.2.102	kriptográfiai mechanizmusokat alkalmaznak a távoli hozzáférési munkamenetek biztonságának és integritásának védelmére

160.	2.103. Távoli hozzáférés – Menedzselt hozzáférés-felügyeleti pontok	K02.103_O.2.103	a távoli hozzáférések engedélyezett és menedzselt hálózati hozzáférés-ellenőrző pontokon keresztül kerülnek irányításra
161.	2.104. Távoli hozzáférés – Privilegizált parancsok és hozzáférés	K02.104_P[1]	a privilegizált jogosultságot igénylő műveletekhez kapcsolódó követelmények meghatározottak
162.		K02.104_P[2]	a biztonságkritikus információkhoz kapcsolódó követelmények meghatározottak
163.		K02.104_O.2.104.1.(a)	a privilegizált műveletek távoli hozzáférésen keresztül történő végrehajtása csak olyan formátumban engedélyezett, amely értékelhető bizonyítékot szolgáltat
164.		K02.104_O.2.104.1.(b)	a biztonságkritikus információkhoz való hozzáférés távoli hozzáférésen keresztül csak olyan formátumban engedélyezett, amely értékelhető bizonyítékot szolgáltat
165.		K02.104_O.2.104.1.(c)	a privilegizált műveletek távoli hozzáférésen keresztül történő végrehajtása csak a K02.104_P[1] által meghatározottak szerint történik
166.		K02.104_O.2.104.1.(d)	a biztonságkritikus információkhoz való hozzáférés távoli hozzáférésen keresztül csak a K02.104_P[2] által meghatározottak szerint történik
167.		K02.104_O.2.104.2	a távoli hozzáférés szabályait a rendszerbiztonsági tervben dokumentálták
168.	2.108. Vezeték nélküli hozzáférés	K02.108_O.2.108.1.(a)	a használati korlátozások a vezeték nélküli hozzáférés minden egyes típusára vonatkozóan kidolgozottak és dokumentáltak
169.		K02.108_O.2.108.1.(b)	a konfigurációs követelmények a vezeték nélküli hozzáférés minden egyes típusára vonatkozóan kidolgozottak és dokumentáltak
170.		K02.108_O.2.108.1.(c)	a kapcsolódási követelmények a vezeték nélküli hozzáférés minden egyes típusára vonatkozóan kidolgozottak és dokumentáltak
171.		K02.108_O.2.108.2	a vezeték nélküli hozzáférés minden egyes típusa esetén engedélyezési eljárás történik az ilyen kapcsolatok lehetővé tételét megelőzően
172.	2.109. Vezeték nélküli hozzáférés – Hitelesítés és titkosítás	K02.109_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {felhasználók; eszközök}
173.		K02.109_O.2.109.1.(a)	az EIR-hez való vezeték nélküli hozzáférés a K02.109_P[1] által meghatározott entitás esetén hitelesítéssel védett
174.		K02.109_O.2.109.1.(b)	az EIR-hez való vezeték nélküli hozzáférés titkosítással védett
175.	2.110. Vezeték nélküli hozzáférés – Vezeték nélküli hálózat letiltása	K02.110_O.2.110	a rendszerelemekbe ágyazott vezeték nélküli hálózati hozzáférések – ha azok használata nem szükséges – tiltottak
176.	2.111. Vezeték nélküli hozzáférés – Felhasználók általi konfiguráció korlátozása	K02.111_O.2.111.1.(a)	a vezeték nélküli hálózati funkciók önálló konfigurálására jogosult felhasználók azonosítottak
177.		K02.111_O.2.111.1.(b)	a vezeték nélküli hálózati funkciók önálló konfigurálására jogosult felhasználók engedélyezésre kerültek

178.	2.112. Vezeték nélküli hozzáférés – Antennák és átviteli teljesítmény	K02.112_O.2.112.1.(a)	a rádióantennákat úgy választják ki, hogy csökkentsék annak valószínűségét, hogy a vezeték nélküli hozzáférési pontok jeleit a szervezet által ellenőrzött határokon kívül is fogni lehessen
179.		K02.112_O.2.112.1.(b)	az átviteli teljesítményszintek úgy vannak kalibrálva, hogy csökkentsék annak valószínűségét, hogy a vezeték nélküli hozzáférési pontok jeleit a szervezet által ellenőrzött határokon kívül is fogni lehessen
180.	2.113. Mobil eszközök hozzáférés-ellenőrzése	K02.113_O.2.113.1.(a)	a szervezet által ellenőrzött mobil eszközök tekintetében a kapcsolódási követelmények kidolgozottak és dokumentáltak
181.		K02.113_O.2.113.1.(b)	a szervezet által ellenőrzött mobil eszközök tekintetében a konfigurációs követelmények kidolgozottak és dokumentáltak
182.		K02.113_O.2.113.1.(c)	a szervezet által ellenőrzött mobil eszközök tekintetében az alkalmazási útmutatók kidolgozottak és dokumentáltak
183.		K02.113_O.2.113.2	a szervezet által ellenőrzött mobil eszközök esetében engedélyezési eljárás történik a szervezet EIR-jeihez történő hozzáférést megelőzően
184.	2.114. Mobil eszközök hozzáférés-ellenőrzése – Teljes eszköz vagy konténer-alapú titkosítás	K02.114_P[1]	a következő PARAMÉTER-ÉRTÉKEK egyike került kiválasztásra: {teljes készüléktitkosítás; konténeralapú titkosítás}
185.		K02.114_P[2]	meghatározásra kerültek azok a mobil alkalmazások, amelyeken a titkosítást alkalmazni kell
186.		K02.114_O.2.114	a K02.114_P[2] által meghatározott mobil eszközökön lévő információk a K02.114_P[1] szerinti titkosítással védettek
187.	2.115. Külső elektronikus információs rendszerek használata	K02.115_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {megállapítja az <K02.115_P[2] feltételeket>; azonosítja az <K02.115_P[3] ellenőrzéseket>}
188.		K02.115_P[2]	meghatározottak a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel kialakított bizalmi kapcsolatokkal összhangban lévő feltételek
189.		K02.115_P[3]	meghatározottak a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel kialakított bizalmi kapcsolatokkal összhangban lévő, a külső rendszereken végrehajtandó ellenőrzések
190.		K02.115_P[4]	meghatározottak azon külső rendszerek típusai, amelyek használata tiltott
191.		K02.115_O.2.115.1.1	a K02.115_P[1] által meghatározottak összhangban állnak a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel kialakított bizalmi kapcsolatokkal, lehetővé téve az arra jogosult személyek számára a rendszerhez való hozzáférést külső rendszerekből
192.		K02.115_O.2.115.1.2	a K02.115_P[1] által meghatározottak összhangban állnak a külső rendszereket birtokló, üzemeltető, illetve karbantartó más szervezetekkel kialakított bizalmi kapcsolatokkal, lehetővé téve az arra jogosult személyek számára a szervezet által ellenőrzött információk feldolgozását, tárolását vagy továbbítását külső rendszerek használatával
193.		K02.115_O.2.115.2	a K02.115_P[4] által meghatározott típusú külső rendszerek használata tiltott és a tiltás érvényesül

194.	2.116. Külső rendszerek használata – Engedélyezett használat korlátozásai	K02.116_O.2.116.1 (a)	külső rendszer használata csak a külső rendszeren alkalmazott védelmi intézkedések ellenőrzését követően kerül engedélyezésre
195.		K02.116_O.2.116.1 (b)	külső rendszerhez való hozzáférés csak a külső rendszeren alkalmazott védelmi intézkedések ellenőrzését követően engedélyezhető
196.		K02.116_O.2.116.1 (c)	a szervezet által ellenőrzött információk feldolgozására, tárolására vagy továbbítására külső rendszer csak akkor alkalmazható, ha a külső rendszeren alkalmazott védelmi intézkedések ellenőrzése megtörtént
197.		K02.116_O.2.116.2 (a)	a szervezet a külső rendszert üzemeltető szervezettel rendszerkapcsolati vagy feldolgozási megállapodást kötött
198.		K02.116_O.2.116.2 (b)	a szervezet a rendszerkapcsolati vagy feldolgozási megállapodásokban foglaltakat betartja és betartatja
199.	2.117. Külső rendszerek használata – Hordozható adattárolók használatának korlátozása	K02.117_P[1]	a szervezet által ellenőrzött hordozható adattároló eszközök külső rendszereken történő, felhatalmazott személyek általi használatára vonatkozó korlátozások meghatározásra kerültek
200.		K02.117_O.2.117	a szervezet által ellenőrzött hordozható adattároló eszközök engedélyezett személyek általi használata külső rendszereken a K02.117_P[1] által meghatározottak szerint korlátozott
201.	2.121. Információmegosztás	K02.121_P[1]	meghatározásra kerültek azok az információmegosztási körülmények, amikor a felhasználónak mérlegelnie kell, hogy a megosztásban résztvevő partnerhez rendelt hozzáférési jogosultságok megfelelnek-e az információ hozzáférési és felhasználási korlátozásoknak
202.		K02.121_P[2]	olyan automatizált mechanizmusokat vagy kézi folyamatokat határoznak meg, amelyek segítik a felhasználókat az információmegosztási és együttműködési döntések meghozatalában
203.		K02.121_O.2.121.1	az engedélyezett felhasználók számára lehetővé válik annak megállapítása, hogy a partnerhez rendelt hozzáférési jogosultságok megfelelnek-e az információ hozzáférési és felhasználási korlátozásoknak a K02.121_P[1] által meghatározottak szerint
204.		K02.121_O.2.121.2	a K02.121_P[2] által meghatározottak szerinti automatizált mechanizmusokat alkalmaznak, hogy segítsék a felhasználókat az információmegosztási és együttműködési döntések meghozatalában
205.	2.124. Nyilvánosan elérhető tartalom	K02.124_P[1]	meghatározott, hogy milyen gyakorisággal kell felülvizsgálni a nyilvánosan hozzáférhető EIR tartalmát a nem nyilvános információk tekintetében
206.		K02.124_O.2.124.1	a szervezet kijelölte azokat a személyeket, akik jogosultak arra, hogy információkat tegyenek nyilvánosan hozzáférhetővé
207.		K02.124_O.2.124.2	az erre felhatalmazott személyek képzést kapnak annak biztosítására, hogy a nyilvánosan hozzáférhető információk között ne szerepeljenek nem nyilvános információk
208.		K02.124_O.2.124.3	K02.124_O.2.124.1 szerinti feljogosított személy áttekinti az információ tervezett tartalmát a nyilvánosan hozzáférhető rendszerbe történő közzététel előtt, annak érdekében, hogy biztosítsa, hogy az nem tartalmaz nem nyilvános információkat
209.		K02.124_O.2.124.4.(a)	a K02.124_P[1] szerint meghatározott gyakorisággal áttekintik a nyilvánosan hozzáférhető rendszer tartalmát a nem nyilvános információk szempontjából

210.		K02.124_O.2.124.4.(b)	eltávolítják a nem nyilvános információkat, ha felfedezik őket

3. Tudatosság és képzés

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	3.1. Szabályzat és eljárásrendek	K03.001_P[1]	meghatározottak azok a személyek vagy szerepkörök, akikkel a tudatossági és képzési szabályzatot meg kell ismertetni
3.		K03.001_P[2]	meghatározottak azokat a személyek vagy szerepkörök, akikkel a tudatossági és képzési eljárásokat meg kell ismertetni
4.		K03.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K03.001_P[4]	a tudatossági és képzési szabályzat és eljárások irányítására egy meghatározott személy került kijelölésre
6.		K03.001_P[5]	a tudatossági és képzési szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K03.001_P[6]	meghatározottak azokat az események, amelyek a tudatossági és képzési szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K03.001_O.3.1.1.(a)	tudatossági és képzési szabályzatot dolgoztak ki és dokumentáltak
9.		K03.001_O.3.1.1.(b)	a tudatossági és képzési szabályzatot a K03.001_P[1] által meghatározott személyek vagy szerepkörök megismerték
10.		K03.001_O.3.1.1.(c)	a tudatossági és képzési szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő tudatossági és képzési eljárások kidolgozásra és dokumentálásra kerültek
11.		K03.001_O_3.1.1.(d)	a tudatossági és képzési eljárásokat a K03.001_P[2] által meghatározott személyekkel vagy szerepkörökkel megismertették
12.		K03.001_O_3.1.2	a K03.001_P[4] által meghatározott személy a tudatossági és képzési szabályzat és eljárások kidolgozását, dokumentálását, kiadását és megismertetésének irányítását elvégezte
13.		K03.001_O_3.1.3.(a)	a tudatossági és képzési szabályzatot, a tudatossági és képzési eljárásokat és eljárásrendeket felülvizsgálják és frissítik a K03.001_P[5] által meghatározott gyakorisággal
14.		K03.001_O_3.1.3.(b)	a tudatossági és képzési szabályzatot, a tudatossági és képzési eljárásokat és eljárásrendeket felülvizsgálják és frissítik a K03.001_P[6] által meghatározott eseményeket követően
15.		K03.001_O_3.1.1.1.1.(a)	a tudatossági és képzési szabályzat célja meghatározásra került a K03.001_P[3] által meghatározottak szerint

16.		K03.001_O_3.1.1.1.1.(b)	a tudatossági és képzési szabályzat hatóköre meghatározásra került a K03.001_P[3] által meghatározottak szerint
17.		K03.001_O_3.1.1.1.1.(c)	a tudatossági és képzési szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K03.001_P[3] által meghatározottak szerint
18.		K03.001_O_3.1.1.1.1.(d)	a tudatossági és képzési szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K03.001_P[03] által meghatározottak szerint
19.		K03.001_O_3.1.1.1.1.(e)	a tudatossági és képzési szabályzathoz kapcsolódó vezetői elkötelezettség meghatározásra került a K03.001_P[3] által meghatározottak szerint
20.		K03.001_O_3.1.1.1.1.(f)	a tudatossági és képzési szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K03.001_P[3] által meghatározottak szerint
21.		K03.001_O_3.1.1.1.1.(g)	a tudatossági és képzési szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K03.001_P[3] által meghatározottak szerint
22.		K03.001_O_3.1.1.1.2.	a K03.001_P[3] által meghatározott tudatossági és képzési szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal
23.	3.2. Biztonságtudatossági képzés	K03.002_P[1]	meghatározták, hogy az alapképzést követően milyen gyakorisággal kell biztonsági ismeretekkel kapcsolatos képzést nyújtani a rendszerhasználóknak, beleértve a vezetőket, felsővezetőket és szerződéses partnereket
24.		K03.002_P[2]	meghatározták azokat az eseményeket, amelyek a felhasználók számára biztonsági ismeretek oktatását igénylik
25.		K03.002_P[3]	meghatározása kerültek a rendszerhasználók biztonságtudatosságának növelése érdekében alkalmazandó technikák
26.		K03.002_P[4]	meghatározták, hogy milyen gyakorisággal kell frissíteni a képzési és tudatossági tananyag tartalmát
27.		K03.002_P[5]	meghatározásra kerültek azok az események, amelyek a képzési és tudatossági tananyag tartalmának frissítését igénylik
28.		K03.002_O.3.2.1.1.(a)	az új felhasználók alapképzésének részeként a rendszer felhasználói – beleértve a vezetőket, felsővezetőket és szerződéses partnereket – biztonsági ismeretekkel kapcsolatos képzésben részesültek
29.		K03.002_O.3.2.1.1.(b)	a rendszer felhasználói – beleértve a vezetőket, a felsővezetőket és a szerződéses partnereket – a K03.002_P[1] által meghatározott gyakorisággal biztonsági ismeretekkel kapcsolatos képzésben részesülnek
30.		K03.002_O.3.2.1.2.	a rendszerhasználók – beleértve a vezetőket, felsővezetőket és szerződéses partnereket – biztonsági ismeretekkel kapcsolatos képzésben részesültek, ha a rendszerváltozások vagy a K03.002_P[2] által meghatározott események ezt megkövetelték
31.		K03.002_O.3.2.2	a K03.002_P[3] által meghatározott technikák kerülnek alkalmazásra a rendszer felhasználói biztonságtudatosságának növelésére
32.		K03.002_O.3.2.3.(a)	a képzési és tudatossági tananyag tartalma a K03.002_P[4] által meghatározott gyakorisággal kerül frissítésre

33.		K03.002_O.3.2.3.(b)	a képzési és tudatossági tananyag tartalma a K03.002_P[5] által meghatározott eseményeket követően frissítésre kerül
34.		K03.002_O.3.2.4	a belső vagy külső biztonsági eseményekből vagy jogsértésekből levont tanulságok beépítésre kerültek a képzési anyagokba, valamint az alkalmazott biztonságtudatossági technikákba
35.	3.4. Biztonságtudatossági képzés – Belső fenyegetés	K03.004_O.3.4.1.(a)	a belső fenyegetés potenciális jeleinek felismeréséről szóló felkészítő képzés megtartásra került
36.		K03.004_O.3.4.1.(b)	a belső fenyegetés potenciális jeleinek jelentésére vonatkozó felkészítő képzés megtartásra került
37.	3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés	K03.005_O.3.5.1.(a)	a pszichológiai manipulációs tevékenység potenciális és tényleges eseteinek felismerésére vonatkozó felkészítő képzés megtartásra került
38.		K03.005_O.3.5.1.(b)	a pszichológiai manipulációs tevékenység potenciális és tényleges eseteinek jelentésére vonatkozó felkészítő képzés megtartásra került
39.		K03.005_O.3.5.1.(c)	az adatgyűjtés potenciális és tényleges eseteinek felismerésére vonatkozó felkészítő képzés megtartásra került
40.		K03.005_O.3.5.1.(d)	az adatgyűjtés potenciális és tényleges eseteinek jelentésére vonatkozó felkészítő képzés megtartásra került
41.	3.9. Szerepkör alapú biztonsági képzés	K03.009_P[1]	a szerepek és felelősségi körök meghatározásra kerültek a szerepkör alapú biztonsági képzéshez
42.		K03.009_P[2]	meghatározták, hogy az alapképzést követően milyen gyakorisággal kell szerepkör alapú biztonsági képzést tartani a kijelölt személyzetnek
43.		K03.009_P[3]	a szerepkör alapú képzési tartalom frissítésének gyakorisága meghatározott
44.		K03.009_P[4]	meghatározásra kerültek azok az események, amelyek a szerepkör-alapú képzési tartalom frissítését igénylik
45.		K03.009_O.3.9.1.1.(a)	a K03.009_P[1] által meghatározott szerepek és felelősségi körök szerepkör alapú biztonsági képzésben részesültek, mielőtt a rendszerhez, információhoz való hozzáférést vagy a kijelölt feladatok végrehajtásához szükséges hozzáféréseket megkapták
46.		K03.009_O.3.9.1.1.(b)	a K03.009_P[1] szerinti szerepek és felelősségi körök és a K03.009_P[2] által meghatározott gyakoriság szerinti szerepkör alapú biztonsági képzés megtartásra került
47.		K03.009_O.3.9.1.2	a kijelölt biztonsági szerepkörökkel és felelősségi körökkel rendelkező személyzet számára szerepalapú biztonsági képzést biztosítanak, ha a rendszerváltozások ezt megkövetelik
48.		K03.009_O.3.9.2.(a)	a szerepkör alapú képzési tartalom frissítése a K03.009_P[3] által meghatározott gyakorisággal történik
49.		K03.009_O.3.9.2.(b)	a szerepkör alapú képzési tartalom a K03.009_P[4] által meghatározott eseményeket követően frissül
50.		K03.009_O.3.9.3	a belső vagy külső biztonsági eseményekből vagy jogsértésekből levont tanulságok beépítésre kerülnek a szerepkör alapú biztonsági képzésbe

51.	3.13. A biztonsági képzésre vonatkozó dokumentációk	K03.013_P[1]	meghatározott az egyéni képzési dokumentumok megőrzésének időtartama
52.		K03.013_O.3.13.1.(a)	az információbiztonsági képzési tevékenységek, beleértve a biztonsági tudatosságra vonatkozó képzéseket és a konkrét szerepkörökön alapuló biztonsági képzéseket dokumentálták
53.		K03.013_O.3.13.1.(b)	az információbiztonsági képzési tevékenységeket, beleértve a biztonsági tudatosságra vonatkozó képzéseket és a konkrét szerepkörökön alapuló biztonsági képzéseket nyomon követik
54.		K03.013_O.3.13.2	az egyéni képzésről készült dokumentumokat a K03.013_P[1] által meghatározott időtartamig megőrzik

4. Naplózás és elszámoltathatóság

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi intézkedés**
2.	4.1. Szabályzat és eljárásrendek	K04.001_P[1]	meghatározottak azok a személyek vagy szerepkörök, akikkel a naplózásra és elszámoltathatóságra vonatkozó szabályzatot meg kell ismertetni
3.		K04.001_P[2]	meghatározottak azok a személyek vagy szerepkörök, akikkel a naplózási és elszámoltathatósági eljárásokat meg kell ismertetni
4.		K04.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K04.001_P[4]	a naplózásra és elszámoltathatóságra vonatkozó szabályzat és eljárások irányítására egy meghatározott személy kijelölésre került
6.		K04.001_P[5]	a naplózási és elszámoltathatósági szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K04.001_P[6]	meghatározták azokat az eseményeket, amelyek a naplózási és elszámoltathatósági szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K04.001_P[7]	meghatározták a naplózási és elszámoltathatósági eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K04.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a naplózási és elszámoltathatósági eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K04.001_O_4.1.1.(a)	naplózási és elszámoltathatósági szabályzatot dolgoztak ki és dokumentáltak
11.		K04.001_O_4.1.1.(b)	a naplózási és elszámoltathatósági szabályzatot megismertetették a K04.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K04.001_O_4.1.1.(c)	a naplózási és elszámoltathatósági szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő naplózási és elszámoltathatósági eljárások kidolgozásra és dokumentálásra kerültek

13.		K04.001_O_4.1.1.(d)	a naplózási és elszámoltathatósági eljárásokat megismertették a K04.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K04.001_O_4.1.2	a K04.001_P[4] által meghatározott személy a naplózási és elszámoltathatósági szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányítását ellátja
15.		K04.001_O_4.1.3.(a)	a naplózási és elszámoltathatósági szabályzatot felülvizsgálják és frissítik a K04.001_P[5] által meghatározott gyakorisággal
16.		K04.001_O_4.1.3.(b)	a naplózási és elszámoltathatósági szabályzatot felülvizsgálják és frissítik a K04.001_P[6] által meghatározott eseményeket követően
17.		K04.001_O_4.1.3.(c)	a naplózási és elszámoltathatósági eljárásokat felülvizsgálják és frissítik a K04.001_P[7] által meghatározott gyakorisággal
18.		K04.001_O_4.1.3.(d)	a naplózási és elszámoltathatósági eljárásokat felülvizsgálják és frissítik a K04.001_P[8] által meghatározott eseményeket követően
19.		K04.001_O_4.1.1.1.1.(a)	a naplózási és elszámoltathatósági szabályzat célja meghatározásra került a K04.001_P[3] által meghatározottak szerint
20.		K04.001_O_4.1.1.1.1.(b)	a naplózási és elszámoltathatósági szabályzat hatóköre meghatározásra került a K04.001_P[3] által meghatározottak szerint
21.		K04.001_O_4.1.1.1.1.(c)	a naplózási és elszámoltathatósági szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K04.001_P[3] által meghatározottak szerint
22.		K04.001_O_4.1.1.1.1.(d)	a naplózási és elszámoltathatósági szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K04.001_P[03] által meghatározottak szerint
23.		K04.001_O_4.1.1.1.1.(e)	a naplózási és elszámoltathatósági szabályzathoz kapcsolódó vezetői elkötelezettség meghatározásra kerültek a K04.001_P[3] által meghatározottak szerint
24.		K04.001_O_4.1.1.1.1.(f)	a naplózási és elszámoltathatósági szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K04.001_P[3] által meghatározottak szerint
25.		K04.001_O_4.1.1.1.1.(g)	a naplózási és elszámoltathatósági szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K04.001_P[3] által meghatározottak szerint
26.		K04.001_O_4.1.1.1.2.	a K04.001_P[3] által meghatározott naplózási és elszámoltathatósági szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal
27.	4.2. Naplózható események	K04.002_P[1]	meghatározásra kerültek azok az eseménytípusok, amelyek az EIR-ek által általánosságban naplózandóak
28.		K04.002_P[2]	az EIR-en belül naplózandó eseménytípusok a K04.002_P[1]-ben meghatározott események közül meghatározásra kerültek

29.		K04.002_P[3]	az egyes meghatározott eseménytípusok elvárt naplózási gyakorisága, illetve az azt szükségessé tevő események meghatározásra kerültek
30.		K04.002_P[4]	a naplózásra kiválasztott eseménytípusok felülvizsgálatának és frissítésének gyakorisága meghatározott
31.		K04.002_O.4.2.1	a K04.002_P[2] által meghatározott eseménytípusok naplózására az EIR-ek felkészítése megtörtént
32.		K04.002_O.4.2.2	az eseménynaplózási elvárásokat összehangolják más, a naplózási információkat igénylő szervezeti egységekkel
33.		K04.002_O.4.2.3.(a)	a K04.002_P[2] által meghatározott rendszeren belüli eseménytípusok – azaz a K04.002_P[1] alcsoportja – naplózása megtörténik
34.		K04.002_O.4.2.3.(b)	a K04.002_P[2] által meghatározott rendszeren belüli eseménytípusok naplózásra kerülnek a K04.002_P[3] szerint
35.		K04.002_O.4.2.4	a naplózásra kiválasztott eseménytípusok a biztonsági események utólagos kivizsgálásának támogatására való alkalmassága indoklással ellátott
36.		K04.002_O.4.2.5	a naplózásra kiválasztott eseménytípusok felülvizsgálata és frissítése a K04.002_P[4] által meghatározott gyakorisággal megtörténik
37.	4.3. Naplóbejegyzések tartalma	K04.003_O.4.3.1	a naplóbejegyzések tartalmazzák azokat az információkat, amelyekből megállapítható, hogy milyen típusú esemény történt
38.		K04.003_O.4.3.2	a naplóbejegyzések tartalmazzák azokat az információkat, amelyekből megállapítható, hogy mikor történt az esemény
39.		K04.003_O.4.3.3	a naplóbejegyzések tartalmazzák azokat az információkat, amelyekből megállapítható, hogy hol történt az esemény
40.		K04.003_O.4.3.4	a naplóbejegyzések olyan információkat tartalmaznak, amelyekből megállapítható az esemény forrása
41.		K04.003_O.4.3.5	a naplóbejegyzések olyan információkat tartalmaznak, amelyekből megállapítható az esemény kimenetele
42.		K04.003_O.4.3.6	a naplóbejegyzések olyan információkat tartalmaznak, amelyekből megállapíthatóak az eseményhez kapcsolódó személyek, alanyok, illetve tárgyak vagy objektumok
43.	4.4. Naplóbejegyzések tartalma – Kiegészítő naplóinformációk	K04.004_P[1]	a naplóbejegyzésekben feltüntetendő további információk meghatározásra kerültek
44.		K04.004_O.4.4	a naplóbejegyzések a K04.004_P[1] által meghatározott kiegészítő információkat tartalmazzák
45.	4.5. Naplózás tárkapacitása	K04.005_P[1]	a naplóbejegyzések megőrzési követelményei meghatározásra kerülnek
46.		K04.005_O.4.5	a K04.005_P[1] által meghatározott megőrzési követelményeknek megfelelő tárkapacitás biztosított
47.	4.7. Naplózási hiba kezelése	K04.007_P[1]	a naplózási folyamat hibajelzéseit fogadó személyek vagy szerepkörök meghatározásra kerültek
48.		K04.007_P[2]	a naplózási folyamat hibajelzései kapcsán előírt értesítési idő meghatározásra került
49.		K04.007_P[3]	az audit naplózási folyamat hibája esetén további végrehajtandó intézkedések meghatározásra kerültek

50.		K04.007_O.4.7.1	a K04.007_P[1] által meghatározott személyek vagy szerepkörök riasztást kapnak, ha a K04.007_P[2] által meghatározott időtartamot követően, ha a naplózási folyamat meghibásodik
51.		K04.007_O.4.7.2	a 04.007_P[3] által meghatározott további intézkedések végrehajtása megtörténik a naplózási folyamat hibája esetén
52.	4.8. Naplózási hiba kezelése – Tárhelykapacitás figyelmeztetés	K04.008_P[1]	meghatározásra kerültek azon személyek, szerepkörök, illetve helyszínek, akiket figyelmeztetni kell, ha a kiosztott naplózási tárhely eléri a tárhely maximális naplótárolási kapacitásának bizonyos százalékát
53.		K04.008_P[2]	meghatározott az az időtartam, amelyet követően a K04.008_P[1] szerinti entitások értesítése meg kell, hogy történjen
54.		K04.008_P[3]	a naplózási tárhely maximális tárhely kapacitásának százalékos értéke meghatározásra került
55.		K04.008_O.4.8	a K04.008_P[1] által meghatározott személyek, szerepkörök, illetve helyszínek figyelmeztetést kapnak a K04.008_P[2] által meghatározott időn belül, amikor a kiosztott naplózási tárhely kapacitása eléri a K04.008_P[3] által meghatározott százalékos értéket
56.	4.9. Naplózási hiba kezelése – Valós idejű riasztások	K04.009_P[1]	a K04.009_P[3] által meghatározott audit hibaesemények bekövetkezésekor valós idejű riasztási idő meghatározásra került
57.		K04.009_P[2]	a K04.009_P[3] által meghatározott audit hibaesemények bekövetkezésekor valós időben riasztandó személyek, szerepkörök, illetve helyszínek meghatározásra kerültek
58.		K04.009_P[3]	a valós idejű riasztást igénylő auditnaplózási hibaesemények meghatározásra kerültek
59.		K04.009_O.4.9	az EIR a K04.009_P[1] által meghatározott valós idejű riasztási időn belül riasztást küld a K04.009_P[2] által meghatározott személyeknek, szerepköröknek, illetve helyszíneknek, amikor a K04.009_P[3] által meghatározott valós idejű riasztást igénylő auditnaplózási hibaesemények következnek be
60.	4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel	K04.013_P[1]	meghatározásra került a rendszer naplóbejegyzései felülvizsgálatának és elemzésének gyakorisága
61.		K04.013_P[2]	a nem megfelelő vagy szokatlan tevékenység meghatározásra került
62.		K04.013_P[3]	meghatározásra kerültek azon személyek vagy szerepkörök, amelyek felé a rendszer naplóbejegyzéseinek felülvizsgálatából és elemzéséből származó megállapítások, jelentések megküldésre kerülnek
63.		K04.013_O.4.13.1	a rendszer naplóbejegyzéseit felülvizsgálják és elemzik a K04.013_P[1] által meghatározott gyakorisággal a K04.013_P[2]-ben meghatározott tevékenységre utaló jelek és e tevékenységek lehetséges hatásai szempontjából
64.		K04.013_O.4.13.2	a felülvizsgálat megállapításait a K04.013_P[3] által meghatározott személyeknek vagy szerepköröknek jelentik
65.		K04.013_O.4.13.3	az audit naplóbejegyzések felülvizsgálatának, elemzésének és jelentésének szintjét a rendszeren belül kiigazítják, ha a bűnüldözési információk, hírszerzési információk vagy más hiteles információforrások alapján változás áll be a kockázatban

66.	4.14. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Automatizált folyamatintegráció	K04.014_P[1]	a naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak integrálására használt automatizált mechanizmusok meghatározásra kerültek
67.		K04.014_O.4.14	a naplóbejegyzések felülvizsgálata, elemzése és a jelentéstételi folyamatai a K04.014_P[1] által meghatározott automatizált mechanizmusok segítségével történnek
68.	4.15. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Naplózási tárhelyek összekapcsolása	K04.015_O.4.15	a különböző tárhelyeken található naplóbejegyzések elemzése és korrelálása megtörtént az egész szervezetre kiterjedő helyzetfelismerés érdekében
69.	4.17. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Felügyeleti képességek integrálása	K04.017_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {sérülékenységvizsgálat során keletkezett információk, teljesítményadatok; rendszerfelügyeleti információk, a K04.017_P[2] által meghatározott egyéb forrásokból begyűjtött adatok/információk}
70.		K04.017_P[2]	az egyéb forrásokból begyűjtött, elemezendő adatok, illetve információk meghatározásra kerültek
71.		K04.017_O.4.17	a naplóbejegyzések elemzése integrálódik a K04.017_P[1] által meghatározott értékek elemzése céljából
72.	4.18. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Összevetés a fizikai felügyelettel	K04.018_O.4.18	a naplóbejegyzésekből származó információk összevetésre kerülnek a fizikai hozzáférés ellenőrzéséből származó információkkal
73.	4.22. Naplóbejegyzések csökkentése és jelentéskészítés	K04.022_O.4.22.1	a szervezet olyan naplóbejegyzés csökkentési és jelentéskészítési képességet alkalmaz, amely támogatja a naplóbejegyzések igény szerinti felülvizsgálatát, elemzését és a jelentéstételi követelményeket, valamint a biztonsági események utólagos kivizsgálását
74.		K04.022_O.4.22.2	a szervezet olyan naplóbejegyzés csökkentési és jelentéskészítési lehetőséget alkalmaz, amely nem változtatja meg a naplóbejegyzések eredeti tartalmát vagy időbeli sorrendjét
75.	4.23. Naplóbejegyzések csökkentése és jelentéskészítés – Automatikus feldolgozás	K04.023_P[1]	meghatározottak a naplóbejegyzéseken belüli, feldolgozható, rendezhető vagy kereshető mezők
76.		K04.023_O.4.23.1.(a)	a K04.023_P[1] által meghatározott adatmezők feldolgozhatósága biztosított
77.		K04.023_O.4.23.1.(b)	a K04.023_P[1] által meghatározott adatmezők rendezhetősége biztosított
78.		K04.023_O.4.23.1.(c)	a K04.023_P[1] által meghatározott adatmezők kereshetősége biztosított
79.	4.24. Időbélyegek	K04.024_P[1]	meghatározott a naplóbejegyzések esetében alkalmazandó időbélyegek elvárt pontossága
80.		K04.024_O.4.24.1	a naplóbejegyzések időbélyegzőinek létrehozására belső rendszerórák szolgálnak
81.		K04.024_O.4.24.2	a K04.024_P[1] által meghatározott időmérési pontosságnak megfelelő, a koordinált világidőhöz képest helyi időeltolódást az időbélyeg részeként tartalmazó időbélyegekkel keletkeznek a naplóbejegyzések
82.	4.25. Naplóinformációk védelme	K04.025_P[1]	a naplóbejegyzések jogosulatlan hozzáférésének, módosításának vagy törlésének észlelésekor riasztandó személyek vagy szerepkörök meghatározásra kerültek

83.		K04.025_O.4.25.1	a naplóbejegyzések és a naplókezelő eszközök védettek a jogosulatlan hozzáféréstől, módosítástól és törléstől
84.		K04.025_O.4.25.2	a K04.025_P[1] által meghatározott személyek vagy szerepkörök riasztást kapnak az naplózási információk jogosulatlan hozzáférésének, módosításának vagy törlésének észlelésekor
85.	4.27. A naplóinformációk védelme – Tárolás fizikailag különálló rendszereken vagy rendszerelemeken	K04.027_P[1]	a naplóbejegyzések olyan tárhelyen történő tárolásának gyakorisága meghatározott, amely a naplóbejegyzés keletkezési helyétől fizikailag elkülönült rendszer vagy rendszerelem része
86.		K04.027_O.4.27	a K04.027_P[1] által meghatározott gyakoriságú naplóbejegyzéseket olyan adattárban tárolják, amely az ellenőrzött rendszertől vagy rendszerelemtől fizikailag eltérő rendszer vagy rendszerelem része
87.	4.28. A naplóinformációk védelme – Kriptográfiai védelem	K04.028_O.4.28	a naplóbejegyzések és a naplókezelő eszközök integritásának védelmét szolgáló kriptográfiai mechanizmusok bevezetésre kerültek
88.	4.29. A naplóinformációk védelme – Privilegizált felhasználók hozzáférése	K04.029_P[1]	meghatározásra került a privilegizált felhasználók vagy szerepkörök azon részhalmaza, amelyek jogosultak hozzáférni a naplózási funkciók kezeléséhez
89.		K04.029_O.4.29	a naplózási funkciók kezelése csak a K04.029_P[1] által meghatározott privilegizált felhasználók vagy szerepkörök alcsoportja számára engedélyezett
90.	4.33. Letagadhatatlanság	K04.033_P[1]	a letagadhatatlanság követelménye alá tartozó tevékenységek meghatározásra kerülnek
91.		K04.033_O.4.33	a szervezet megcáfolhatatlan bizonyítékot szolgáltat arra, ha egy személy (vagy egy személy nevében eljáró folyamat) a K04.033_P[1] által meghatározott tevékenységeket hajtott végre
92.	4.38. A naplóbejegyzések megőrzése	K04.038_P[1]	meghatározzák a naplóbejegyzések megőrzésének időtartamát, amely összhangban van a jogszabályi és a szervezeten belüli információmegőrzési követelményekkel
93.		K04.038_O.4.38	a naplóbejegyzéseket a K04.038_P[1] által meghatározott időtartamig megőrzik
94.	4.40. Naplóbejegyzések létrehozása	K04.040_P[1]	biztosítottak olyan rendszerkomponensek, amelyek az eseménytípusokra vonatkozó naplóbejegyzések létrehozására alkalmasak a K04.002_P[1] által meghatározottak szerint
95.		K04.040_P[2]	a rendszer komponensei által naplózandó eseménytípusok kiválasztására jogosult személyek vagy szerepkörök meghatározásra kerültek
96.		K04.040_O.4.40.1	a K04.002_P[1] által meghatározott, a rendszer által naplózható események esetén a K04.040_P[1] által meghatározott rendszerkomponensek naplóbejegyzés generálási képességet biztosítanak
97.		K04.040_O.4.40.2	a K04.040_P[2] által meghatározott személyek vagy a szerepkörök kiválaszthatják azokat az eseménytípusokat, amelyeket a rendszer egyes összetevői naplóznak
98.		K04.040_O.4.40.3	a K04.002_P[1] által meghatározott eseményekre vonatkozó, a 4.3. Naplóbejegyzések tartalma pontban meghatározott naplóbejegyzések keletkeznek

99.	4.41. Naplóbejegyzések létrehozása – Az egész rendszerre kiterjedő és időbeli naplózási nyomvonal	K04.041_P[1]	meghatározottak azok a rendszerelemek, amelyekből a naplóbejegyzéseket, melyekből rendszerszintű naplót kell elállítani
100.		K04.041_P[2]	a rendszerszintű naplóegyes bejegyzéseinek időbélyegei közötti kapcsolatra vonatkozó tűrésszintet meghatározott
101.		K04.041_O.4.41	a K04.041_P[1] által meghatározott rendszerelemekből származó naplóbejegyzéseket az egész rendszerre kiterjedően állítják össze, amelyek a K04.041_P[2] által meghatározott tűréshatáron belül időben összekapcsoltak
102.	4.43. Naplóbejegyzések létrehozása – Felhatalmazott személyek változtatásai	K04.043_P[1]	a rendszerelemek naplózásának módosítására jogosult személyek vagy szerepkörök meghatározásra kerültek
103.		K04.043_P[2]	meghatározták azokat a rendszerelemeket, amelyeken naplózást kell végezni
104.		K04.043_P[3]	meghatározottak azok a választható eseménykritériumok, amelyekkel a változásnaplózást végre kell hajtani
105.		K04.043_P[4]	meghatározottak azok az időbeli küszöbértékek, amelyeken belül a naplózási műveleteket meg kell változtatni
106.		K04.043_O.4.43	a K04.043_P[1] által meghatározott személyek vagy szerepkörök számára biztosított a K04.043_P[2] által meghatározott rendszerelemeken a K04.043_P[3] által meghatározott választható eseménykritériumok alapján a K04.043_P[4] által meghatározott időtartamon belül végrehajtandó naplózás megváltoztatásának lehetősége

5. Értékelés, engedélyezés és monitorozás

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	5.1. Szabályzat és eljárásrendek	K05.001_P[1]	meghatározásra kerültek azok a személyek vagy szerepkörök, akikkel a naplózásra és elszámoltathatóságra vonatkozó szabályzatot meg kell ismertetni
3.		K05.001_P[2]	meghatározásra kerültek azok a személyek vagy szerepkörök, akikkel a naplózási és elszámoltathatósági eljárásokat meg kell ismertetni
4.		K05.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K05.001_P[4]	kijelölésre került az értékelésre, engedélyezésre és monitorozásra vonatkozó szabályzat és eljárások irányítására egy meghatározott személy
6.		K05.001_P[5]	az értékelési, engedélyezési és monitorozási szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K05.001_P[6]	meghatározottak azok az események, amelyek az értékelési, engedélyezési és monitorozási szabályzat felülvizsgálatát és aktualizálását teszik szükségessé

8.		K05.001_P[7]	meghatározottak az értékelési, engedélyezési és monitorozási eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K05.001_P[8]	meghatározottak azok az események, amelyek miatt az értékelési, engedélyezési és monitorozási eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K05.001_O.5.1.1.(a)	értékelési, engedélyezési és monitorozási szabályzatot dolgoztak ki és dokumentáltak
11.		K05.001_O.5.1.1.(b)	az értékelési, engedélyezési és monitorozási szabályzat megismertetésre került a K05.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K05.001_O.5.1.1.(c)	az értékelési, engedélyezési és monitorozási szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő értékelési, engedélyezési és monitorozási eljárások kidolgozásra és dokumentálásra kerültek
13.		K05.001_O.5.1.1.(d)	az értékelési, engedélyezési és monitorozási eljárások megismertetésre kerültek a K05.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K05.001_O.5.1.2	a K05.001_P[4] által meghatározott személy kijelölése megtörtént
15.		K05.001_O.5.1.3.(a)	az értékelési, engedélyezési és monitorozási szabályzatot felülvizsgálják és frissítik a K05.001_P[5] által meghatározott gyakorisággal
16.		K05.001_O.5.1.3.(b)	az értékelési, engedélyezési és monitorozási szabályzatot felülvizsgálják és frissítik a K05.001_P[6] által meghatározott eseményeket követően
17.		K05.001_O.5.1.3.(c)	az értékelési, engedélyezési és monitorozási eljárásokat felülvizsgálják és frissítik a K05.001_P[7] által meghatározott gyakorisággal
18.		K05.001_O.5.1.3.(d)	az értékelési, engedélyezési és monitorozási eljárásokat felülvizsgálják és frissítik a K05.001_P[8] által meghatározott eseményeket követően
19.		K05.001_O.5.1.1.1.1.(a)	az értékelési, engedélyezési és monitorozási szabályzat célja meghatározásra került a K05.001_P[3] által meghatározottak szerint
20.		K05.001_O.5.1.1.1.1.(b)	az értékelési, engedélyezési és monitorozási szabályzat hatálya meghatározásra került a K05.001_P[3] által meghatározottak szerint
21.		K05.001_O.5.1.1.1.1.(c)	az értékelési, engedélyezési és monitorozási szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K05.001_P[3] által meghatározottak szerint
22.		K05.001_O.5.1.1.1.1.(d)	az értékelési, engedélyezési és monitorozási szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K05.001_P[3] által meghatározottak szerint
23.		K05.001_O.5.1.1.1.1.(e)	az értékelési, engedélyezési és monitorozási szabályzat céljával kapcsolatos vezetői elkötelezettség rögzítésre került a K05.001_P[3] által meghatározottak szerint

24.		K05.001_O.5.1.1.1.1.(f)	az értékelési, engedélyezési és monitorozási szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K05.001_P[3] által meghatározottak szerint
25.		K05.001_O.5.1.1.1.1.(g)	az értékelési, engedélyezési és monitorozási szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K05.001_P[3] által meghatározottak szerint
26.		K05.001_O.5.1.1.1.2	a K05.001_P[3] által meghatározott értékelési, engedélyezési és monitorozási szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal
27.	5.2. Biztonsági értékelések	K05.002_P[1]	meghatározott, hogy milyen gyakorisággal kell értékelni a rendszerben és annak működési környezetében lévő intézkedéseket
28.		K05.002_P[2]	meghatározásra kerültek azok a személyek vagy szerepkörök, akiknek a biztonsági értékelés eredményeit át kell adni
29.		K05.002_O.5.2.1	a szervezet az elvégzendő értékelés típusának megfelelő értékelőt vagy értékelőcsoportot választott ki
30.		K05.002_O.5.2.2.1	kidolgozásra került egy biztonságértékelési terv, amely leírja az értékelés hatókörét, az értékelendő védelmi intézkedéseket, azok kiterjesztését és továbbfejlesztését
31.		K05.002_O.5.2.2.2	kidolgozásra került egy biztonságértékelési terv, amely leírja az értékelés hatókörét, beleértve az intézkedés hatékonyságának meghatározásához használandó értékelési eljárásokat
32.		K05.002_O.5.2.2.3.(a)	kidolgozásra került egy biztonságértékelési terv, amely leírja az értékelés hatókörét, beleértve az értékelési környezetet is
33.		K05.002_O.5.2.2.3.(b)	kidolgozásra került egy biztonságértékelési terv, amely leírja az értékelés terjedelmét, valamint az értékelő csoportot is
34.		K05.002_O.5.2.2.3.(c)	kidolgozásra került egy biztonságértékelési terv, amely leírja az értékelés hatókörét, beleértve az értékelési szerepeket és felelősségi köröket
35.		K05.002_O.5.2.3	a biztonságértékelési tervet az engedélyezésre jogosult tisztviselő vagy kijelölt képviselője az értékelés elvégzése előtt felülvizsgálta és jóváhagyta
36.		K05.002_O.5.2.4	az intézkedéseket a rendszerben és annak működési környezetében a K05.002_P[1] által meghatározott értékelési gyakorisággal értékelik annak megállapítása érdekében, hogy az intézkedések milyen mértékben, illetve helyesen vannak-e végrehajtva, rendeltetésszerűen működnek-e, és a kívánt eredményt hozzák-e a megállapított biztonsági követelmények teljesítése tekintetében
37.		K05.002_O.5.2.5	biztonságértékelési jelentés készült, amely dokumentálja az értékelés eredményeit
38.		K05.002_O.5.2.6	a biztonságértékelés eredményeit a K05.002_P[2] által meghatározott személyek vagy szerepkörök rendelkezésére bocsátották

39.	5.3. Biztonsági értékelések – Független értékelők	K05.003_O.5.3	a szervezet független értékelőket vagy értékelőcsoportokat alkalmaz a biztonsági értékelések elvégzésére [csak az MKr. 1. § (1) bekezdése szerinti szervezetek esetén alkalmazandó]
40.	5.4. Biztonsági értékelések – Kiberbiztonsági audit	K05.004_O.5.4	a szervezet a kiberbiztonsági auditot a jogszabályban meghatározottak szerint lefolytatja
41.	5.5. Biztonsági értékelések – Speciális értékelések	K05.005_P[1]	meghatározzák azt a gyakoriságot, amellyel a szervezet speciális biztonsági értékelésére speciális vizsgálatot végez
42.		K05.005_P[2]	a következő PARAMÉTER-ÉRTÉKEK egyike került kiválasztásra: {bejelentett; be nem jelentett}
43.		K05.005_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {mélységi monitorozás; biztonsági berendezések; automatizált biztonsági tesztek; sérülékenységszkennelés; rosszindulatú felhasználók tesztelése; belső fenyegetések értékelése; teljesítmény- és terhelésvizsgálat; adatszivárgás vagy adatvesztés értékelése; a K05.005_P[4] által meghatározott egyéb értékelési formák}
44.		K05.005_P[4]	egyéb értékelési formák meghatározásra kerültek
45.		K05.005_O.5.5.1	a K05.005_P[1] által meghatározott gyakorisággal a K05.005_P[2] és a K05.005_P[3] által meghatározottak szerinti értékelések biztonsági értékelések részeként lefolytatásra kerültek
46.	5.7. Információcsere	K05.007_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra:{összekapcsolási biztonsági megállapodások; információcsere-biztonsági megállapodások; egyetértési vagy megállapodási memorandumok; szolgáltatási szintű megállapodások; felhasználói megállapodások; titoktartási megállapodások; a K05.007_P[2] által meghatározott megállapodások}
47.		K05.007_P[2]	az információcsere jóváhagyására és kezelésére használt megállapodás típusa meghatározott
48.		K05.007_P[3]	meghatározott a megállapodások felülvizsgálatának és frissítésének gyakorisága
49.		K05.007_O.5.7.1	a K05.007_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK használatával jóváhagyják és kezelik a rendszer és más rendszerek közötti információcserét
50.		K05.007_O.5.7.2.(a)	az interfész jellemzőit az információcsere-megállapodás részeként dokumentálják
51.		K05.007_O.5.7.2.(b)	a biztonsági követelményeket az információcsere-megállapodás részeként dokumentálják
52.		K05.007_O.5.7.2.(c)	az intézkedéseket az információcsere-megállapodás részeként dokumentálják
53.		K05.007_O.5.7.2.(d)	az egyes rendszerekre vonatkozó felelősségi köröket az információcsere-megállapodás részeként dokumentálják
54.		K05.007_O.5.7.2.(e)	a közölt információk hatásszintjét az információcsere-megállapodás részeként dokumentálják
55.		K05.007_O.5.7.3	a megállapodásokat felülvizsgálják és frissítik a K05.007_P[3] által meghatározott gyakorisággal
56.	5.8. Információcsere – Átviteli engedélyek	K05.008_O.5.8	az összekapcsolt rendszerek között adatokat továbbító személyek vagy rendszerek rendelkeznek a szükséges jogosultságokkal (pl. írási engedélyek vagy jogosultságok) az adatok átvétele előtt

57.	5.10. Az intézkedési terv és mérföldkövei	K05.010_P[1]	meghatározott, hogy milyen gyakorisággal kell frissíteni a meglévő intézkedési tervet és a mérföldköveket a biztonsági értékelések, a független auditok vagy felülvizsgálatok és a folyamatos felügyeleti tevékenységek megállapításai alapján
58.		K05.010_O.5.10.1	az EIR-re vonatkozóan intézkedési tervet és mérföldköveket dolgoztak ki, hogy dokumentálják a szervezet tervezett korrekciós intézkedéseit a védelmi intézkedések értékelése során feltárt gyengeségek vagy hiányosságok kijavítása, valamint a rendszer ismert sérülékenységeinek csökkentése vagy megszüntetése érdekében
59.		K05.010_O.5.10.2	a meglévő intézkedési tervet és a mérföldköveket a K05.010_P[1] által meghatározott gyakorisággal frissítik a biztonsági értékelések, a független auditok vagy felülvizsgálatok és a folyamatos felügyeleti tevékenységek megállapításai alapján
60.	5.12. Engedélyezés	K05.012_P[1]	az engedélyek frissítésének gyakorisága meghatározásra került
61.		K05.012_O.5.12.1	engedélyezésért felelős személy kijelölése megtörtént
62.		K05.012_O.5.12.2	a közös biztonsági követelményekért felelős személy kijelölése megtörtént
63.		K05.012_O.5.12.3.1	a műveletek megkezdése előtt a rendszer engedélyezésre jogosult tisztviselője elfogadja a másik EIR által áthozott közös biztonsági követelményeket
64.		K05.012_O.5.12.3.2	az EIR használatba vétele előtt a szervezet vezetője engedélyezte a rendszer működését
65.		K05.012_O.5.12.4	a közös biztonsági követelményekért felelős személy engedélyezte a biztonsági követelmények használatát, amelyek más rendszer által biztosítottak
66.		K05.012_O.5.12.5	az engedélyek frissítése a K05.012_P[1] által meghatározott gyakorisággal történik
67.	5.15. Folyamatos felügyelet	K05.015_P[1]	a rendszerszintű metrikák meghatározásra kerültek
68.		K05.015_P[2]	meghatározták azokat a gyakoriságokat, amelyekkel a felügyelet hatékonyságát nyomon kell követni
69.		K05.015_P[3]	meghatározták, hogy milyen gyakorisággal kell a védelmi intézkedések hatékonyságát értékelni
70.		K05.015_P[4]	meghatározták azokat a személyeket vagy szerepköröket, akiknek a rendszer biztonsági állapotáról jelentést kell tenni
71.		K05.015_P[5]	a rendszer biztonsági állapotának jelentési gyakorisága meghatározásra került
72.		K05.015_O.5.15.(a)	rendszerszintű folyamatos felügyeleti stratégiát dolgoztak ki
73.		K05.015_O.5.15.(b)	a szervezet a rendszerszintű folyamatos felügyeletet a szervezeti szintű folyamatos felügyeleti stratégiával összhangban hajtja végre
74.		K05.015_O.5.15.1	a rendszerszintű folyamatos felügyelet magában foglalja a K05.015_P[1] által meghatározott rendszerszintű mérőszámokat

75.		K05.015_O.5.15.2.(a)	a rendszerszintű folyamatos felügyelet magában foglalja a K05.015_P[2] által meghatározott ellenőrzési gyakoriságot
76.		K05.015_O.5.15.2.(b)	a rendszerszintű folyamatos felügyelet magában foglalja a K05.015_P[3] által meghatározott gyakoriságokat a védelmi intézkedések hatékonyságának értékelésére
77.		K05.015_O.5.15.3	a rendszerszintű folyamatos felügyelet magában foglalja a folyamatos felügyeleti stratégiával összhangban lévő védelmi intézkedések folyamatos értékelését
78.		K05.015_O.5.15.4	a rendszerszintű folyamatos felügyelet magában foglalja a rendszer és a szervezet által meghatározott mutatók folyamatos felügyeletét a folyamatos felügyeleti stratégiával összhangban
79.		K05.015_O.5.15.5	a rendszerszintű folyamatos felügyelet magában foglalja a védelmi intézkedések és a felügyelet által generált információk összegzését és elemzését
80.		K05.015_O.5.15.6	a rendszerszintű folyamatos felügyelet magában foglalja a védelmi intézkedések és a felügyeleti információk elemzésének eredményeire adott válaszintézkedéseket
81.		K05.015_O.5.15.7	a rendszerszintű folyamatos felügyelet magában foglalja a rendszer biztonsági állapotának jelentését a K05.015_P[4] által meghatározott személyeknek vagy szerepköröknek a K05.015_P[5] által meghatározott gyakorisággal
82.	5.16. Folyamatos felügyelet – Független értékelés	K05.016_O.5.16	független értékelőket vagy értékelőcsoportokat alkalmaznak a rendszerben lévő védelmi intézkedések folyamatos ellenőrzésére
83.	5.18. Folyamatos felügyelet – Kockázatmonitorozás	K05.018_O.5.18	a kockázatmonitorozás a folyamatos felügyeleti stratégia szerves részét képezi
84.		K05.018_O.5.18.1	a hatékonyság nyomonkövetése a kockázatmonitorozás részét képezi
85.		K05.018_O.5.18.2	a megfelelőség nyomonkövetése a kockázatmonitorozás részét képezi
86.		K05.018_O.5.18.3	a változáskövetés a kockázatmonitorozás részét képezi
87.	5.22. Behatolásvizsgálat – Független szakértő vagy csapat	K05.022_O.5.22	független szakértőt vagy szakértői csapatot alkalmaznak a rendszer vagy a rendszerelemek behatolásvizsgálatának elvégzésére
88.	5.25. Belső rendszerkapcsolatok	K05.025_P[1]	a belső rendszerkapcsolatokat igénylő rendszerelemeket vagy rendszerelem kategóriákat meghatározottak
89.		K05.025_P[2]	a belső rendszerkapcsolatok megszüntetését eredményező feltételek meghatározottak
90.		K05.025_P[3]	meghatározták, hogy milyen gyakorisággal kell felülvizsgálni az egyes belső rendszerkapcsolatok további szükségességét
91.		K05.025_O.5.25.1	a K05.025_P[1] által meghatározott rendszerelemek belső csatlakoztatása engedélyezett
92.		K05.025_O.5.25.2.(a)	minden egyes belső kapcsolat esetében az interfész jellemzői dokumentáltak

93.		K05.025_O.5.25.2.(b)	minden egyes belső kapcsolatra vonatkozóan dokumentálják a biztonsági követelményeket
94.		K05.025_O.5.25.2.(c)	minden egyes belső kapcsolat esetében dokumentálják a közölt információ jellegét
95.		K05.025_O.5.25.3	a belső rendszerkapcsolatok a K05.025_P[2] által meghatározott feltételek teljesülése után megszűnnek, megszüntetésre kerültek
96.		K05.025_O.5.25.4	az egyes belső kapcsolatok szükségessége a K05.025_P[3] által meghatározott gyakorisággal felülvizsgálatra kerül

6. Konfigurációkezelés

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi intézkedés**
2.	6.1. Szabályzat és eljárásrendek	K06.001_P[1]	meghatározottak azon személyek vagy szerepkörök, akikkel a konfigurációkezelésre vonatkozó szabályzatot meg kell ismertetni
3.		K06.001_P[2]	meghatározottak azon személyek vagy szerepkörök, akikkel a konfigurációkezelési eljárásokat meg kell ismertetni
4.		K06.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K06.001_P[4]	megtörtént a konfigurációkezelésre vonatkozó szabályzatok és eljárások életciklusának irányításáért felelős személy kijelölése
6.		K06.001_P[5]	a konfigurációkezelési szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K06.001_P[6]	meghatározták azokat az eseményeket, amelyek a konfigurációkezelési szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K06.001_P[7]	meghatározták a konfigurációkezelési eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K06.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a konfigurációkezelési eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K06.001_O_6.1.1.(a)	konfigurációkezelési szabályzatot dolgoztak ki és dokumentáltak
11.		K06.001_O_6.1.1.(b)	a konfigurációkezelési szabályzatot megismertetésre került a K06.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K06.001_O_6.1.1.(c)	a konfigurációkezelési szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő konfigurációkezelési eljárások kidolgozása és dokumentálása megtörtént

13.		K06.001_O_6.1.1.(d)	a konfigurációkezelési eljárások megismertetése a K06.001_P[2] által meghatározott személyekkel vagy szerepkörökkel megtörtént
14.		K06.001_O_6.1.2	a K06.001_P[4] által meghatározott személy kijelölése megtörtént
15.		K06.001_O_6.1.3.(a)	a konfigurációkezelési szabályzatot felülvizsgálják és frissítik a K06.001_P[5] által meghatározott gyakorisággal
16.		K06.001_O_6.1.3.(b)	a konfigurációkezelési szabályzatot felülvizsgálják és frissítik a K06.001_P[6] által meghatározott eseményeket követően
17.		K06.001_O_6.1.3.(c)	a konfigurációkezelési eljárásokat felülvizsgálják és frissítik a K06.001_P[7] által meghatározott gyakorisággal
18.		K06.001_O_6.1.3.(d)	a konfigurációkezelési eljárásokat felülvizsgálják és frissítik a K06.001_P[8] által meghatározott eseményeket követően
19.		K06.001_O_6.1.1.1.1.(a)	a konfigurációkezelési szabályzat céljának meghatározása a K06.001_P[3] által meghatározottak szerint megtörtént
20.		K06.001_O_6.1.1.1.1.(b)	a konfigurációkezelési szabályzat hatókörének meghatározása a K06.001_P[3] által meghatározottak szerint megtörtént
21.		K06.001_O_6.1.1.1.1.(c)	a konfigurációkezelési szabályzathoz kapcsolódó szerepkörök meghatározása a K06.001_P[3] által meghatározottak szerint megtörtént
22.		K06.001_O_6.1.1.1.1.(d)	a konfigurációkezelési szabályzathoz kapcsolódó felelősségek meghatározása a K06.001_P[3] által meghatározottak szerint megtörtént
23.		K06.001_O_6.1.1.1.1.(e)	a konfigurációkezelési szabályzathoz kapcsolódó vezetői elkötelezettség rögzítése a K06.001_P[3] által meghatározottak szerint megtörtént
24.		K06.001_O_6.1.1.1.1.(f)	a konfigurációkezelési szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározása a K06.001_P[3] által meghatározottak szerint megtörtént
25.		K06.001_O_6.1.1.1.1.(g)	a konfigurációkezelési szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározása a K06.001_P[3] által meghatározottak szerint megtörtént
26.		K06.001_O_6.1.1.1.2.	a konfigurációkezelési szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal
27.	6.2. Alapkonfiguráció	K06.002_P[1]	meghatározták az alapkonfiguráció felülvizsgálatának és frissítésének gyakoriságát
28.		K06.002_P[2]	az alapkonfiguráció felülvizsgálatát és frissítését igénylő körülmények meghatározása megtörtént
29.		K06.002_O.6.2.1.(a)	az EIR alapkonfigurációját kidolgozták és dokumentálták
30.		K06.002_O.6.2.1.(b)	az EIR alapkonfigurációját a konfiguráció-ellenőrzés keretében karbantartják
31.		K06.002_O.6.2.2.1	a rendszer alapkonfigurációjának felülvizsgálata és frissítése a K06.002_P[1] által meghatározott időközönként megtörténik

32.		K06.002_O.6.2.2.2	a rendszer alapkonfigurációját felülvizsgálják és frissítik, ha az a K06.002_P[2] által meghatározott körülmények miatt szükséges
33.		K06.002_O.6.2.2.3	a rendszer alapkonfigurációját a rendszerelemek telepítésekor vagy frissítésekor felülvizsgálják és frissítik
34.	6.3. Alapkonfiguráció – Automatikus támogatás a pontosság és a napra készség érdekében	K06.003_P[1]	meghatározottak a rendszer alapkonfigurációjának karbantartására szolgáló automatizált mechanizmusok
35.		K06.003_O.6.3.(a)	a rendszer alapkonfigurációjának naprakészsége a K06.003_P[1] által meghatározott automatizált mechanizmusok segítségével biztosított
36.		K06.003_O.6.3.(b)	a rendszer alapkonfigurációjának teljessége a K06.003_P[1] által meghatározott automatizált mechanizmusok segítségével biztosított
37.		K06.003_O.6.3.(c)	a rendszer alapkonfigurációjának pontossága a K06.003_P[1] által meghatározott automatizált mechanizmusok segítségével biztosított
38.		K06.003_O.6.3.(d)	a rendszer alapkonfigurációjának állandó rendelkezésre állása a K06.003_P[1] által meghatározott automatizált mechanizmusok segítségével biztosított
39.	6.4. Alapkonfiguráció – Korábbi konfigurációk megőrzése	K06.004_P[1]	meghatározott a megtartandó korábbi alapkonfigurációs verziók száma
40.		K06.004_O.6.4	a K06.004_P[1] által meghatározott a rendszer korábbi alapkonfigurációs verzió(i) megőrzésre kerültek
41.	6.6. Alapkonfiguráció – Rendszerek és rendszerelemek konfigurálása magas kockázatú területekre	K06.006_P[1]	meghatározták azokat az EIR-eket vagy rendszerelemeket, amelyek a szervezet által jelentős kockázatú helyszíneken használhatóak
42.		K06.006_P[2]	meghatározottak azok a konfigurációs beállítások, amelyeket a szervezet által jelentős kockázatú helyszíneken történő használat esetén szükséges alkalmazni
43.		K06.006_P[3]	meghatározottak a védelmi intézkedések, amelyeket a jelentős kockázatú helyszíneken történő használatot követően szükséges végrehajtani
44.		K06.006_O.6.6.1	jelentős kockázatú helyszíneken történő használatra a K06.006_P[1] által meghatározott és K06.006_P[2] által meghatározott konfigurációs beállításokkal rendelkező EIR-ek vagy rendszerelemek használata engedélyezett
45.		K06.006_O.6.6.2	a K06.006_P[3] által meghatározott védelmi intézkedéseket alkalmaznak az EIR-ekre vagy rendszerelemekre, amikor azok jelentős kockázatú helyszíneken történő használata befejeződik
46.	6.7. A konfigurációváltozások felügyelete (változáskezelés)	K06.007_P[1]	a konfigurációváltozások dokumentumainak megőrzési ideje meghatározott
47.		K06.007_P[2]	a konfigurációváltoztatások koordinációját és felügyeletét ellátó egység meghatározott
48.		K06.007_O.6.7.1.(a)	a rendszer konfigurációvezérelt módosításaihoz kapcsolódó tevékenységek ellenőrzése megvalósul
49.		K06.007_O.6.7.1.(b)	a konfiguráció ellenőrzés hatálya alá eső változtatásokkal kapcsolatos tevékenységek ellenőrzése megtörténik
50.		K06.007_O.6.7.2.(a)	a konfigurációváltozás-ellenőrzési tevékenységeket a K06.007_P[2] által meghatározott egység koordinálja és felügyeli

51.		K06.007_O.6.7.2.(b)	a konfigurációváltoztatások koordinációját és felügyeletét ellátó egység a K06.007_P[1] által meghatározottak szerint végzi tevékenységét
52.	6.8. A konfigurációváltozások felügyelete – Automatizált dokumentáció, értesítés és változtatási tilalom	K06.008_P[1]	a konfigurációváltozás-ellenőrzés automatizálására használt mechanizmusok meghatározottak
53.		K06.008_P[2]	az EIR javasolt változtatásairól értesítendő és azok jóváhagyására jogosult személyek meghatározottak
54.		K06.008_P[3]	meghatározott az az időtartam, amely után a jóvá nem hagyott vagy késedelmesen jóváhagyott változtatásokat eszkalálni szükséges
55.		K06.008_P[4]	a jóváhagyott módosítások végrehajtásáról értesítendő személyek meghatározottak
56.		K06.008_O.6.8.1	a K06.008_P[1] által meghatározott automatizált mechanizmusokat alkalmaznak a rendszer javasolt módosításainak dokumentálására
57.		K06.008_O.6.8.2	a K06.008_P[1] által meghatározott automatizált mechanizmusok segítségével értesítik a K06.008_P[2] által meghatározott jóváhagyásra jogosultakat a rendszer javasolt változtatásairól és kérik a változtatás jóváhagyását
58.		K06.008_O.6.8.3	a K06.008_P[1] által meghatározott automatizált mechanizmusokat alkalmaznak a rendszer javasolt módosításainak kiemelésére, amelyeket a K06.008_P[3] által meghatározott időtartamon belül nem hagytak jóvá vagy késedelmesen hagytak jóvá
59.		K06.008_O.6.8.4	a K06.008_P[1] által meghatározott automatizált mechanizmusok segítségével megakadályozzák a rendszer módosítását a kijelölt jóváhagyások beérkezéséig
60.		K06.008_O.6.8.5	a K06.008_P[1] által meghatározott automatizált mechanizmusokat használnak a rendszer valamennyi változtatásának dokumentálására
61.		K06.008_O.6.8.6	a K06.008_P[1] által meghatározott automatizált mechanizmusok segítségével értesítik a K06.008_P[4] által meghatározott személyeket a rendszer jóváhagyott módosításainak végrehajtásáról
62.	6.9. A konfigurációváltozások felügyelete – Változások tesztelése, jóváhagyása és dokumentálása	K06.009_O.6.9.(a)	az EIR változtatásai a bevezetésük előtt tesztelésre kerültek
63.		K06.009_O.6.9.(b)	az EIR változtatásai a bevezetésük előtt jóváhagyásra kerültek
64.	6.12. A konfigurációváltozások felügyelete – Kriptográfia kezelése	K06.012_P[1]	a konfigurációkezelés hatálya alá tartozó kriptográfiai mechanizmusok által biztosított ellenőrzések meghatározottak
65.		K06.012_O.6.12	a K06.012_P[1] által meghatározott ellenőrzéshez használt kriptográfiai mechanizmusok a konfigurációkezelés hatálya alá tartoznak
66.	6.15. Biztonsági hatásvizsgálatok	K06.015_O.6.15	az EIR-t érintő változtatásokat a változtatás bevezetése előtt elemzik a lehetséges biztonsági hatások meghatározása érdekében

67.	6.16. Biztonsági hatásvizsgálatok – Különálló tesztkörnyezetek	K06.016_O.6.16.(a)	az EIR változtatásait különálló tesztkörnyezetben elemzik a hibákból eredő biztonsági hatások szempontjából
68.		K06.016_O.6.16.(b)	az EIR változtatásait különálló tesztkörnyezetben elemzik a sérülékenységek szempontjából
69.		K06.016_O.6.16.(c)	az EIR változtatásait különálló tesztkörnyezetben elemzik az inkompatibilitás miatti biztonsági hatások szempontjából
70.		K06.016_O.6.16.(d)	az EIR változtatásait különálló tesztkörnyezetben elemzik a szándékos rosszindulatból eredő biztonsági hatások szempontjából
71.	6.17. Biztonsági hatásvizsgálatok – Követelmények ellenőrzése	K06.017_O.6.17.(a)	ellenőrzésre kerül, hogy az EIR változtatását követően az érintett védelmi intézkedések helyesen kerültek-e bevezetésre
72.		K06.017_O.6.17.(b)	ellenőrzésre kerül, hogy az EIR változtatását követően az érintett védelmi intézkedések helyesen működnek-e
73.		K06.017_O.6.17.(c)	ellenőrzésre kerül, hogy az EIR változtatását követően az érintett védelmi intézkedések biztosítják-e a biztonsági célok teljesülését
74.	6.18. A változtatásokra vonatkozó hozzáférés korlátozások	K06.018_O.6.18.(a)	az EIR megváltoztatásához kapcsolódó fizikai hozzáférési korlátozások meghatározottak és dokumentáltak
75.		K06.018_O.6.18.(b)	az EIR megváltoztatásához kapcsolódó fizikai hozzáférési korlátozások jóváhagyása megtörtént
76.		K06.018_O.6.18.(c)	az EIR megváltoztatásához kapcsolódó fizikai hozzáférési korlátozásokat érvényesítik
77.		K06.018_O.6.18.(d)	az EIR megváltoztatásához kapcsolódó logikai hozzáférési korlátozások meghatározottak és dokumentáltak
78.		K06.018_O.6.18.(e)	az EIR megváltoztatásához kapcsolódó logikai hozzáférési korlátozások jóváhagyása megtörtént
79.		K06.018_O.6.18.(f)	az EIR megváltoztatásához kapcsolódó logikai hozzáférési korlátozásokat érvényesítik
80.	6.19. A változtatásokra vonatkozó hozzáférés korlátozások – Automatizált hozzáférés-érvényesítés és naplóbejegyzések	K06.019_P[1]	a hozzáférési korlátozások érvényesítésének automatizálására használt mechanizmusok meghatározottak
81.		K06.019_O.6.19.1	a változtatásra vonatkozó hozzáférési korlátozásokat a K06.019_P[1] által meghatározott automatizált mechanizmusok segítségével érvényesítik
82.		K06.019_O.6.19.2	az érvényesítési műveletek naplóbejegyzései automatikusan generálódnak
83.	6.23. Konfigurációs beállítások	K06.023_P[1]	egységes biztonsági konfigurációkat határoztak meg a rendszerelemekben alkalmazott konfigurációs beállítások létrehozására és dokumentálására
84.		K06.023_P[2]	meghatározottak azok a rendszerelemek, amelyek esetében az eltérések jóváhagyása szükséges
85.		K06.023_P[3]	az eltérések jóváhagyását szükségessé tevő működési követelmények meghatározottak
86.		K06.023_O.6.23.1	a K06.023_P[1] által meghatározott egységes biztonságos konfigurációkat használó rendszerelemek esetében az üzemeltetési követelményekkel összhangban lévő legkorlátozottabb üzemmódot tükröző konfigurációs beállításokat állapítottak meg és dokumentáltak
87.		K06.023_O.6.23.2	a K06.023_P[1] által meghatározott konfigurációs beállítások végrehajtásra kerülnek

88.		K06.023_O.6.23.3.(a)	a K06.023_P[2] által meghatározott rendszerelemek konfigurációs beállításaitól való eltérések azonosítása és dokumentálása a K06.023_P[3] által meghatározott működési követelmények alapján történt
89.		K06.023_O.6.23.3.(b)	a K06.023_P[2] által meghatározott rendszerelemek konfigurációs beállításaitól való bármilyen eltérés jóváhagyott
90.		K06.023_O.6.23.4.(a)	a konfigurációs beállítások módosításait a szervezeti szabályzatoknak és eljárásoknak megfelelően figyelemmel kísérik
91.		K06.023_O.6.23.4.(b)	a konfigurációs beállítások módosításait a szervezeti szabályzatoknak és eljárásoknak megfelelően ellenőrzik
92.	6.24. Konfigurációs beállítások – Automatizált kezelés, alkalmazás és ellenőrzés	K06.024_P[1]	meghatározottak azok a rendszerelemek, amelyekhez a konfigurációs beállításait automatizált mechanizmusokkal irányítják
93.		K06.024_P[2]	a konfigurációs beállítások irányítására használt automatizált mechanizmusok meghatározottak
94.		K06.024_P[3]	a konfigurációs beállítások alkalmazására használt automatizált mechanizmusok meghatározottak
95.		K06.024_P[4]	a konfigurációs beállítások ellenőrzésére használt automatizált mechanizmusok meghatározottak
96.		K06.024_O.6.24.(a)	a K06.024_P[1] által meghatározott rendszerelemek konfigurációs beállításait a K06.024_P[2] által meghatározott automatizált mechanizmusok segítségével irányítják
97.		K06.024_O.6.24.(b)	a K06.024_P[1] által meghatározott rendszerelemek konfigurációs beállításait a K06.024_P[3] által meghatározott automatizált mechanizmusok segítségével alkalmazzák
98.		K06.024_O.6.24.(c)	a K06.024_P[1] által meghatározott rendszerelemek konfigurációs beállításait a K06.024_P[4] által meghatározott automatizált mechanizmusok segítségével ellenőrzik
99.	6.25. Konfigurációs beállítások – Reagálás a jogosulatlan változtatásokra	K06.025_P[1]	meghatározottak a jogosulatlan változtatás esetén végrehajtandó intézkedések
100.		K06.025_P[2]	olyan konfigurációs beállítások vannak meghatározva, amelyek jogosulatlan módosítás esetén intézkedést igényelnek
101.		K06.025_O.6.25	a K06.025_P[1] által meghatározott intézkedéseket a K06.025_P[2] által meghatározott konfigurációs beállításainak jogosulatlan megváltoztatása esetén végrehajtják
102.	6.26. Legszűkebb funkcionalitás	K06.026_P[1]	a rendszer ügy- és üzletmenete szempontjából lényeges képességek meghatározottak
103.		K06.026_P[2]	a tiltandó vagy korlátozandó funkciók meghatározottak
104.		K06.026_P[3]	a tiltandó vagy korlátozandó portok meghatározottak
105.		K06.026_P[4]	a tiltandó vagy korlátozandó protokollok meghatározottak
106.		K06.026_P[5]	a tiltandó vagy korlátozandó szoftverek meghatározottak
107.		K06.026_P[6]	a tiltandó vagy korlátozandó szolgáltatások meghatározottak

108.		K06.026_O.6.26.1	a rendszer úgy van konfigurálva, hogy csak a K06.026_P[1] által meghatározott ügy- és üzletmenet szempontjából lényeges képességeket nyújtsa
109.		K06.026_O.6.26.2.(a)	a K06.026_P[2] által meghatározott funkciók használata tilos vagy korlátozott
110.		K06.026_O.6.26.2.(b)	a K06.026_P[3] által meghatározott portok használata tilos vagy korlátozott
111.		K06.026_O.6.26.2.(c)	a K06.026_P[4] által meghatározott protokollok használata tilos vagy korlátozott
112.		K06.026_O.6.26.2.(d)	a K06.026_P[5] által meghatározott szoftverek használata tilos vagy korlátozott
113.		K06.026_O.6.26.2.(e)	a K06.026_P[6] által meghatározott szolgáltatások használata tilos vagy korlátozott
114.	6.28. Legszűkebb funkcionalitás – Program futtatásának megakadályozása	K06.028_P[1]	a programok használatára és korlátozásaira vonatkozó feltételek szabályzatokban, illetve eljárásrendekben dokumentáltak
115.		K06.028_O.6.28	a program futtatása a K06.028_P[1] által meghatározott feltételek szerint kontrollált
116.	6.31. Legszűkebb funkcionalitás – Engedélyezett Szoftverek – Kivételes Engedélyezés	K06.031_P[1]	meghatározottak az EIR-en vagy EIR által futtatásra engedélyezett szoftverek
117.		K06.031_P[2]	meghatározott az engedélyezett szoftverek listájának felülvizsgálatára és frissítésére vonatkozó gyakoriság
118.		K06.031_O.6.31.1	a K06.031_P[1] által meghatározott szoftverek futtatását whitelist biztosítja
119.		K06.031_O.6.31.2	csak a K06.031_P[1] szerinti szoftverek futtatása engedélyezett
120.		K06.031_O.6.31.3	az engedélyezett szoftverek listáját felülvizsgálják és frissítik a K06.031_P[2] által meghatározott gyakorisággal
121.	6.36. Rendszerelem leltár	K06.036_P[1]	a rendszerelemek hatékony elszámoltathatóságának eléréséhez szükségesnek ítélt információk meghatározásra kerültek
122.		K06.036_P[2]	meghatározzák a rendszerelem-leltár felülvizsgálatának és frissítésének gyakoriságát
123.		K06.036_O.6.36.1.1	a rendszerelemek leltára, kidolgozott és dokumentált
124.		K06.036_O.6.36.1.2	a rendszerelemek leltára az EIR összes elemére kiterjed
125.		K06.036_O.6.36.1.3	a rendszerelemek leltára mellőzi a többszörös elszámolást
126.		K06.036_O.6.36.1.4	a rendszerelemek leltára a nyomonkövetéshez és a jelentéstételhez szükségesnek ítélt részletességű
127.		K06.036_O.6.36.1.5	a K06.036_P[1] által meghatározott információkat a rendszerelemek leltára tartalmazza
128.		K06.036_O.6.36.2	a rendszerelemek leltárát felülvizsgálják és frissítik a K06.036_P[2] által meghatározott gyakorisággal
129.	6.37. Rendszerelem leltár – Frissítések a telepítés és eltávolítás során	K06.037_O.6.37.(a)	a rendszerelemek leltárát a rendszerelemek telepítésekor frissítik
130.		K06.037_O.6.37.(b)	a rendszerelemek leltárát a rendszerelemek eltávolításakor frissítik
131.		K06.037_O.6.37.(c)	a rendszerelemek leltárát a rendszerfrissítések esetén frissítik

132.	6.38. Rendszerelem leltár – Automatizált karbantartás	K06.038_P[1]	a rendszerelem leltár naprakészségének fenntartására használt automatizált mechanizmusok meghatározottak
133.		K06.038_P[2]	a rendszerelem leltár teljességének fenntartására használt automatizált mechanizmusok meghatározottak
134.		K06.038_P[3]	a rendszerelem leltár pontosságának fenntartására használt automatizált mechanizmusok meghatározottak
135.		K06.038_P[4]	a rendszerelem leltár hozzáférhetőségének fenntartására használt automatizált mechanizmusok meghatározottak
136.		K06.038_O.6.38.(a)	a K06.038_P[1] által meghatározott automatizált mechanizmusokat használják a rendszerelem leltár naprakészségének fenntartására
137.		K06.038_O.6.38.(b)	a K06.038_P[2] által meghatározott automatizált mechanizmusokat használják a rendszerelem leltár teljességének fenntartására
138.		K06.038_O.6.38.(c)	a K06.038_P[3] által meghatározott automatizált mechanizmusokat használják a rendszerelem leltár pontosságának fenntartására
139.		K06.038_O.6.38.(d)	a K06.038_P[4] által meghatározott automatizált mechanizmusokat használják a rendszerelem leltár hozzáférhetőségének fenntartására
140.	6.39. Rendszerelem leltár – Jogosulatlan elemek automatikus észlelése	K06.039_P[1]	a rendszeren belüli jogosulatlan hardver jelenlétének észlelésére használt automatizált mechanizmusok meghatározottak
141.		K06.039_P[2]	a rendszeren belüli jogosulatlan szoftver jelenlétének észlelésére használt automatizált mechanizmusok meghatározottak
142.		K06.039_P[3]	a rendszeren belüli jogosulatlan firmware jelenlétének észlelésére használt automatizált mechanizmusok meghatározottak
143.		K06.039_P[4]	meghatározott, hogy milyen gyakorisággal használják az automatizált mechanizmusokat a rendszerben lévő jogosulatlan rendszerelemek jelenlétének észlelésére
144.		K06.039_P[5]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {a jogosulatlan elemek hálózati hozzáférésének letiltása; a jogosulatlan elemek elszigetelése; a K06.039_P[6] által meghatározott személyek vagy szerepkörök értesítése}
145.		K06.039_P[6]	a jogosulatlan elemek észlelésekor értesítendő személyek vagy szerepkörök meghatározottak
146.		K06.039_O.6.39.1.(a)	a jogosulatlan hardver jelenlétét a rendszeren belül a K06.039_P[1] által meghatározott automatizált mechanizmusok a K06.039_P[4] szerinti gyakorisággal észlelik
147.		K06.039_O.6.39.1.(b)	a jogosulatlan szoftver jelenlétét a rendszeren belül a K06.039_P[2] által meghatározott automatizált mechanizmusok által a K06.039_P[4] szerinti gyakorisággal észlelik
148.		K06.039_O.6.39.1.(c)	a jogosulatlan firmware jelenlétét a rendszeren belül a K06.039_P[3] által meghatározott automatizált mechanizmusok a K06.039_P[4] szerinti gyakorisággal észlelik
149.		K06.039_O.6.39.2.(a)	a K06.039_P[5] által meghatározott PARAMÉTER-ÉRTÉKEK érvényesülnek, ha jogosulatlan hardvert észlelnek

150.		K06.039_O.6.39.2.(b)	a K06.039_P[5] által meghatározott PARAMÉTER-ÉRTÉKEK érvényesülnek, ha jogosulatlan szoftvert észlelnek
151.		K06.039_O.6.39.2.(c)	a K06.039_P[5] által meghatározott PARAMÉTER-ÉRTÉKEK érvényesülnek, ha jogosulatlan firmware-t észlelnek
152.	6.40. Rendszerelem leltár – Elszámoltathatósággal kapcsolatos információk	K06.040_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {név; munkakör; szerepkör}
153.		K06.040_O.6.40	a szervezet a rendszerelemek kezeléséért felelős és elszámoltatható személyeket a K06.040_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK alapján azonosítja a rendszerelemek leltárában
154.	6.45. Konfigurációkezelési terv	K06.045_P[1]	a konfigurációkezelési terv felülvizsgálatára és jóváhagyására kijelölt személyek vagy szerepkörök meghatározottak
155.		K06.045_O.6.45.(a)	a rendszer konfigurációkezelési terve kidolgozott és dokumentált
156.		K06.045_O.6.45.(b)	a rendszer konfigurációkezelési terve végrehajtásra került
157.		K06.045_O.6.45.1.(a)	a konfigurációkezelési terv figyelembe veszi a szerepköröket
158.		K06.045_O.6.45.1.(b)	a konfigurációkezelési terv figyelembe veszi a felelősségeket
159.		K06.045_O.6.45.1.(c)	a konfigurációkezelési terv figyelembe veszi a konfigurációkezelési folyamatokat és eljárásokat
160.		K06.045_O.6.45.2.(a)	a konfigurációkezelési terv a konfigurációs elemek azonosítására létrehoz egy folyamatot a rendszerfejlesztési életciklus során
161.		K06.045_O.6.45.2.(b)	a konfigurációkezelési terv a konfigurációs elemek konfigurációjának kezelésére létrehoz egy folyamatot a rendszerfejlesztési életciklus során
162.		K06.045_O.6.45.3.(a)	a konfigurációkezelési terv meghatározza az EIR konfigurációs elemeit
163.		K06.045_O.6.45.3.(b)	a konfigurációkezelési terv a konfigurációs elemeket a konfigurációkezelés hatálya alá helyezi
164.		K06.045_O.6.45.4	a konfigurációkezelési terv a K06.045_P[1] által meghatározott személyek vagy szerepkörök által felülvizsgált és jóváhagyott
165.		K06.045_O.6.45.5.(a)	a konfigurációkezelési terv védett a jogosulatlan közzététellel szemben
166.		K06.045_O.6.45.5.(b)	a konfigurációkezelési terv védett a jogosulatlan módosítással szemben
167.	6.47. A szoftverhasználat korlátozásai	K06.047_O.6.47.1	a szoftver és a kapcsolódó dokumentációinak felhasználása a szerződéses megállapodásoknak és a szerzői jogot szabályozó jogszabályoknak megfelelően történik
168.		K06.047_O.6.47.2	a mennyiségi licencek által védett szoftver és a kapcsolódó dokumentáció használatát nyomon követik a másolás és a megosztás ellenőrzése érdekében
169.		K06.047_O.6.47.3	állománymegosztó technológia használatakor ellenőrzik, hogy az állománymegosztást ne használják szerzői jogi védelem alatt álló művek engedély nélküli terjesztésére, megjelenítésére, előadására vagy sokszorosítására

170.	6.49. Felhasználó által telepített szoftver	K06.049_P[1]	a szoftverek felhasználók általi telepítését szabályozó követelmények meghatározottak
171.		K06.049_P[2]	a szoftvertelepítési szabályok érvényesítésére használt módszerek meghatározottak
172.		K06.049_P[3]	meghatározott a szabályoknak történő megfelelés ellenőrzésének gyakorisága
173.		K06.049_O.6.49.1	a K06.049_P[1] által meghatározott szoftverek felhasználók általi telepítését szabályozó követelmények kialakításra kerültek
174.		K06.049_O.6.49.2	a szoftvertelepítési szabályok érvényesítése a K06.049_P[2] által meghatározott módszerekkel történik
175.		K06.049_O.6.49.3	a K06.049_P[1] által meghatározott követelményeknek való megfelelést a K06.049_P[3] által meghatározott gyakorisággal ellenőrzik
176.	6.52. Információ helyének azonosítása és dokumentálása	K06.052_P[1]	meghatározottak azok az információk, amelyek esetében a feldolgozási és tárolási helyszín dokumentálandó
177.		K06.052_O.6.52.1.(a)	a K06.052_P[1] által meghatározott információk helye azonosított és dokumentált
178.		K06.052_O.6.52.1.(b)	azonosítottak és dokumentáltak azok a konkrét rendszerelemek, amelyeken a K06.052_P[1] által meghatározott információkat feldolgozzák
179.		K06.052_O.6.52.1.(c)	azonosítottak és dokumentáltak azok a konkrét rendszerelemek, amelyeken a K06.052_P[1] által meghatározott információkat tárolják
180.		K06.052_O.6.52.2.(a)	a K06.052_P[1] által meghatározott információk feldolgozási helyszínéhez hozzáféréssel rendelkező felhasználók azonosítottak és hozzáférésük dokumentált
181.		K06.052_O.6.52.2.(b)	a K06.052_P[1] által meghatározott információk tárolási helyszínéhez hozzáféréssel rendelkező felhasználók azonosítottak és hozzáférésük dokumentált
182.		K06.052_O.6.52.3.(a)	a K06.052_P[1] által meghatározott információk feldolgozásának helyét – azaz a rendszert vagy a rendszerelemeket – érintő változásokat dokumentálják
183.		K06.052_O.6.52.3.(b)	a K06.052_P[1] által meghatározott információk tárolásának helyét – azaz a rendszert vagy a rendszerelemeket – érintő változásokat dokumentálják

7. Készenléti tervezés

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	7.1. Szabályzat és eljárásrendek	K07.001_P[1]	meghatározottak azok a személyek, illetve szerepkörök, akikkel az üzletmenet-folytonosságra vonatkozó szabályzatot meg kell ismertetni
3.		K07.001_P[2]	meghatározottak azok a személyek, illetve szerepkörök, akikkel az üzletmenet-folytonossági eljárásokat meg kell ismertetni
4.		K07.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K07.001_P[4]	az üzletmenet-folytonosságra vonatkozó szabályzat és eljárások irányítására kijelölésre került egy személy
6.		K07.001_P[5]	az üzletmenet-folytonossági szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K07.001_P[6]	meghatározottak azok az események, amelyek az üzletmenet-folytonossági szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K07.001_P[7]	meghatározott az üzletmenet-folytonossági eljárások felülvizsgálatának és frissítésének gyakorisága
9.		K07.001_P[8]	meghatározottak azok az események, amelyek miatt az üzletmenet-folytonossági eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K07.001_O_7.1.1.(a)	üzletmenet-folytonossági szabályzatot dolgoztak ki és dokumentáltak
11.		K07.001_O_7.1.1.(b)	az üzletmenet-folytonossági szabályzatot megismertették a K07.001_P[1] által meghatározott személyekkel, illetve szerepkörökkel
12.		K07.001_O_7.1.1.(c)	az üzletmenet-folytonossági szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő üzletmenet-folytonossági eljárások kidolgozásra és dokumentálásra kerültek
13.		K07.001_O_7.1.1.(d)	az üzletmenet-folytonossági eljárások megismertetésre kerültek a K07.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K07.001_O_7.1.2	a K07.001_P[4] által meghatározott személyt kijelölték az üzletmenet-folytonossági szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítására
15.		K07.001_O_7.1.3.(a)	az üzletmenet-folytonossági szabályzatot felülvizsgálják és frissítik a K07.001_P[5] által meghatározott gyakorisággal
16.		K07.001_O_7.1.3.(b)	az üzletmenet-folytonossági szabályzatot felülvizsgálják és frissítik a K07.001_P[6] által meghatározott eseményeket követően

17.		K07.001_O_7.1.3.(c)	az üzletmenet-folytonossági eljárásokat felülvizsgálják és frissítik a K07.001_P[7] által meghatározott gyakorisággal
18.		K07.001_O_7.1.3.(d)	az üzletmenet-folytonossági eljárásokat felülvizsgálják és frissítik a K07.001_P[8] által meghatározott eseményeket követően
19.		K07.001_O_7.1.1.1.1.(a)	az üzletmenet-folytonossági szabályzat célja meghatározásra került a K07.001_P[3] által meghatározottak szerint
20.		K07.001_O_7.1.1.1.1.(b)	az üzletmenet-folytonossági szabályzat hatóköre meghatározásra került a K07.001_P[3] által meghatározottak szerint
21.		K07.001_O_7.1.1.1.1.(c)	az üzletmenet-folytonossági szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K07.001_P[3] által meghatározottak szerint
22.		K07.001_O_7.1.1.1.1.(d)	az üzletmenet-folytonossági szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K07.001_P[3] által meghatározottak szerint
23.		K07.001_O_7.1.1.1.1.(e)	az üzletmenet-folytonossági szabályzatban foglalt célok iránti vezetői elkötelezettség rögzítésre került a K07.001_P[3] által meghatározottak szerint
24.		K07.001_O_7.1.1.1.1.(f)	az üzletmenet-folytonossági szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K07.001_P[3] által meghatározottak szerint
25.		K07.001_O_7.1.1.1.1.(g)	az üzletmenet-folytonossági szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K07.001_P[3] által meghatározottak szerint
26.		K07.001_O_7.1.1.1.2.	az üzletmenet-folytonossági szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal
27.	7.2. Üzletmenet-folytonossági terv	K07.002_P[1]	az üzletmenet-folytonossági tervet felülvizsgáló személyek vagy szerepek meghatározásra kerültek
28.		K07.002_P[2]	az üzletmenet-folytonossági terv jóváhagyására jogosult személyeket vagy szerepeket meghatározták
29.		K07.002_P[3]	meghatározták azokat az üzletmenet-folytonosság szempontjából kulcsfontosságú személyeket – név, illetve szerepkör szerint azonosítva –, akiknek az üzletmenet-folytonossági terv kihirdetésre kerül
30.		K07.002_P[4]	meghatározták azokat a működés szempontjából kulcsfontosságú szervezeti egységeket, amelyek számára az üzletmenet-folytonossági terv kihirdetésre kerül
31.		K07.002_P[5]	az üzletmenet-folytonossági terv felülvizsgálatának gyakorisága meghatározott
32.		K07.002_P[6]	meghatározták azokat a – név szerint, illetve szerepkör szerint azonosított – folyamatos működés szempontjából kulcsfontosságú személyeket, akikkel a változásokat közölni kell
33.		K07.002_P[7]	meghatározták azokat a – név szerint, illetve szerepkör szerint azonosított – folyamatos működés szempontjából kulcsfontosságú szervezeti egységeket, akikkel a változásokat közölni kell
34.		K07.002_O.7.2.1.1	az üzletmenet-folytonossági terv meghatározza az alapvető feladatokat és funkciókat, valamint a kapcsolódó vészhelyzeti követelményeket

35.		K07.002_O.7.2.1.2.(a)	az üzletmenet-folytonossági terv meghatározza a helyreállítási célokat
36.		K07.002_O.7.2.1.2.(b)	az üzletmenet-folytonossági terv meghatározza a helyreállítási prioritásokat
37.		K07.002_O.7.2.1.2.(c)	az üzletmenet-folytonossági terv meghatározza a helyreállítási metrikákat
38.		K07.002_O.7.2.1.3.(a)	az üzletmenet-folytonossági terv meghatározza a vészhelyzeti szerepköröket
39.		K07.002_O.7.2.1.3.(b)	az üzletmenet-folytonossági terv meghatározza a vészhelyzeti felelősségeket
40.		K07.002_O.7.2.1.3.(c)	az üzletmenet-folytonossági terv tartalmazza a vészhelyzeti szerepköröket betöltő személyeket és azok elérhetőségeit
41.		K07.002_O.7.2.1.4	az üzletmenet-folytonossági terv tartalmazza az EIR összeomlása, kompromittálódás vagy meghibásodása esetében biztosítandó alapvető üzleti funkciókat
42.		K07.002_O.7.2.1.5	az üzletmenet-folytonossági terv tartalmazza az eredetileg tervezett és végrehajtott védelmi intézkedések romlása nélkül a rendszer végleges, teljes körű helyreállításának leírását
43.		K07.002_O.7.2.1.6	az üzletmenet-folytonossági terv szabályozza az üzletmenet-folytonossági információk megosztását
44.		K07.002_O.7.2.1.7.(a)	az üzletmenet-folytonossági tervet K07.002_P[1] által meghatározott személyek vagy szerepkörök felülvizsgálják
45.		K07.002_O.7.2.1.7.(b)	az üzletmenet-folytonossági tervet a K07.002_P[2] által meghatározott személyek vagy szerepkörök jóváhagyták
46.		K07.002_O.7.2.2.(a)	az üzletmenet-folytonossági tervet ismertették a K07.002_P[3] által meghatározott az üzletmenet-folytonosság szempontjából kulcsfontosságú személyekkel
47.		K07.002_O.7.2.2.(b)	az üzletmenet-folytonossági tervet ismertették a K07.002_P[4] által meghatározott az üzletmenet-folytonosság szempontjából kulcsfontosságú szervezeti egységekkel
48.		K07.002_O.7.2.3	az üzletmenet-folytonosság tervezési tevékenységek összehangoltak a biztonsági eseménykezelési tevékenységekkel
49.		K07.002_O.7.2.4	az üzletmenet-folytonossági terv felülvizsgálatra kerül a K07.002_P[5] által meghatározott gyakorisággal
50.		K07.002_O.7.2.5.(a)	az üzletmenet-folytonossági tervet a szervezet a rendszer vagy a működési környezet változásainak figyelembevételével frissíti
51.		K07.002_O.7.2.5.(b)	az üzletmenet-folytonossági tervet frissítik az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerült problémák kezelése érdekében
52.		K07.002_O.7.2.6.(a)	az üzletmenet-folytonossági terv változásait közlik a K07.002_P[6] által meghatározott, a működés szempontjából kulcsfontosságú személyekkel
53.		K07.002_O.7.2.6.(b)	az üzletmenet-folytonossági terv változásait közlik a K07.002_P[7] által meghatározott, a működés szempontjából kulcsfontosságú szervezeti egységekkel

54.		K07.002_O.7.2.7.(a)	az üzletmenet-folytonossági terv teszteléséből vagy a tényleges alkalmazásából levont tanulságokat beépítik az üzletmenet-folytonosság tesztelési folyamatába
55.		K07.002_O.7.2.7.(b)	az üzletmenet-folytonossági terv gyakorlatából vagy a tényleges alkalmazásából levont tanulságokat beépítik az üzletmenet-folytonosság tesztelési és gyakorlati folyamatába
56.		K07.002_O.7.2.8.(a)	az üzletmenet-folytonossági terv védett a jogosulatlan nyilvánosságra hozatallal szemben
57.		K07.002_O.7.2.8.(b)	az üzletmenet-folytonossági terv védett a jogosulatlan módosítással szemben
58.	7.3. Üzletmenet-folytonossági terv – Összehangolás a kapcsolódó tervekkel	K07.003_O.7.3	az üzletmenet-folytonossági terv kidolgozását összehangolták a kapcsolódó tervekért felelős szervezeti egységekkel
59.	7.4. Üzletmenet-folytonossági terv – Kapacitás tervezése	K07.004_O.7.4.(a)	a kapacitástervezést úgy végzik, hogy az információfeldolgozáshoz szükséges kapacitás rendelkezésre álljon a folyamatos működés során
60.		K07.004_O.7.4.(b)	a kapacitástervezést úgy végzik, hogy az infokommunikációhoz szükséges kapacitás rendelkezésre álljon a folyamatos működés során
61.		K07.004_O.7.4.(c)	a kapacitástervezést úgy végzik, hogy a környezeti képességek biztosításához szükséges kapacitás rendelkezésre álljon a folyamatos működés során
62.	7.5. Üzletmenet-folytonossági terv – Üzleti (ügymeneti) funkciók visszaállítása	K07.005_P[1]	az üzletmenet-folytonossági tervben meghatározott az az időtartam, amelyen belül a szervezet az alapvető üzleti funkciók újraindításáról gondoskodik
63.		K07.005_O.7.5	az alapvető üzleti funkciók újrakezdését a K07.005_P[1] által meghatározott időn belül valósítják meg
64.	7.6. Üzletmenet-folytonossági terv – Alapfeladatok és alapfunkciók folyamatossága	K07.006_O.7.6.(a)	az alapvető üzleti funkciók fenntartására folyamatot dolgoznak ki a működési folyamatosság csekély veszteséggel járó vagy semmilyen veszteséggel nem járó fenntartása mellett
65.		K07.006_O.7.6.(b)	a működési folyamatosság az elsődleges feldolgozási, illetve tárolási helyszíneken az EIR teljes helyreállításáig fennmarad
66.	7.9. Üzletmenet-folytonossági terv – Kritikus erőforrások meghatározása	K07.009_O.7.9	az alapfeladatokat vagy az alapvető üzleti folyamatokat támogató kritikus erőforrások azonosítottak
67.	7.10. A folyamatos működésre felkészítő képzés	K07.010_P[1]	meghatározott az az időtartam, amelyen belül az új szerepkör vagy felelősségi kör átvételét követően a folyamatos működésre felkészítő képzés megtartásra kerül
68.		K07.010_P[2]	a folyamatos működésre felkészítő képzés gyakorisága meghatározott
69.		K07.010_P[3]	meghatározott, hogy milyen gyakorisággal kell felülvizsgálni és frissíteni a folyamatos működésre felkészítő képzés tartalmát
70.		K07.010_P[4]	a folyamatos működésre felkészítő képzés felülvizsgálatát és frissítését szükségessé tevő események meghatározásra kerültek

71.		K07.010_O.7.10.1.1	a rendszerfelhasználók a K07.010_P[1] által meghatározott időtartamon belül képzésben részesülnek
72.		K07.010_O.7.10.1.2	a rendszerhasználók számára a kijelölt szerepkörökkel és felelősségi körökkel összhangban álló, az EIR változásai által megkövetelt folyamatos működésre felkészítő képzés megtartásra került
73.		K07.010_O.7.10.1.3	a rendszerhasználók számára a kiosztott szerepeknek és felelősségi köröknek megfelelő folyamatos működésre felkészítő képzést biztosítanak a K07.010_P[2] által meghatározott gyakorisággal
74.		K07.010_O.7.10.2.(a)	a folyamatos működésre felkészítő képzés tartalmát felülvizsgálják és frissítik a K07.010_P[3] által meghatározott gyakorisággal
75.		K07.010_O.7.10.2.(b)	a K07.010_P[4] által meghatározott eseményeket követően felülvizsgálják és frissítik a folyamatos működésre felkészítő képzés tartalmát
76.	7.11. A folyamatos működésre felkészítő képzés – Szimulált események	K07.011_O.7.11	szimulált eseményeket építenek be a folyamatos működésre felkészítő képzésbe, hogy megkönnyítsék a személyzet hatékony reagálását kritikus helyzetekben
77.	7.13. Üzletmenet-folytonossági terv tesztelése	K07.013_P[1]	a rendszerre vonatkozó üzletmenet-folytonossági terv tesztelési gyakorisága meghatározásra került
78.		K07.013_P[2]	meghatározták az üzletmenet-folytonossági terv hatékonyságának meghatározására szolgáló teszteket
79.		K07.013_P[3]	meghatározták a szervezet felkészültségének meghatározására szolgáló teszteket
80.		K07.013_O.7.13.1.(a)	a rendszerre vonatkozó üzletmenet-folytonossági terv tesztelése a K07.013_P[1] által meghatározott gyakorisággal történik
81.		K07.013_O.7.13.1.(b)	a K07.013_P[2] által meghatározott tesztek a terv hatékonyságának mérésére alkalmasak
82.		K07.013_O.7.13.1.(c)	a K07.013_P[3] által meghatározott tesztek a terv felkészültségének mérésére alkalmasak
83.		K07.013_O.7.13.1.(d)	az üzletmenet-folytonossági terv tesztelési eredményeinek értékelése megtörténik
84.		K07.013_O.7.13.2	az üzletmenet-folytonossági terv tesztelési eredményeinek felülvizsgálata megtörténik
85.		K07.013_O.7.13.3	szükség esetén korrekciós intézkedések kerülnek végrehajtásra
86.	7.14. Üzletmenet-folytonossági terv tesztelése – Összehangolás a kapcsolódó tervekkel	K07.014_O.7.14	az üzletmenet-folytonossági terv tesztelését összehangolják a kapcsolódó tervekért felelős szervezeti egységek
87.	7.15. Üzletmenet-folytonossági terv tesztelése – Alternatív feldolgozási helyszín	K07.015_O.7.15.1	az üzletmenet-folytonossági tervet az alternatív feldolgozási helyszínen tesztelik annak érdekében, hogy a vészhelyzeti személyzet megismerje a létesítményt és a rendelkezésre álló erőforrásokat
88.		K07.015_O.7.15.2	az üzletmenet-folytonossági tervet az alternatív feldolgozási helyszínen tesztelik, hogy értékeljék az alternatív feldolgozási helyszín képességeit a vészhelyzeti műveletek támogatására

89.	7.19. Biztonsági tárolási helyszín	K07.019_O.7.19.1.(a)	biztonsági tárolási helyszín biztosított
90.		K07.019_O.7.19.1.(b)	a biztonsági tárolási helyszín létrehozása magában foglalja a rendszer biztonsági másolatainak tárolásához és visszakereséséhez szükséges megállapodásokat
91.		K07.019_O.7.19.2	a biztonsági tárolási helyszín az elsődleges tárolási helyszínnel egyenértékű védelmi intézkedéseket biztosít
92.	7.20. Biztonsági tárolási helyszín – Elkülönítés az elsődleges tárolási helyszíntől	K07.020_O.7.20	az elsődleges tárolási helyszíntől elkülönített alternatív tárolási helyszín került meghatározásra, ami csökkenti az ugyanezen veszélyekre való kitettséget
93.	7.21. Biztonsági tárolási helyszín – Helyreállítási idő és helyreállítási pont céljai	K07.021_O.7.21.(a)	a biztonsági tárolási helyszín úgy van konfigurálva, hogy megkönnyítse a helyreállítási műveleteket a helyreállítási idő céljainak megfelelően
94.		K07.021_O.7.21.(b)	a biztonsági tárolási helyszín úgy van konfigurálva, hogy megkönnyítse a helyreállítási műveleteket a helyreállítási pont céljainak megfelelően
95.	7.22. Biztonsági tárolási helyszín – Hozzáférhetőség	K07.022_P[1]	meghatározásra került az a terület a biztonsági tárolási helyszínen, amelyre kiterjedő zavar vagy katasztrófa esetén kockázatcsökkentő intézkedések alkalmazása szükséges
96.		K07.022_P[2]	a zavar vagy katasztrófa esetén alkalmazandó konkrét kockázatcsökkentő intézkedések meghatározottak
97.		K07.022_O.7.22	a szervezet azonosítja a potenciális hozzáférési problémákat a K07.022_P[1]-ben meghatározott helyszínen, amire reagálva a K07.022_P[2]-ben meghatározott intézkedéseket hozza
98.	7.23. Alternatív feldolgozási helyszín	K07.023_P[1]	az alapvető üzleti funkciók meghatározottak
99.		K07.023_P[2]	a helyreállítási idővel és a helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő, alternatív helyszínre való átállás időtartama meghatározott
100.		K07.023_O.7.23.1	a K07.023_P[2] által meghatározott időtartamon belül alternatív feldolgozási helyszínt hoznak létre, beleértve a K07.023_P[1] által meghatározott rendszerműveletek átadásához és újraindításához szükséges megállapodásokat az alapvető üzleti funkciók tekintetében, ha az elsődleges feldolgozási képességek nem állnak rendelkezésre
101.		K07.023_O.7.23.2.(a)	a műveletek áthelyezéséhez szükséges berendezések és felszerelések rendelkezésre állnak az alternatív feldolgozási helyszínen, vagy megkötésre kerültek a szerződések a K07.023_P[2] által meghatározott átadási időtartamon belül a helyszínre történő szállítás támogatására
102.		K07.023_O.7.23.2.(b)	a műveletek újraindításához szükséges berendezések és felszerelések rendelkezésre állnak az alternatív feldolgozási helyszínen, vagy megkötésre kerültek a szerződések a K07.023_P[2] által meghatározott átadási időtartamon belül a helyszínre történő szállítás támogatására
103.		K07.023_O.7.23.3	az alternatív feldolgozási helyszínen biztosított védelmi intézkedések egyenértékűek az elsődleges feldolgozási helyszínen biztosított védelmi intézkedésekkel
104.	7.24. Alternatív feldolgozási helyszín – Elkülönítés az elsődleges helyszíntől	K07.024_O.7.24	az elsődleges feldolgozási helyszíntől elkülönített alternatív feldolgozási helyszín került meghatározásra

105.	7.25. Alternatív feldolgozási helyszín – Hozzáférhetőség	K07.025_O.7.25.(a)	az alternatív feldolgozási helyszín esetleges hozzáférési problémáinak azonosítása biztosított az egész területre kiterjedő üzemzavar vagy katasztrófa esetén
106.		K07.025_O.7.25.(b)	az azonosított hozzáférhetőségi problémák megoldására irányuló kockázatcsökkentő intézkedések meghatározásra kerültek
107.	7.26. Alternatív feldolgozási helyszín – Szolgáltatás prioritása	K07.026_O.7.26	olyan alternatív feldolgozás helyszíni megállapodások kerülnek megkötésre, amelyek a rendelkezésre állási követelményekkel – beleértve a helyreállítási időkre vonatkozó célkitűzéseket is – összhangban a szolgáltatás prioritására vonatkozó rendelkezéseket tartalmaznak
108.	7.27. Alternatív feldolgozási helyszín – Használatra való felkészítés	K07.027_O.7.27	az alternatív feldolgozási helyszínt úgy készítik elő, hogy a helyszín az alapvető küldetési és üzleti funkciókat támogató operatív helyszínként szolgálhasson
109.	7.29.Telekommunikációs szolgáltatások	K07.029_P[1]	az alapvető üzleti funkciók meghatározottak
110.		K07.029_P[2]	meghatározták azt az időtartamot, amelyen belül az alapvető üzleti funkciókat újra kell indítani, ha az elsődleges infokommunikációs képességek nem állnak rendelkezésre
111.		K07.029_O.7.29	a K07.029_P[1] által meghatározott rendszerműveletek újraindításához szükséges megállapodásokat is tartalmazó alternatív infokommunikációs szolgáltatásokat a K07.029_P[2] által meghatározott időtartamon belül az alapvető üzleti funkciókhoz létrehozzák, ha az elsődleges infokommunikációs képességek nem állnak rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszíneken
112.	7.30. Telekommunikációs szolgáltatások – Szolgáltatásprioritási rendelkezések	K07.030_O.7.30.(a)	az elsődleges infokommunikációs szolgáltatásra vonatkozó szerződés tartalmaz szolgáltatásprioritási rendelkezéseket, beleértve a helyreállítási időkre vonatkozó időcélokat is
113.		K07.030_O.7.30.(b)	a tartalék infokommunikációs szolgáltatáshoz tartozó szerződés tartalmaz szolgáltatásprioritási rendelkezéseket, beleértve a helyreállítási időkre vonatkozó időcélokat is
114.	7.31. Telekommunikációs szolgáltatások – Kritikus meghibásodási pont	K07.031_O.7.31	olyan tartalék infokommunikációs szolgáltatásokat szereztek be, amelyek csökkenti a kritikus meghibásodási pontok valószínűségét
115.	7.32. Telekommunikációs szolgáltatások – Elsődleges és másodlagos szolgáltatók különválasztása	K07.032_O.7.32	a szervezet – nem az elsődleges szolgáltatótól – tartalék infokommunikációs szolgáltatásokat vesz igénybe
116.	7.33. Telekommunikációs szolgáltatások – Szolgáltatói üzletmenet-folytonossági terv	K07.033_P[1]	meghatározták azt a gyakoriságot, amellyel a szolgáltatóknak be kell szerezniük a tesztelésre vonatkozó bizonyítékokat
117.		K07.033_P[2]	meghatározták azt a gyakoriságot, amellyel a szolgáltatóknak be kell szerezniük a folyamatos működésre felkészítő képzésre vonatkozó dokumentációt
118.		K07.033_O.7.33.1.(a)	az elsődleges infokommunikációs szolgáltatók rendelkeznek üzletmenet-folytonossági tervekkel
119.		K07.033_O.7.33.1.(b)	a tartalék infokommunikációs szolgáltatók rendelkeznek üzletmenet-folytonossági tervekkel

120.		K07.033_O.7.33.2	a szolgáltató üzletmenet-folytonossági terveit felülvizsgálják annak biztosítása érdekében, hogy a tervek megfeleljenek a szervezet üzletmenet-folytonossági követelményeinek
121.		K07.033_O.7.33.3.(a)	a szolgáltatók által végzett folyamatos működéssel kapcsolatos tesztek bizonyítékait a szervezet a K07.033_P[1] által meghatározott gyakorisággal beszerzi
122.		K07.033_O.7.33.3.(b)	a szolgáltatók folyamatos működésre felkészítő képzésének bizonyítékait a szervezet a K07.033_P[2] által meghatározott gyakorisággal beszerzi
123.	7.35. Az elektronikus információs rendszer mentései	K07.035_P[1]	meghatározottak azok a rendszerelemek, amelyek esetében a felhasználói szintű információk biztonsági mentését el kell végezni
124.		K07.035_P[2]	meghatározásra került a felhasználói szintű információk biztonsági mentési gyakorisága, amely összhangban van a helyreállítási idővel és a helyreállítási pontokkal kapcsolatos célkitűzésekkel
125.		K07.035_P[3]	meghatározásra került, hogy milyen gyakorisággal kell biztonsági mentéseket készíteni a rendszerszintű információkról, ami összhangban van a helyreállítási idővel és a helyreállítási pontokkal kapcsolatos célkitűzésekkel
126.		K07.035_P[4]	meghatározásra került, hogy milyen gyakorisággal kell biztonsági mentéseket készíteni a rendszerdokumentációról, ami összhangban van a helyreállítási idővel és a helyreállítási pontokkal kapcsolatos célkitűzésekkel
127.		K07.035_O.7.35.1	a K07.035_P[1] által meghatározott rendszerelemek felhasználói szintű információinak biztonsági mentése a K07.035_P[2] által meghatározott gyakorisággal történik
128.		K07.035_O.7.35.2	a rendszerben található rendszerszintű információk biztonsági mentése a K07.035_P[3] által meghatározott gyakorisággal történik
129.		K07.035_O.7.35.3	a rendszer dokumentációjának biztonsági mentése, beleértve a biztonsággal kapcsolatos információkat is a K07.035_P[4] által meghatározott gyakorisággal történik
130.		K07.035_O.7.35.4.(a)	a mentési információk bizalmassága biztosított
131.		K07.035_O.7.35.4.(b)	a mentési információk sértetlensége biztosított
132.		K07.035_O.7.35.4.(c)	a mentési információk rendelkezésre állása biztosított
133.	7.36. Az elektronikus információs rendszer mentései – Megbízhatóság és sértetlenség tesztelése	K07.036_P[1]	meghatározott, hogy milyen gyakorisággal kell tesztelni a biztonsági mentéseket az adathordozó megbízhatósága szempontjából
134.		K07.036_P[2]	meghatározott, hogy milyen gyakorisággal kell tesztelni a biztonsági mentéseket az információk sértetlensége szempontjából
135.		K07.036_O.7.36.(a)	a mentési információk tesztelése a K07.036_P[1] által meghatározott gyakorisággal történik az adathordozó megbízhatóságának biztosítása érdekében
136.		K07.036_O.7.36.(b)	a mentési információk tesztelése a K07.036_P[2] által meghatározott gyakorisággal történik az információk sértetlenségének biztosítása érdekében

137.	7.37. Az elektronikus információs rendszer mentései – Visszaállítás tesztelése mintavétellel	K07.037_O.7.37	a helyreállítási terv tesztelésének részeként a kiválasztott rendszerfunkciók helyreállítása során legalább a biztonsági mentésekből származó információk mintáját használják
138.	7.38. Az elektronikus információs rendszer mentései – Kritikus információk elkülönített tárhelye	K07.038_P[1]	a szervezet működése szempontjából kritikus szoftverek és egyéb biztonsággal kapcsolatos információk azonosítottak
139.		K07.038_O.7.38	a K07.038_P[1] által meghatározott szoftverek és egyéb biztonsággal kapcsolatos információk mentéseit az elsődleges feldolgozási helyszíntől eltérő létesítményben vagy tűzbiztos tárolóban tárolják
140.	7.39. Az elektronikus információs rendszer mentései – Átvitel másodlagos tárolási helyszínre	K07.039_P[1]	a helyreállítási idővel és a helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban a másodlagos tárolási helyszínre történő adatátvitel időtartama meghatározott
141.		K07.039_P[2]	a helyreállítási idővel és a helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő, a másodlagos tárolási helyszínre történő másoláshoz szükséges minimális átviteli sebességet meghatározták
142.		K07.039_O.7.39.(a)	a rendszer biztonsági mentésének információi a K07.039_P[1] által meghatározott időtartamra átkerülnek az alternatív tárolási helyszínre
143.		K07.039_O.7.39.(b)	a rendszer biztonsági mentésének információi a K07.039_P[2] által meghatározott átviteli sebességgel továbbításra kerülnek alternatív tárolási helyszínre
144.	7.42. Az elektronikus információs rendszer mentései – Kriptográfiai védelem	K07.042_P[1]	a biztonsági mentések védelme biztosított a jogosulatlan felfedéssel és módosítással szemben
145.		K07.042_O.7.42	a K07.042_P[1] által meghatározott biztonsági mentés információinak jogosulatlan felfedésének és módosításának megakadályozására kriptográfiai mechanizmusokat alkalmaznak
146.	7.43. Az elektronikus információs rendszer helyreállítása és újraindítása	K07.043_P[1]	az EIR helyreállítási idejére és helyreállítási pontjára a vonatkozó célkitűzésekkel összhangban lévő időtartamot határoztak meg
147.		K07.043_P[2]	az EIR újraindítási idejére és újraindítási pontjára a vonatkozó célkitűzésekkel összhangban lévő időtartamot határoztak meg
148.		K07.043_O.7.43.(a)	az EIR ismert állapotba történő helyreállítása megtörténik a K07.043_P[1] által meghatározott időtartamon belül összeomlást, kompromittálódást vagy hibát követően
149.		K07.043_O.7.43.(b)	az EIR ismert állapotba történő újraindítása megtörténik a K07.043_P[2] által meghatározott időtartamon belül összeomlást, kompromittálódást vagy hibát követően
150.	7.44. Az elektronikus információs rendszer helyreállítása és újraindítása – Tranzakciók helyreállítása	K07.044_O.7.44	a tranzakció-alapú rendszerek esetében tranzakció-helyreállítást hajtanak végre

151.	7.45. Az elektronikus információs rendszer helyreállítása és újraindítása – Meghatározott időn belüli visszaállítás	K07.045_P[1]	meghatározásra került az az elvárt helyreállítási időszak, amelyen belül a rendszerelemek ismert, üzemképes állapotba történő visszaállítása megtörténik
152.		K07.045_O.7.45	biztosított a K07.045_P[1] által meghatározott helyreállítási időtartamon belül a rendszerelemek helyreállításának képessége a konfiguráció által ellenőrzött és sértetlenség védett információkból, amelyek a rendszerelemek ismert, működőképes állapotát reprezentálják

8. Azonosítás és hitelesítés

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	8.1. Szabályzat és eljárásrendek	K08.001_P[1]	meghatározottak azok a személyek vagy szerepkörök, akikkel az azonosítási és hitelesítési eljárásokat meg kell ismertetni
3.		K08.001_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}.
4.		K08.001_P[3]	az azonosítási és hitelesítési szabályzat és eljárások irányítására egy meghatározott személyt került kijelölésre
5.		K08.001_P[4]	az azonosítási és hitelesítési szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
6.		K08.001_P[5]	meghatározták azokat az eseményeket, amelyek az azonosítási és hitelesítési szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
7.		K08.001_P[6]	meghatározták az azonosítási és hitelesítési eljárások felülvizsgálatának és frissítésének gyakoriságát
8.		K08.001_P[7]	meghatározták azokat az eseményeket, amelyek miatt az azonosítási és hitelesítési eljárásokat felül kell vizsgálni és aktualizálni kell
9.		K08.001_O_8.1.1.(a)	azonosítási és hitelesítési szabályzatot dolgoztak ki és dokumentáltak
10.		K08.001_O_8.1.1.(b)	az azonosítási és hitelesítési szabályzatot megismertették a K08.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
11.		K08.001_O_8.1.1.(c)	az azonosítási és hitelesítési szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő azonosítási és hitelesítési eljárások kidolgozása és dokumentálása megtörtént
12.		K08.001_O_8.1.2	a K08.001_P[3] által meghatározott személyt jelöltek ki az azonosítási és hitelesítési szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítására
13.		K08.001_O_8.1.3.(a)	az azonosítási és hitelesítési szabályzatot felülvizsgálják és frissítik a K08.001_P[4] által meghatározott gyakorisággal

14.		K08.001_O_8.1.3.(b)	az azonosítási és hitelesítési szabályzatot felülvizsgálják és frissítik a K08.001_P[5] által meghatározott eseményeket követően
15.		K08.001_O_8.1.3.(c)	az azonosítási és hitelesítési eljárásokat felülvizsgálják és frissítik a K08.001_P[6] által meghatározott gyakorisággal
16.		K08.001_O_8.1.3.(d)	az azonosítási és hitelesítési eljárásokat felülvizsgálják és frissítik a K08.001_P[7] által meghatározott eseményeket követően
17.		K08.001_O_8.1.1.1.1.(a)	az azonosítási és hitelesítési szabályzat célja meghatározásra került a K08.001_P[2] által meghatározottak szerint
18.		K08.001_O_8.1.1.1.1.(b)	az azonosítási és hitelesítési szabályzat hatóköre meghatározásra került a K08.001_P[2] által meghatározottak szerint
19.		K08.001_O_8.1.1.1.1.(c)	az azonosítási és hitelesítési szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K08.001_P[2] által meghatározottak szerint
20.		K08.001_O_8.1.1.1.1.(d)	az azonosítási és hitelesítési szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K08.001_P[2] által meghatározottak szerint
21.		K08.001_O_8.1.1.1.1.(e)	az azonosítási és hitelesítési szabályzatban foglalt célok iránti vezetői elkötelezettség rögzítésre került a K08.001_P[2] által meghatározottak szerint
22.		K08.001_O_8.1.1.1.1.(f)	az azonosítási és hitelesítési szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K08.001_P[2] által meghatározottak szerint
23.		K08.001_O_8.1.1.1.1.(g)	az azonosítási és hitelesítési szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K08.001_P[2] által meghatározottak szerint
24.		K08.001_O_8.1.1.1.2.	az azonosítási és hitelesítési szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel. szabályozásokkal, szabványokkal és ajánlásokkal
25.	8.2. Azonosítás és hitelesítés	K08.002_O.8.2.(a)	a szervezeti felhasználók egyedi azonosítása és hitelesítése megtörténik
26.		K08.002_O.8.2.(b)	a hitelesített szervezeti felhasználók által végzett tevékenységek egyedi azonosítóhoz kapcsoltak
27.	8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése	K08.003_P[1]	a privilegizált fiókok meghatározásra kerültek
28.		K08.003_O.8.3	a K08.003_P[1]-ben meghatározott privilegizált fiókokhoz való hozzáféréshez többtényezős hitelesítést alkalmaznak
29.	8.4. Azonosítás és hitelesítés (felhasználók) – Nem-privilegizált fiókok többtényezős hitelesítése	K08.004_O.8.4	a nem privilegizált fiókokhoz való hozzáféréshez többtényezős hitelesítést alkalmaznak
30.	8.5. Azonosítás és hitelesítés (felhasználók) – Egyéni azonosítás csoportos hitelesítéssel	K08.005_O.8.5	közös használatú fiókok vagy hitelesítők használata esetén a felhasználókat egyénileg hitelesítik, mielőtt hozzáférést biztosítanának a megosztott fiókokhoz vagy erőforrásokhoz

31.	8.7. Azonosítás és hitelesítés (felhasználók) – Hozzáférés a fiókokhoz – Visszajátszás elleni védelem	K08.007_O.8.7	az authentikációs mechanizmusban visszajátszásbiztos hitelesítési mechanizmusok vannak bevezetve
32.	8.10. Eszközök azonosítása és hitelesítése	K08.010_P[1]	meghatározottak azok az eszközök, illetve eszköztípusok, amelyeket a kapcsolat létrehozása előtt egyértelműen azonosítani és hitelesíteni kell
33.		K08.010_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {helyi; távoli; hálózati}.
34.		K08.010_O.8.10	a K08.010_P[1] által meghatározott eszközök, illetve eszköztípusok egyedi azonosítása és hitelesítése a K08.010_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK kapcsolattípusok létrehozása előtt megtörténik
35.	8.14. Azonosító kezelés	K08.014_P[1]	meghatározzák azokat a személyeket vagy szerepköröket, akik az egyedi azonosítók kiosztását engedélyezik
36.		K08.014_P[2]	meghatározzák az azonosítók újrafelhasználásának megakadályozására szolgáló időtartamot
37.		K08.014_O.8.14.1	a rendszerazonosítók kezelése úgy történik, hogy a K08.014_P[1] által meghatározott személyek vagy szerepkörök felhatalmazást kapnak egy személyhez, csoporthoz, szerepkörhöz vagy eszközazonosítóhoz való hozzárendelésre
38.		K08.014_O.8.14.2	a rendszerazonosítók kezelése a személy, csoport, szerepkör, szolgáltatás vagy eszköz azonosító kiválasztásával történik
39.		K08.014_O.8.14.3	a rendszerazonosítók kezelése úgy történik, hogy az azonosítót hozzárendelik a kívánt személyhez, csoporthoz, szerepkörhöz, szolgáltatáshoz vagy eszközhöz
40.		K08.014_O.8.14.4	a rendszerazonosítókat úgy kezelik, hogy megakadályozzák az azonosítók K08.014_P[2] által meghatározott időtartamon belüli újrafelhasználását
41.	8.16. Azonosító kezelés – Felhasználói státusz azonosítása	K08.016_P[1]	az azonosító státuszának azonosítására használt jellemzők meghatározásra kerültek
42.		K08.016_O.8.16	az egyéni azonosítókat úgy kezelik, hogy minden egyes személyt egyedileg azonosítanak a K08.016_P[1] által meghatározott jellemzőkkel
43.	8.21. A hitelesítésre szolgáló eszközök kezelése	K08.021_P[1]	a hitelesítő eszközök típusonkénti megváltoztatására vagy frissítésére vonatkozó időszakot meghatározták
44.		K08.021_P[2]	a hitelesítő eszközök megváltoztatását vagy frissítését kiváltó események meghatározottak
45.		K08.021_O.8.21.1	a rendszerhitelesítő eszközök kezelése a hitelesítőt kapó egyén, csoport, szerepkör, szolgáltatás vagy eszköz személyazonosságának ellenőrzésével történik a kezdeti hitelesítők kiosztásának részeként
46.		K08.021_O.8.21.2	a rendszerhitelesítő eszközök kezelése a szervezet által kibocsátott hitelesítők kezdeti hitelesítőtartalmának létrehozásával történik
47.		K08.021_O.8.21.3	a rendszerhitelesítő eszközöket úgy kezelik, hogy a hitelesítők a rendeltetésszerű használatukhoz megfelelő erősségű mechanizmussal rendelkezzenek

48.		K08.021_O.8.21.4	a rendszerhitelesítő eszközök kezelése a kezdeti hitelesítők kiosztására, az elveszett, kompromittált vagy sérült hitelesítőkre, valamint a hitelesítők visszavonására vonatkozó adminisztratív eljárások létrehozásával és végrehajtásával történik
49.		K08.021_O.8.21.5	a rendszerhitelesítő eszközök kezelése az alapértelmezett hitelesítők megváltoztatásával történik az első használat előtt
50.		K08.021_O.8.21.6	a rendszerhitelesítő eszközök kezelése a K08.021_P[1] által meghatározott időszakának hitelesítőtípusonkénti megváltoztatásával vagy frissítésével, illetve a K08.021_P[2] által meghatározott események bekövetkezésekor történik
51.		K08.021_O.8.21.7	a rendszer hitelesítő eszközeinek kezelése a hitelesítő tartalmának a jogosulatlan nyilvánosságra hozataltól és módosítástól való védelme biztosítása mellett történik
52.		K08.021_O.8.21.8.(a)	a rendszerhitelesítő eszközök kezelése azáltal történik, hogy az egyéneknek meghatározott védelmi intézkedéseket kell végrehajtaniuk a hitelesítő eszközök védelme érdekében
53.		K08.021_O.8.21.8.(b)	a rendszerhitelesítő eszközök kezelése során az eszközök védelme garantált
54.		K08.021_O.8.21.9	a rendszerhitelesítő eszközök kezelése a csoport- vagy szerepkörfiókok hitelesítőinek megváltoztatásával történik, amikor a fiókok tagsága megváltozik
55.	8.22. A hitelesítésre szolgáló eszközök kezelése – Jelszó alapú hitelesítés	K08.022_P[1]	meghatározásra került, hogy milyen gyakorisággal kell frissíteni a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját
56.		K08.022_P[2]	a hitelesítők összetételére és komplexitására vonatkozó szabályok meghatározásra kerültek
57.		K08.022_O.8.22.1	jelszóalapú hitelesítés esetén a K08.022_P[1] által meghatározott gyakorisággal és a szervezeti jelszavak közvetlen vagy közvetett kompromittálódásának gyanúja esetén a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját vezetik és frissítik
58.		K08.022_O.8.22.2	jelszóalapú hitelesítés esetén, amikor a jelszavakat a felhasználók hozzák létre vagy frissítik, ellenőrizni kell, hogy a jelszavak nem szerepelnek a K08.022_O.8.22.1 pontban szereplő, gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján
59.		K08.022_O.8.22.3	jelszóalapú hitelesítés esetén a jelszavak csak kriptográfiailag védett csatornákon keresztül kerülnek továbbításra
60.		K08.022_O.8.22.4	jelszóalapú hitelesítés esetén a jelszavak tárolása jóváhagyott sózott kulcsszármaztatási függvény, lehetőleg egykulcsos hash használatával történik
61.		K08.022_O.8.22.5	jelszóalapú hitelesítés esetén a fiók helyreállításakor azonnal új jelszót kell választani
62.		K08.022_O.8.22.6	jelszóalapú hitelesítés esetén a felhasználó hosszú jelszavakat és jelszókifejezéseket választhat, beleértve a szóközöket és az összes nyomtatható karaktert
63.		K08.022_O.8.22.7	jelszóalapú hitelesítés esetén automatizált eszközöket alkalmaznak, amelyek segítik a felhasználót az erős jelszavak kiválasztásában

64.		K08.022_O.8.22.8	jelszóalapú hitelesítés esetén K08.022_P[2] által meghatározott összetételi és komplexitási szabályok érvényesülnek
65.	8.23. A hitelesítésre szolgáló eszközök kezelése – Nyilvános kulcs alapú hitelesítés	K08.023_O.8.23.1.1	a nyilvános kulcs alapú hitelesítés esetén a megfelelő privát kulcshoz való jogosultságot kell érvényesíteni
66.		K08.023_O.8.23.1.2	a hitelesített személyazonosságot a nyilvános kulcs alapú hitelesítéshez az egyén vagy a csoport fiókjához rendelik hozzá
67.		K08.023_O.8.23.1.3	ha nyilvános kulcsú infrastruktúrát (PKI) használnak, a tanúsítványok hitelesítésére egy elfogadott megbízható pontig tartó tanúsítványlánc létrehozásával és ellenőrzésével kerül sor, beleértve a tanúsítványok állapotára vonatkozó információk ellenőrzését is
68.		K08.023_O.8.23.1.4	ha nem nyilvános kulcsú infrastruktúrát (PKI) használnak, a visszavonási adatok helyi tárolását kell létrehozni a tanúsítványlánc felépítésének és ellenőrzésének támogatására
69.	8.25. A hitelesítésre szolgáló eszközök kezelése – A hitelesítő eszközök védelme	K08.025_O.8.25	a hitelesítő eszközök védelme annak az információnak a biztonsági besorolásával arányos, amelyhez a hitelesítők használata hozzáférést biztosít
70.	8.36. Hitelesítési információk visszajelzésének elrejtése	K08.036_O.8.36	a hitelesítési információk visszajelzését a hitelesítési folyamat során elrejtik, hogy megvédjék az információkat a jogosulatlan személyek általi esetleges felfedéstől és felhasználástól
71.	8.37. Hitelesítés kriptográfiai modul esetén	K08.037_O.8.37	a kriptográfiai modul hitelesítésére olyan mechanizmusokat alkalmaznak, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának, a jogszabályoknak, a végrehajtási utasításoknak, szabályzatoknak, szabványoknak
72.	8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	K08.038_O.8.38	a nem szervezeti felhasználók vagy a nem szervezeti felhasználók nevében eljáró folyamatok egyedi azonosítása és hitelesítése megtörténik
73.	8.39. Azonosítás és hitelesítés (szervezeten kívüli felhasználók) – Meghatározott azonosítási profilok használata	K08.039_P[1]	az azonosításkezelési profilok meghatározottak
74.		K08.039_O.8.39	a személyazonosság-kezelés megfelel a K08.039_P[1] által meghatározott személyazonosság-kezelési profiloknak
75.	8.43. Újrahitelesítés	K08.043_P[1]	az újbóli hitelesítést igénylő körülmények vagy helyzetek meghatározásra kerültek
76.		K08.043_O.8.43	a felhasználóknak újra kell hitelesíteniük magukat a K08.043_P[1] által meghatározott körülmények vagy helyzetek bekövetkezése esetén
77.	8.44. Személyazonosság igazolása	K08.044_O.8.44.1	azok a felhasználók, akiknek a rendszerekhez való logikai hozzáféréshez a vonatkozó szabványokban vagy irányelvekben meghatározott megfelelő személyazonosság-biztosítási szintű követelményeken alapuló fiókokra van szükségük, a személyazonosságot igazolják
78.		K08.044_O.8.44.2	a felhasználói azonosítók egyedi személyhez vannak hozzárendelve
79.		K08.044_O.8.44.3.(a)	a személyazonosságra vonatkozó bizonyítékok összegyűjtése megtörtént
80.		K08.044_O.8.44.3.(b)	a személyazonosságra vonatkozó bizonyítékokat hitelesítik
81.		K08.044_O.8.44.3.(c)	a személyazonosságra vonatkozó bizonyítékokat ellenőrizték

82.	8.46. Személyazonosság igazolása – Személyazonosság bizonyítéka	K08.046_O.8.46	a személyi azonosítást igazoló bizonyítékot bemutatása a fiókok regisztrációját végző szerv felé előírt
83.	8.47. Személyazonosság igazolása – Személyazonossági bizonyítékok hitelesítése és ellenőrzése	K08.047_P[1]	a személyazonossági bizonyítékok hitelesítésének és ellenőrzésének módszereit meghatározták
84.		K08.047_O.8.47	a bemutatott személyazonossági bizonyítékokat a K08.047_P[1] által meghatározott hitelesítési és ellenőrzési módszerekkel validálják és ellenőrzik
85.	8.48. Személyazonosság igazolása – Személyes jelenlét melletti hitelesítés és ellenőrzés	K08.048_O.8.48	a személyazonosságot igazoló bizonyítékok hitelesítését és ellenőrzését személyesen, a fiókok regisztrációját végző szerv előtt végzik
86.	8.49. Személyazonosság igazolása – Cím megerősítése	K08.049_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy került kiválasztásra: {regisztrációs kód; megerősítő értesítés}
87.		K08.049_O.8.49	a K08.049_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK egy másodlagos csatornán keresztül kerülnek kézbesítésre a felhasználó fizikai vagy elektronikus nyilvántartott címének ellenőrzésére

9. Biztonsági események kezelése

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	9.1. Szabályzat és eljárásrendek	K09.001_P[1]	meghatározásra kerültek azok a személyek vagy szerepkörök, akikkel a biztonsági eseménykezelési szabályzatot meg kell ismertetni
3.		K09.001_P[2]	meghatározásra kerültek azok a személyek vagy szerepkörök, akikkel a biztonsági eseménykezelési eljárásokat meg kell ismertetni
4.		K09.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K09.001_P[4]	a biztonsági eseménykezelési szabályzat és eljárások irányítására egy meghatározott személy került kijelölésre
6.		K09.001_P[5]	az eseménykezelési szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K09.001_P[6]	meghatározták azokat az eseményeket, amelyek a biztonsági eseménykezelési szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K09.001_P[7]	meghatározták az eseménykezelési eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K09.001_P[8]	meghatározzák azokat az eseményeket, amelyek miatt a biztonsági eseménykezelési eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K09.001_O_9.1.1.(a)	a biztonsági eseménykezelési szabályzatot kidolgozták ki és dokumentálták

11.		K09.001_O_9.1.1.(b)	a biztonsági eseménykezelési szabályzat megismertetésre került a K09.001_P[1] által meghatározott személyekkel vagy szerepkörökkel körében
12.		K09.001_O_9.1.1.(c)	a biztonsági eseménykezelési szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő eseménykezelési eljárások kidolgozásra és dokumentálásra kerültek
13.		K09.001_O_9.1.1.(d)	a biztonsági eseménykezelési eljárások megismertetésre kerültek a K09.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K09.001_O_9.1.2	a K09.001_P[4] által meghatározott személyt kijelölték az eseménykezelési szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítására
15.		K09.001_O_9.1.3.(a)	a biztonsági eseménykezelési szabályzatot felülvizsgálják és frissítik a K09.001_P[5] által meghatározott gyakorisággal
16.		K09.001_O_9.1.3.(b)	a biztonsági eseménykezelési szabályzatot felülvizsgálják és frissítik a K09.001_P[6] által meghatározott eseményeket követően
17.		K09.001_O_9.1.3.(c)	a biztonsági eseménykezelési eljárásokat felülvizsgálják és frissítik a K09.001_P[7] által meghatározott gyakorisággal
18.		K09.001_O_9.1.3.(d)	a biztonsági eseménykezelési eljárásokat felülvizsgálják és frissítik a K09.001_P[8] által meghatározott eseményeket követően
19.		K09.001_O_9.1.1.1.1.(a)	a biztonsági eseménykezelési szabályzat céljának meghatározása a K09.001_P[3] által meghatározottak szerint megtörtént
20.		K09.001_O_9.1.1.1.1.(b)	a biztonsági eseménykezelési szabályzat hatályának meghatározása a K09.001_P[3] által meghatározottak szerint megtörtént
21.		K09.001_O_9.1.1.1.1.(c)	meghatározták a biztonsági eseménykezelési szabályzathoz kapcsolódó szerepköröket a K09.001_P[3] szerinti szinteken
22.		K09.001_O_9.1.1.1.1.(d)	a biztonsági eseménykezelési szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K09.001_P[3] által meghatározottak szerint
23.		K09.001_O_9.1.1.1.1.(e)	a biztonsági eseménykezelési szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K09.001_P[3] által meghatározottak szerint
24.		K09.001_O_9.1.1.1.1.(f)	a biztonsági eseménykezelési szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K09.001_P[3] által meghatározottak szerint
25.		K09.001_O_9.1.1.1.1.(g)	a biztonsági eseménykezelési szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K09.001_P[3] által meghatározottak szerint
26.		K09.001_O_9.1.1.1.2.	a biztonsági eseménykezelési szabályzat összhangja a vonatkozó jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal megteremtésre került

27.	9.2. Képzés a biztonsági események kezelésére	K09.002_P[1]	meghatározták azt az időtartamot, amelyen belül eseménykezelési képzést kell biztosítani az eseményre reagáló szerepet vagy felelősséget betöltő rendszerhasználóknak
28.		K09.002_P[2]	meghatározták, hogy milyen gyakorisággal kell a felhasználóknak eseménykezelési képzést tartani
29.		K09.002_P[3]	meghatározták, hogy milyen gyakorisággal kell felülvizsgálni és frissíteni az eseménykezelési képzés tartalmát
30.		K09.002_P[4]	meghatározták azokat az eseményeket, amelyek miatt az eseménykezelési képzés tartalmának felülvizsgálatát kell kezdeményezni
31.		K09.002_O.9.2.1.1	a rendszerfelhasználók a K09.002_P[1] által meghatározott időtartamon belül az eseménykezelési szerepkör vagy felelősség átvételétől, illetve a rendszerhez való hozzáférés megszerzésétől számított, K09.002_P[1] szerinti időn belül a kiosztott szerepköröknek és felelősségi köröknek megfelelő eseménykezelési képzést kapnak
32.		K09.002_O.9.2.1.2	a rendszerfelhasználók számára a kijelölt szerepkörökkel és felelősségi körökkel összhangban álló eseménykezelési képzés biztosított, ha a rendszerváltozások ezt megkövetelik
33.		K09.002_O.9.2.1.3	a rendszerhasználók számára a kijelölt szerepkörökkel és felelősségi körökkel összhangban álló eseménykezelési képzés biztosított a K09.002_P[2] által meghatározott gyakorisággal
34.		K09.002_O.9.2.2.(a)	az eseménykezelési képzés tartalmát felülvizsgálják és frissítik a K09.002_P[3] által meghatározott gyakorisággal
35.		K09.002_O.9.2.2.(b)	a K09.002_P[4] által meghatározott eseményeket követően felülvizsgálják és frissítik az eseménykezelési képzés tartalmát
36.	9.3. Képzés a biztonsági események kezelésére – Szimulált események	K09.003_O.9.3	a szervezet szimulált eseményeket épít be az események kezelésére vonatkozó képzésbe, hogy elősegítse a személyzet számára a válsághelyzetekben szükséges reagálást
37.	9.4. Képzés a biztonsági események kezelésére – Automatizált képzési környezet	K09.004_P[1]	meghatározták az eseménykezelési képzési környezetben használt automatizált mechanizmusokat
38.		K09.004_O.9.4	a K09.004_P[1] által meghatározott automatizált mechanizmusok felhasználásával a valósághű eseménykezelési képzési környezet biztosított
39.	9.5. Biztonsági események kezelésének tesztelése	K09.005_P[1]	meghatározták azt a gyakoriságot, amellyel a szervezet eseménykezelési képességének hatékonyságát tesztelni kell
40.		K09.005_P[2]	meghatározták a szervezet eseménykezelési képessége hatékonyságának tesztelésére használt módszereket
41.		K09.005_O.9.5	a rendszer eseménykezelési képességének hatékonyságát a K09.005_P[1] által meghatározott gyakorisággal a K09.005_P[2] által meghatározott tesztekkel vizsgálják
42.	9.7. Biztonsági események kezelésének tesztelése – Összehangolás a kapcsolódó tervekkel	K09.007_O.9.7	az eseménykezelés tesztelése összehangolásra került a kapcsolódó tervekért felelős szervezeti egységekkel
43.	9.9. Biztonsági események kezelése	K09.009_O.9.9.2.(a)	az események kezelésére az eseménykezelési tervvel összhangban lévő eseménykezelési képességek kerültek kialakításra

44.		K09.009_O.9.9.2.(b)	az eseménykezelési képesség az eseményekre való felkészülést is magában foglalja
45.		K09.009_O.9.9.2.(c)	az eseménykezelési képesség magában foglalja az események észlelését és elemzését
46.		K09.009_O.9.9.2.(d)	az eseménykezelési képesség magában foglalja az események elszigetelését
47.		K09.009_O.9.9.2.(e)	az eseménykezelési képesség magában foglalja az események felszámolását
48.		K09.009_O.9.9.2.(f)	az eseménykezelési képesség magában foglalja a helyreállítást
49.		K09.009_O.9.9.3	az eseménykezelési tevékenységeket összehangolták az üzletmenet-folytonossági tervezési tevékenységekkel
50.		K09.009_O.9.9.4.(a)	a folyamatban lévő eseménykezelési tevékenységekből levont tanulságokat beépítik az eseménykezelési eljárásokba, a képzésbe és a tesztelésbe
51.		K09.009_O.9.9.4.(b)	a beépített tanulságokból eredő változtatásokat annak megfelelően hajtják végre
52.		K09.009_O.9.9.5.	az eseménykezelési tevékenységek összehasonlíthatóak és kiszámíthatóak az egész szervezeten belül
53.	9.10. Biztonsági események kezelése – Automatizált eseménykezelő folyamatok	K09.010_P[1]	meghatározták az eseménykezelési folyamat támogatására használt automatizált mechanizmusokat
54.		K09.010_O.9.10	az eseménykezelési folyamatot a K09.010_P[1] által meghatározott automatizált mechanizmusok támogatják
55.	9.13. Biztonsági események kezelése – Információk korrelációja	K09.013_O.9.13	a biztonsági eseményekre vonatkozó információk és a szervezet egyéb releváns információi korreláltak
56.	9.20. Biztonsági események kezelése – Integrált eseménykezelő csoport	K09.020_P[1]	meghatározták azt az időtartamot, amelyen belül egy integrált eseménykezelő csoport bevethető
57.		K09.020_O.9.20.(a)	a szervezet integrált eseménykezelő csoportot hozott létre és tart fenn
58.		K09.020_O.9.20.(b)	az integrált eseménykezelő csoport a K09.020_P[1] által meghatározott időtartamon belül a szervezet által meghatározott bármely helyszínen bevethető
59.	9.25. A biztonsági események nyomonkövetése	K09.025_O.9.25.(a)	a biztonsági eseményeket nyomon követik
60.		K09.025_O.9.25.(b)	a biztonsági eseményeket dokumentálják
61.	9.26. A biztonsági események nyomonkövetése – Automatizált nyomon követés, adatgyűjtés és elemzés	K09.026_P[1]	meghatározottak az események nyomon követésére használt automatizált mechanizmusok
62.		K09.026_P[2]	meghatározottak az eseményekkel kapcsolatos információk gyűjtésére használt automatizált mechanizmusok
63.		K09.026_P[3]	meghatározottak az események vizsgálatára használt automatizált mechanizmusok
64.		K09.026_O.9.26.(a)	az eseményeket a K09.026_P[1] által meghatározott automatizált mechanizmusok segítségével követik nyomon
65.		K09.026_O.9.26.(b)	az eseményekkel kapcsolatos információkat a K09.026_P[2] által meghatározott automatizált mechanizmusok segítségével gyűjtik
66.		K09.026_O.9.26.(c)	az eseményeket a K09.026_P[3] által meghatározott automatizált mechanizmusok segítségével vizsgálják

67.	9.27. A biztonsági események jelentése	K09.027_O.9.27.1	a személyzet jelentéstételre való kötelezése megtörtént belső szabályozóval a biztonsági esemény gyanúja vagy bekövetkezése esetére
68.		K09.027_O.9.27.2 (a)	a korábban bekövetkezett biztonsági események bejelentése a jogszabályokban foglalt szervezetek felé megtörtént
69.		K09.027_O.9.27.2 (b)	a korábban bekövetkezett biztonsági események bejelentése a jogszabályokban foglalt határidőben megtörtént
70.	9.28. A biztonsági események jelentése – Automatizált jelentés	K09.028_P[1]	meghatározottak az események bejelentésére használt automatizált mechanizmusok
71.		K09.028_O.9.28	az események a K09.028_P[1] által meghatározott automatizált mechanizmusok segítségével kerülnek bejelentésre
72.	9.30. A biztonsági események jelentése – Ellátási lánc koordinációja	K09.030_O.9.30	az eseményre vonatkozó információkat a termék vagy szolgáltatás szállítója és az ellátási láncban vagy az ellátási lánc irányításában részt vevő más szervezetek kapják meg az eseménnyel kapcsolatos rendszerek vagy rendszerelemek tekintetében
73.	9.31. Segítségnyújtás a biztonsági események kezeléséhez	K09.031_O.9.31.(a)	a szervezet eseménykezelést támogató erőforrást biztosít a rendszerfelhasználók számára
74.		K09.031_O.9.31.(b)	a szervezet eseménybejelentést támogató megoldást biztosít a rendszerfelhasználók számára
75.	9.32. Segítségnyújtás biztonsági események kezeléséhez – Automatizált támogatás az információk és a támogatás elérhetőségéhez	K09.032_P[1]	az eseményekre adott információk és a támogatás hozzáférhetőségének növelésére használt automatizált mechanizmusok meghatározásra kerültek
76.		K09.032_O.9.32	a K09.032_P[1] által meghatározott automatizált mechanizmusok segítségével növelik az eseményekre adott információk és a támogatás hozzáférhetőségét
77.	9.34. Biztonsági eseménykezelési terv	K09.034_P[1]	az eseménykezelési tervet felülvizsgáló és jóváhagyó személyek vagy szerepkörök meghatározásra kerültek
78.		K09.034_P[2]	meghatározták az eseménykezelési terv felülvizsgálatának és jóváhagyásának gyakoriságát
79.		K09.034_P[3]	az események kezeléséért felelős szervezetek, személyek vagy szerepkörök meghatározásra kerültek
80.		K09.034_P[4]	meghatározásra került az az eseménykezelő személyzet – név, illetve szerepkör szerint azonosítva –, amellyel az eseménykezelési tervet meg kell ismertetni
81.		K09.034_P[5]	meghatározták azokat a szervezeti egységeket, amelyekkel az eseménykezelési tervet meg kell ismertetni
82.		K09.034_P[6]	meghatározták azt az eseménykezelő személyzetet – név, illetve szerepkör szerint azonosítva –, amellyel az eseménykezelési terv változásait ismertetik
83.		K09.034_P[7]	meghatározták azokat a szervezeti egységeket, amelyekkel az eseménykezelési terv változásait ismertetik
84.		K09.034_O.9.34.1.1	eseménykezelési tervet dolgoztak ki, amely iránymutatást biztosít a szervezet számára az eseménykezelési képesség megvalósításához
85.		K09.034_O.9.34.1.2	eseménykezelési tervet dolgoztak ki, amely leírja az eseménykezelési képesség struktúráját és szervezetét
86.		K09.034_O.9.34.1.3	eseménykezelési tervet dolgoztak ki, amely átfogó megközelítést biztosít arra vonatkozóan, hogy az eseménykezelési képesség hogyan illeszkedik a szervezeti struktúrába

87.		K09.034_O.9.34.1.4	eseménykezelési tervet dolgoztak ki, amely megfelel a szervezet egyedi igényeinek a feladatkör, a méret, a szervezeti felépítés és a funkciók tekintetében
88.		K09.034_O.9.34.1.5	eseménykezelési tervet dolgoztak ki, amely meghatározza a bejelentendő eseményeket
89.		K09.034_O.9.34.1.6	eseménykezelési tervet dolgoznak ki, amely metrikákat biztosít a szervezeten belüli eseménykezelési képesség mérésére
90.		K09.034_O.9.34.1.7	eseménykezelési tervet dolgoznak ki, amely meghatározza az eseménykezelési képesség hatékony fenntartásához és kiépítéséhez szükséges erőforrásokat és vezetői támogatást
91.		K09.034_O.9.34.1.8	eseménykezelési tervet dolgoznak ki, amely foglalkozik az eseménnyel kapcsolatos információk megosztásával
92.		K09.034_O.9.34.1.9	a K09.034_P[1] által meghatározott személyek és szerepkörök a K09.034_P[2] által meghatározott gyakorisággal felülvizsgálják és jóváhagyják az eseménykezelési tervet
93.		K09.034_O.9.34.1.10	eseménykezelési tervet dolgoztak ki, amely meghatározza a K09.034_P[3] által meghatározott szervezetek, személyek és szerepkörök felelősségét az események kezeléséért
94.		K09.034_O.9.34.2.(a)	a K09.034_P[4] által meghatározott személyzettel megismertették az eseménykezelési tervet
95.		K09.034_O.9.34.2.(b)	a K09.034_P[5] által meghatározott szervezeti egységekkel megismertették az eseménykezelési tervet
96.		K09.034_O.9.34.3	az eseménykezelési tervet frissítik a rendszer és a szervezeti változások vagy a terv megvalósítása, végrehajtása vagy tesztelése során felmerült problémák kezelése érdekében
97.		K09.034_O.9.34.4.(a)	az eseménykezelési terv változásait ismertették a K09.034_P[6] által meghatározott eseménykezelő személyzettel
98.		K09.034_O.9.34.4.(b)	az eseménykezelési terv változásait ismertették a K09.034_P[7] által meghatározott szervezeti egységekkel
99.		K09.034_O.9.34.5.(a)	az eseménykezelési terv védett a jogosulatlan megismeréssel szemben
100.		K09.034_O.9.34.5.(b)	az eseménykezelési terv védett a jogosulatlan módosítással szemben

10. Karbantartás

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	10.1. Szabályzat és eljárásrendek	K10.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a karbantartási szabályzatot meg kell ismertetni
3.		K10.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a karbantartási eljárásokat meg kell ismertetni
4.		K10.001_P[3]	meghatározott, hogy a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}

5.		K10.001_P[4]	meghatározott a karbantartási szabályzat és eljárások irányítására kijelölt személy
6.		K10.001_P[5]	a karbantartási szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K10.001_P[6]	meghatározták azokat az eseményeket, amelyek a karbantartási szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K10.001_P[7]	meghatározták a karbantartási eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K10.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a karbantartási eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K10.001_O_10.1.1.(a)	karbantartási szabályzatot dolgoztak ki és dokumentáltak
11.		K10.001_O_10.1.1.(b)	a karbantartási szabályzatot megismertették a K10.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K10.001_O_10.1.1.(c)	a karbantartási szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő karbantartási eljárások kidolgozása és dokumentálása megtörtént
13.		K10.001_O_10.1.1.(d)	a karbantartási eljárások megismertetése megtörtént a K10.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K10.001_O_10.1.2	megtörtént a K10.001_P[4] által meghatározott személy kijelölése a karbantartási szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítására
15.		K10.001_O_10.1.3.(a)	a karbantartási szabályzatot felülvizsgálják és frissítik a K10.001_P[5] által meghatározott gyakorisággal
16.		K10.001_O_10.1.3.(b)	a karbantartási szabályzatot felülvizsgálják és frissítik a K10.001_P[6] által meghatározott eseményeket követően
17.		K10.001_O_10.1.3.(c)	a karbantartási eljárásokat felülvizsgálják és frissítik a K10.001_P[7] által meghatározott gyakorisággal
18.		K10.001_O_10.1.3.(d)	a karbantartási eljárásokat felülvizsgálják és frissítik a K10.001_P[8] által meghatározott eseményeket követően
19.		K10.001_O_10.1.1.1.1.(a)	a karbantartási szabályzat célja meghatározott a K10.001_P[3] szerint
20.		K10.001_O_10.1.1.1.1.(b)	a karbantartási szabályzat hatálya meghatározott a K10.001_P[3] szerint
21.		K10.001_O_10.1.1.1.1.(c)	a karbantartási szabályzathoz kapcsolódó szerepkörök meghatározottak a K10.001_P[3] szerint
22.		K10.001_O_10.1.1.1.1.(d)	a karbantartási szabályzathoz kapcsolódó felelősségek meghatározottak a K10.001_P[3] szerint
23.		K10.001_O_10.1.1.1.1.(e)	a karbantartási szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K10.001_P[3] szerint
24.		K10.001_O_10.1.1.1.1.(f)	a karbantartási szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározott a K10.001_P[3] szerint
25.		K10.001_O_10.1.1.1.1.(g)	a karbantartási szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározottak a K10.001_P[3] szerint

26.		K10.001_O_10.1.1.1.2.	a karbantartási szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	10.2. Szabályozott karbantartás	K10.002_P[1]	a rendszer vagy rendszerelemek szervezeti létesítményekből külső karbantartás vagy javítás céljából történő elszállításának kifejezett jóváhagyására jogosult személyek vagy szerepkörök meghatározottak
28.		K10.002_P[2]	meghatározták a kapcsolódó adathordozókról a szervezeti létesítményekből helyszíni karbantartás, javítás vagy csere céljából történő eltávolítás előtt eltávolítandó információkat
29.		K10.002_P[3]	meghatározták a szervezeti karbantartási nyilvántartásokban feltüntetendő információkat
30.		K10.002_O.10.2.1.(a)	a rendszerelemek karbantartását, javítását és cseréjét a gyártó vagy a szállító előírásainak, illetve a szervezeti követelményeknek megfelelően ütemezik
31.		K10.002_O.10.2.1.(b)	a rendszerelemek karbantartását, javítását és cseréjét a gyártó vagy a szállító előírásainak, illetve a szervezeti követelményeknek megfelelően dokumentálják
32.		K10.002_O.10.2.1.(c)	a rendszerelemek karbantartását, javítását és cseréjét a gyártó vagy a szállító előírásainak, illetve a szervezeti követelményeknek megfelelően felülvizsgálják
33.		K10.002_O.10.2.2.(a)	minden karbantartási tevékenység jóváhagyásra került, függetlenül attól, hogy azt a helyszínen vagy távolról végezték el, és függetlenül attól, hogy a rendszert vagy a rendszerelemeket a helyszínen szervizelték vagy más helyre szállították
34.		K10.002_O.10.2.2.(b)	minden karbantartási tevékenység ellenőrizése biztosított, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a rendszert vagy a rendszerelemeket a helyszínen szervizelik vagy más helyre szállítják
35.		K10.002_O.10.2.3	a K10.002_P[1] által meghatározott személyek vagy szerepkörök által jóváhagyásra kerül a rendszer vagy rendszerelemek elszállítása a szervezeti létesítményekből külső karbantartás, javítás vagy csere céljából
36.		K10.002_O.10.2.4	az adathordozókról biztonságosan törlik a K10.002_P[2] által meghatározott információkat, mielőtt azokat elszállítják a szervezeti létesítményekből helyszíni karbantartás, javítás vagy csere céljából
37.		K10.002_O.10.2.5	minden potenciálisan érintett védelmi intézkedés ellenőrzése megvalósul, ami biztosítja, hogy a karbantartást, javítást vagy cserét követően a védelmi intézkedések továbbra is megfelelően működjenek
38.		K10.002_O.10.2.6	a K10.002_P[3] által meghatározott információkat a szervezeti karbantartási nyilvántartások tartalmazzák
39.	10.3. Rendszeres karbantartás – Automatizált karbantartási tevékenységek	K10.003_P[1]	meghatározottak a rendszer karbantartásának, javításának és cseréjének ütemezésére használt automatizált mechanizmusok
40.		K10.003_P[2]	meghatározottak a rendszer karbantartásának, javításának és cseréjének lefolytatására használt automatizált mechanizmusok
41.		K10.003_P[3]	meghatározottak a rendszer karbantartásának, javításának és cseréjének dokumentálására használt automatizált mechanizmusok

42.		K10.003_O.10.3.1.(a)	a K10.003_P[1] által meghatározott automatizált mechanizmusokat alkalmazzák a rendszer karbantartásának, javításának és cseréjének ütemezésére
43.		K10.003_O.10.3.1.(b)	a K10.003_P[2] által meghatározott automatizált mechanizmusokat alkalmazzák a rendszer karbantartásának, javításának és cseréjének lefolytatására
44.		K10.003_O.10.3.1.(c)	a K10.003_P[3] által meghatározott automatizált mechanizmusokat alkalmazzák a rendszer karbantartásának, javításának és cseréjének dokumentálására
45.		K10.003_O.10.3.2.(a)	a szervezet naprakész, pontos és teljes nyilvántartást vezet az összes igényelt, ütemezett, folyamatban lévő és befejezett karbantartási tevékenységről
46.		K10.003_O.10.3.2.(b)	a szervezet naprakész, pontos és teljes nyilvántartást vezet az összes igényelt, ütemezett, folyamatban lévő és befejezett javítási tevékenységről
47.	10.4. Karbantartási eszközök	K10.004_P[1]	meghatározott a korábban jóváhagyott rendszerkarbantartási eszközök felülvizsgálatának gyakorisága
48.		K10.004_O.10.4.1.(a)	a rendszerkarbantartási eszközök használata jóváhagyott
49.		K10.004_O.10.4.1.(b)	a rendszerkarbantartási eszközök használata nyilvántartott
50.		K10.004_O.10.4.1.(c)	a rendszerkarbantartási eszközök használata ellenőrzött
51.		K10.004_O.10.4.2	a korábban jóváhagyott rendszerkarbantartási eszközöket felülvizsgálják a K10.004_P[1] által meghatározott gyakorisággal
52.	10.5. Karbantartási eszközök – Eszközök vizsgálata	K10.005_O.10.5	a karbantartó személyzet által használt karbantartó eszközöket ellenőrzik a nem megfelelő vagy nem engedélyezett módosítások tekintetében
53.	10.6. Karbantartási eszközök – Adathordozók vizsgálata	K10.006_O.10.6	a diagnosztikai és tesztprogramokat tartalmazó adathordozókat kártékony kódok szempontjából ellenőrzik, mielőtt az adathordozókat a rendszerben használják
54.	10.7. Karbantartási eszközök – Jogosulatlan elszállítás megakadályozása	K10.007_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akik engedélyezhetik a berendezések elszállítását a létesítményből
55.		K10.007_O.10.7.1	a szervezeti információkat tartalmazó karbantartó eszközök elszállítását megelőzően ellenőrzik, hogy a berendezésen nincsenek szervezeti információk
56.		K10.007_O.10.7.2	a szervezeti információkat tartalmazó karbantartó eszközök elszállítását megelőzően a berendezéseket biztonságosan törlik vagy megsemmisítik
57.		K10.007_O.10.7.3	szervezeti információkat tartalmazó karbantartó eszközök csak szervezeti létesítményen belül helyezhetőek el
58.		K10.007_O.10.7.4	a szervezeti információkat tartalmazó karbantartó eszközök elszállítása a K10.007_P[1] által meghatározott személyektől vagy a berendezés létesítményből való eltávolítása kifejezetten engedélyező szerepköröktől kapott jóváhagyást követően valósul meg

59.	10.11. Távoli karbantartás	K10.011_O.10.11.1.(a)	a távoli karbantartási és diagnosztikai tevékenységeket jóváhagyják
60.		K10.011_O.10.11.1.(b)	a távoli karbantartási és diagnosztikai tevékenységeket nyomon követik
61.		K10.011_O.10.11.2.(a)	a távoli karbantartási és diagnosztikai eszközök használata csak a szervezeti szabályokkal összhangban engedélyezett
62.		K10.011_O.10.11.2.(b)	a távoli karbantartási és diagnosztikai eszközök használata dokumentálva van a rendszer biztonsági tervében
63.		K10.011_O.10.11.3	erős hitelesítést alkalmaznak a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásakor
64.		K10.011_O.10.11.4	a távoli karbantartási és diagnosztikai tevékenységekről nyilvántartást vezetnek
65.		K10.011_O.10.11.5.(a)	a munkaszakaszok a távoli karbantartás befejezésekor megszűnnek
66.		K10.011_O.10.11.5.(b)	a hálózati kapcsolatok a távoli karbantartás befejezésekor megszűnnek
67.	10.13. Távoli karbantartás – Azonos szintű biztonság és adattörlés	K10.013_O.10.13.1.(a)	a távoli karbantartási javításokat olyan rendszerből végzik, amely a karbantartott rendszerben alkalmazott képességhez hasonló biztonsági képességet valósít meg
68.		K10.013_O.10.13.1.(b)	a távoli diagnosztikai javításokat olyan rendszerből végzik, amely a karbantartott rendszerben alkalmazott képességhez hasonló biztonsági képességet valósít meg
69.		K10.013_O.10.13.2.(a)	a karbantartandó elemet a távoli karbantartási vagy diagnosztikai javítások előtt leválasztják az EIR-ről
70.		K10.013_O.10.13.2.(b)	a karbantartandó elemről a szervezeti információk törlésre kerülnek
71.		K10.013_O.10.13.2.(c)	a rendszerelemet a karbantartás elvégzése után és az elemnek a rendszerhez való újbóli csatlakoztatása előtt átvizsgálják a potenciálisan kártékony szoftverek észlelése érdekében
72.	10.18. Karbantartó személyek	K10.018_O.10.18.1.(a)	a karbantartó személyzet hozzáféréseinek kezelésére eljárás került kidolgozásra
73.		K10.018_O.10.18.1.(b)	a szervezet nyilvántartást vezet az engedélyezett karbantartó szervezetekről vagy személyekről
74.		K10.018_O.10.18.2	az EIR-en karbantartást végző, kísérő nélküli személyek rendelkeznek a szükséges hozzáférési jogosultságokkal
75.		K10.018_O.10.18.3	a szükséges hozzáférési jogosultsággal nem rendelkező személyek karbantartási tevékenységeinek felügyeletét a szükséges hozzáférési jogosultsággal és műszaki szakértelemmel rendelkező szervezeti személyek látják el
76.	10.19. Karbantartó személyek – Nem megfelelő ellenőrzöttségű személyek	K10.019_P[1]	meghatározták azokat az alternatív eljárásokat, amelyeket arra az esetre kell kidolgozni és végrehajtani, ha egy rendszerelemet nem lehet biztonságosan törölni, eltávolítani vagy leválasztani a rendszerről
77.		K10.019_O.10.19.1.1	megfelelő hozzáférési jogosultságokkal nem rendelkező karbantartó személyek alkalmazására vonatkozóan eljárásokat hajtanak végre, és a karbantartási és diagnosztikai tevékenységek végzése során a szükséges hozzáférési jogosultsággal nem rendelkező karbantartó személyeket kísérő és felügyelő, teljes mértékben átvilágított, megfelelő hozzáférési jogosultsággal rendelkező és szakmailag képzett, jóváhagyott szervezeti személyzetet biztosítanak
78.		K10.019_O.10.19.1.2	megfelelő hozzáférési jogosultságokkal nem rendelkező karbantartó személyek alkalmazására vonatkozó eljárásokat hajtanak végre, amelyek magukban foglalják a rendszerben lévő összes adattároló törlését, valamint a karbantartási

			vagy diagnosztikai tevékenységek megkezdése előtt az összes adattároló eltávolítását vagy fizikai leválasztását a rendszerről
79.		K10.019_O.10.19.2	a K10.019_P[1] által meghatározott alternatív eljárásokat dolgoznak ki és hajtanak végre arra az esetre, ha egy rendszerelemet nem lehet törölni, eltávolítani vagy leválasztani az EIR-ről
80.	10.21. Kellő időben történő karbantartás	K10.021_P[1]	meghatározták azokat a rendszerelemeket, amelyekhez karbantartási támogatást, illetve pótalkatrészeket szereznek be
81.		K10.021_P[2]	meghatározták azt az időtartamot, amelyen belül a meghibásodást követően karbantartási támogatást, illetve pótalkatrészeket kell biztosítani
82.		K10.021_O.10.21	a K10.021_P[1] által meghatározott rendszerelemekhez meghibásodást követően a K10.021_P[2] által meghatározott időtartamon belül karbantartási támogatás, illetve pótalkatrészek biztosítottak

11. Adathordozók védelme

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	11.1. Szabályzat és eljárásrendek	K11.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel az adathordozók védelmére vonatkozó szabályzatot meg kell ismertetni
3.		K11.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel az adathordozók védelmére vonatkozó eljárásokat meg kell ismertetni
4.		K11.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K11.001_P[4]	az adathordozók védelmére vonatkozó szabályzat és eljárások irányítására egy meghatározott személyt jelöltek ki
6.		K11.001_P[5]	meghatározott az adathordozók védelmére vonatkozó szabályzat felülvizsgálatának és frissítésének gyakorisága
7.		K11.001_P[6]	meghatározottak azok az események, amelyek az adathordozók védelmére vonatkozó szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K11.001_P[7]	meghatározott az adathordozók védelmére vonatkozó eljárások felülvizsgálatának és frissítésének gyakorisága
9.		K11.001_P[8]	meghatározottak azok az események, amelyek miatt az adathordozók védelmére vonatkozó eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K11.001_O_11.1.1.(a)	az adathordozók védelmére vonatkozó szabályzatot dolgoztak ki és dokumentáltak

11.		K11.001_O_11.1.1.(b)	az adathordozók védelmére vonatkozó szabályzatot megismertették a K11.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K11.001_O_11.1.1.(c)	az adathordozók védelmére vonatkozó szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő adathordozók védelmére vonatkozó eljárások kidolgozása és dokumentálása megtörtént
13.		K11.001_O_11.1.1.(d)	az adathordozók védelmére vonatkozó eljárások megismertetése a K11.001_P[2] által meghatározott személyekkel vagy szerepkörökkel körében megtörtént
14.		K11.001_O_11.1.2	kijelölték a K11.001_P[4] által meghatározott személyt, aki az adathordozók védelmére vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítását végzi
15.		K11.001_O_11.1.3.(a)	az adathordozók védelmére vonatkozó szabályzatot felülvizsgálják és frissítik a K11.001_P[5] által meghatározott gyakorisággal
16.		K11.001_O_11.1.3.(b)	az adathordozók védelmére vonatkozó szabályzatot felülvizsgálják és frissítik a K11.001_P[6] által meghatározott eseményeket követően
17.		K11.001_O_11.1.3.(c)	az adathordozók védelmére vonatkozó eljárásokat felülvizsgálják és frissítik a K11.001_P[7] által meghatározott gyakorisággal
18.		K11.001_O_11.1.3.(d)	az adathordozók védelmére vonatkozó eljárásokat felülvizsgálják és frissítik a K11.001_P[8] által meghatározott eseményeket követően
19.		K11.001_O_11.1.1.1.1.(a)	az adathordozók védelmére vonatkozó szabályzat célja meghatározott a K11.001_P[3] szerint
20.		K11.001_O_11.1.1.1.1.(b)	az adathordozók védelmére vonatkozó szabályzat hatálya meghatározott a K11.001_P[3] szerint
21.		K11.001_O_11.1.1.1.1.(c)	az adathordozók védelmére vonatkozó szabályzathoz kapcsolódó szerepkörök meghatározottak a K11.001_P[3] szerint
22.		K11.001_O_11.1.1.1.1.(d)	az adathordozók védelmére vonatkozó szabályzathoz kapcsolódó felelősségek meghatározottak a K11.001_P[3] szerint
23.		K11.001_O_11.1.1.1.1.(e)	az adathordozók védelmére vonatkozó szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K11.001_P[3] szerint
24.		K11.001_O_11.1.1.1.1.(f)	az adathordozók védelmére vonatkozó szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés rögzített a K11.001_P[3] szerint
25.		K11.001_O_11.1.1.1.1.(g)	az adathordozók védelmére vonatkozó szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározottak a K11.001_P[3] szerint
26.		K11.001_O_11.1.1.1.2.	az adathordozók védelmére vonatkozó szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal

27.	11.2. Hozzáférés az adathordozókhoz	K11.002_P[1]	meghatározottak a digitális adathordozók azon típusai, amelyekhez a hozzáférés korlátozott
28.		K11.002_P[2]	meghatározottak a digitális adathordozókhoz való hozzáférésre jogosult személyek, illetve szerepkörök
29.		K11.002_P[3]	meghatározottak az analóg adathordozók azon típusai, amelyekhez a hozzáférés korlátozott
30.		K11.002_P[4]	meghatározottak az analóg adathordozókhoz való hozzáférésre jogosult személyek, illetve szerepkörök
31.		K11.002_O.11.2.(a)	a K11.002_P[1] által meghatározott típusú digitális adathordozókhoz való hozzáférés a K11.002_P[2] által meghatározott személyekre vagy szerepkörökre korlátozódik
32.		K11.002_O.11.2.(b)	a K11.002_P[3] által meghatározott típusú analóg adathordozókhoz való hozzáférés a K11.002_P[4] által meghatározott személyekre vagy szerepkörökre korlátozódik
33.	11.3. Adathordozók címkézése	K11.003_P[1]	meghatározottak az adathordozók azon típusai, amelyek mentesülnek a jelölés alól, ha ellenőrzött területeken maradnak
34.		K11.003_P[2]	meghatározottak azok az ellenőrzött területek, ahol az adathordozó mentesül a jelölés alól
35.		K11.003_O.11.3.1	az adathordozó jelöléssel van ellátva, amely jelzi a terjesztési korlátozásokat, a kezelési figyelmeztetéseket és az információkra vonatkozó biztonsági jelzéseket
36.		K11.003_O.11.3.2	a K11.003_P[1] által meghatározott jelölés alól mentesített adathordozó típusok a K11.003_P[2] által meghatározott ellenőrzött területeken belül maradnak
37.	11.4. Adathordozók tárolása	K11.004_P[1]	meghatározottak a fizikailag ellenőrizendő digitális adathordozók típusai
38.		K11.004_P[2]	meghatározottak a fizikailag ellenőrizendő analóg adathordozók típusai
39.		K11.004_P[3]	meghatározottak a biztonságosan tárolandó digitális adathordozók típusai
40.		K11.004_P[4]	meghatározottak a biztonságosan tárolandó analóg adathordozók típusai
41.		K11.004_P[5]	meghatározásra kerültek azok az ellenőrzött területek, ahol a digitális adathordozók biztonságos tárolása engedélyezett
42.		K11.004_P[6]	meghatározásra kerültek azok az ellenőrzött területek, ahol az analóg adathordozók biztonságos tárolása engedélyezett
43.		K11.004_O.11.4.1.(a)	a K11.004_P[1] által meghatározott digitális adathordozók típusait fizikailag ellenőrzik
44.		K11.004_O.11.4.1.(b)	a K11.004_P[2] által meghatározott analóg adathordozók típusait fizikailag ellenőrzik
45.		K11.004_O.11.4.1.(c)	a K11.004_P[3] által meghatározott digitális adathordozók típusait biztonságosan tárolják a K11.004_P[5] által meghatározott ellenőrzött területeken
46.		K11.004_O.11.4.1.(d)	a K11.004_P[4] által meghatározott analóg adathordozók típusait biztonságosan tárolják a K11.004_P[6] által meghatározott ellenőrzött területeken

47.		K11.004_O.11.4.2	a K11.004_P[1]-ben, a K11.004_P[2]-ben, a K11.004_P[3]-ban és a K11.004_P[4]-ben meghatározott adathordozó típusok védettek, amíg a hordozókat meg nem semmisítik vagy törlik jóváhagyott eszközök, technikák és eljárások alkalmazásával
48.	11.6. Adathordozók szállítása	K11.006_P[1]	meghatározottak az ellenőrzött területeken kívüli szállítás során védendő és ellenőrizendő adathordozók típusai
49.		K11.006_P[2]	meghatározottak az ellenőrzött területeken kívüli adathordozók védelmére használt védelmi intézkedések
50.		K11.006_P[3]	az ellenőrzött területeken kívül az adathordozók ellenőrzésére használt védelmi intézkedések meghatározottak
51.		K11.006_P[4]	meghatározottak az adathordozók szállításával kapcsolatos tevékenységekre jogosult személyek
52.		K11.006_O.11.6.1.(a)	a K11.006_P[1] által meghatározott típusú adathordozókat az ellenőrzött területeken kívüli szállítás során a K11.006_P[2] által meghatározott védelmi intézkedésekkel védik
53.		K11.006_O.11.6.1.(b)	a K11.006_P[1] által meghatározott típusú adathordozókat az ellenőrzött területeken kívüli szállítás során a K11.006_P[3] által meghatározott védelmi intézkedésekkel ellenőrzik
54.		K11.006_O.11.6.2	az adathordozók elszámoltathatósága az ellenőrzött területeken kívülre történő szállítás során is fennmarad
55.		K11.006_O.11.6.3	az adathordozók szállításával kapcsolatos tevékenységek dokumentáltak
56.		K11.006_O.11.6.4.	adathordozó szállításával kapcsolatos tevékenységet csak a K11.006_P[4] szerinti személyek végeznek
57.	11.8. Adathordozók törlése	K11.008_P[1]	meghatározásra kerültek a leselejtezés előtt törlendő adathordozók
58.		K11.008_P[2]	meghatározásra kerültek a szervezeti ellenőrzés alól történő kikerülés előtt törlendő adathordozók
59.		K11.008_P[3]	meghatározásra kerültek az újra felhasználás előtt törlendő adathordozók
60.		K11.008_P[4]	meghatározásra kerültek a leselejtezés előtti törlési technikák és eljárások
61.		K11.008_P[5]	meghatározásra kerültek a szervezeti ellenőrzés alól történő kikerülés előtti törlési technikák és eljárások
62.		K11.008_P[6]	meghatározásra kerültek az újra felhasználás előtt alkalmazandó törlési technikák és eljárások
63.		K11.008_O.11.8.1.(a)	a K11.008_P[1] által meghatározott adathordozókat a K11.008_P[4] által meghatározott törlési technikák és eljárások alkalmazásával törlik a leselejtezés előtt
64.		K11.008_O.11.8.1.(b)	a K11.008_P[2] által meghatározott adathordozókat a K11.008_P[5] által meghatározott törlési technikák és eljárások alkalmazásával törlik a szervezeti ellenőrzés alól történő kikerülés előtt
65.		K11.008_O.11.8.1.(c)	a K11.008_P[3] által meghatározott adathordozókat a K11.008_P[6] által meghatározott törlési technikák és eljárások alkalmazásával törlik az újra felhasználás előtt
66.		K11.008_O.11.8.2	az információ biztonsági kategóriájának vagy besorolásának megfelelő erősségű és sértetlenségű törlési mechanizmusokat alkalmaznak

67.	11.9. Adathordozók törlése – Felülvizsgálat, jóváhagyás, nyomon követés, dokumentálás és ellenőrzés	K11.009_O.11.9.(a)	az adathordozók törlésére és megsemmisítésére vonatkozó intézkedéseket felülvizsgálják
68.		K11.009_O.11.9.(b)	az adathordozók törlésére és megsemmisítésére vonatkozó intézkedések jóváhagyottak
69.		K11.009_O.11.9.(c)	az adathordozók törlésére és megsemmisítésére vonatkozó intézkedéseket nyomon követik
70.		K11.009_O.11.9.(d)	az adathordozók törlésére és megsemmisítésére vonatkozó intézkedéseket dokumentálják
71.		K11.009_O.11.9.(e)	az adathordozók törlésére és megsemmisítésére vonatkozó intézkedéseket ellenőrzik
72.	11.10. Adathordozók törlése – Berendezés tesztelése	K11.010_P[1]	meghatározták a törlési eszközök tesztelési gyakoriságát
73.		K11.010_P[2]	meghatározták a törlési eljárások tesztelési gyakoriságát
74.		K11.010_O.11.10.(a)	a törlési eszközöket a K11.010_P[1] által meghatározott gyakorisággal tesztelik annak biztosítása érdekében, hogy a tervezett törlés megvalósuljon
75.		K11.010_O.11.10.(b)	a törlési eljárásokat a K11.010_P[2] által meghatározott gyakorisággal tesztelik annak biztosítása érdekében, hogy a tervezett törlés megvalósuljon
76.	11.11. Adathordozók törlése – Roncsolásmentes technikák	K11.011_P[1]	meghatározásra kerültek a hordozható tárolóeszközök törlését igénylő körülmények
77.		K11.011_O.11.11	a K11.011_P[1] által meghatározott körülmények között a hordozható tárolóeszközökön roncsolásmentes törlési technikákat alkalmaznak, mielőtt ezeket az eszközöket az EIR-hez csatlakoztatják
78.	11.14. Adathordozók használata	K11.014_P[1]	meghatározásra kerültek az EIR-ekben vagy rendszerelemekben korlátozandó vagy tiltandó adathordozók típusai
79.		K11.014_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy került kiválasztásra: {korlátozott, tiltott}
80.		K11.014_P[3]	meghatározásra kerültek az olyan rendszerek vagy rendszerelemek, amelyekben meghatározott típusú adathordozók használatát korlátozni vagy tiltani kell
81.		K11.014_P[4]	meghatározták azokat a mechanizmusokat, amelyek korlátozzák vagy megtiltják bizonyos típusú adathordozók használatát a rendszerekben vagy rendszerelemekben
82.		K11.014_O.11.14.1	a K11.014_P[1] által meghatározott típusú adathordozók használata során a K11.014_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK közül a K11.014_P[3] által meghatározott rendszereken a K11.014_P[4] által meghatározott mechanizmusok érvényesülnek
83.		K11.014_O.11.14.2	a hordozható tárolóeszközök használata az EIR-ekben tiltott, ha az ilyen eszközöknek nincs azonosítható tulajdonosa

12. Fizikai és környezeti védelem

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	12.1. Szabályzat és eljárásrendek	K12.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a fizikai védelmi szabályzatot meg kell ismertetni
3.		K12.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a fizikai védelmi eljárásokat meg kell ismertetni
4.		K12.001_P[3]	meghatározott, hogy a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K12.001_P[4]	a fizikai védelmi szabályzat és eljárások irányítására egy meghatározott személy kijelölése megtörtént
6.		K12.001_P[5]	meghatározásra került a fizikai védelmi szabályzat felülvizsgálatának és frissítésének gyakorisága
7.		K12.001_P[6]	meghatározták azokat az eseményeket, amelyek a fizikai védelmi szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K12.001_P[7]	meghatározták a fizikai védelmi eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K12.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a fizikai védelmi eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K12.001_O_12.1.1.(a)	fizikai védelmi szabályzatot dolgoztak ki és dokumentáltak
11.		K12.001_O_12.1.1.(b)	a fizikai védelmi szabályzatot megismertették a K12.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K12.001_O_12.1.1.(c)	a fizikai védelmi szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő fizikai védelmi eljárások kidolgozása és dokumentálása megtörtént
13.		K12.001_O_12.1.1.(d)	a fizikai védelmi eljárások megismertetése a K12.001_P[2] által meghatározott személyekkel vagy szerepkörökkel megtörtént
14.		K12.001_O_12.1.2	kijelölték azt a K12.001_P[4] által meghatározott személyt, aki a fizikai védelmi szabályzat és eljárások kidolgozásának, dokumentálásának és ismertetésének irányítását végzi
15.		K12.001_O_12.1.3.(a)	a fizikai védelmi szabályzatot felülvizsgálják és frissítik a K12.001_P[5] által meghatározott gyakorisággal
16.		K12.001_O_12.1.3.(b)	a fizikai védelmi szabályzatot felülvizsgálják és frissítik a K12.001_P[6] által meghatározott eseményeket követően
17.		K12.001_O_12.1.3.(c)	a fizikai védelmi eljárásokat felülvizsgálják és frissítik a K12.001_P[7] által meghatározott gyakorisággal
18.		K12.001_O_12.1.3.(d)	a fizikai védelmi eljárásokat felülvizsgálják és frissítik a K12.001_P[8] által meghatározott eseményeket követően
19.		K12.001_O_12.1.1.1.1.(a)	a fizikai védelmi szabályzat célja meghatározott a K12.001_P[3] szerint

20.		K12.001_O_12.1.1.1.1.(b)	a fizikai védelmi szabályzat hatálya meghatározott a K12.001_P[3] szerint
21.		K12.001_O_12.1.1.1.1.(c)	a fizikai védelmi szabályzathoz kapcsolódó szerepkörök meghatározottak a K12.001_P[3] szerint
22.		K12.001_O_12.1.1.1.1.(d)	a fizikai védelmi szabályzathoz kapcsolódó felelősségek rögzítettek a K12.001_P[3] szerint
23.		K12.001_O_12.1.1.1.1.(e)	a fizikai védelmi szabályzathoz kapcsolódó vezetői elkötelezettség rögzített a K12.001_P[3] szerint
24.		K12.001_O_12.1.1.1.1.(f)	a fizikai védelmi szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés rögzített a K12.001_P[3] szerint
25.		K12.001_O_12.1.1.1.1.(g)	a fizikai védelmi szabályzathoz kapcsolódó megfelelőségi kritériumok rögzítettek a K12.001_P[3] szerint
26.		K12.001_O_12.1.1.1.2.	a fizikai védelmi szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	12.2. A fizikai belépési engedélyek	K12.002_P[1]	meghatározták, hogy milyen gyakorisággal kell felülvizsgálni a belépési listát, amely részletezi az egyének engedélyezett létesítmény-hozzáférését
28.		K12.002_O.12.2.1.(a)	összeállításra került egy lista azokról a személyekről, akik jogosultak hozzáférni ahhoz a létesítményhez, ahol az EIR található
29.		K12.002_O.12.2.1.(b)	jóváhagytak egy listát azokról a személyekről, akik jogosultak hozzáférni ahhoz a létesítményhez, ahol az EIR található
30.		K12.002_O.12.2.1.(c)	vezetnek egy listát azokról a személyekről, akik jogosultak hozzáférni ahhoz a létesítményhez, ahol az EIR található
31.		K12.002_O.12.2.2	a létesítménybe való belépéshez jogosultsági igazolványokat adtak ki
32.		K12.002_O.12.2.3	vezetik a belépési listát, amely részletezi az egyének engedélyezett létesítmény-hozzáférését, amelyet a K12.002_P[1] által meghatározott gyakorisággal felülvizsgálnak
33.		K12.002_O.12.2.4	ha a hozzáférésre már nincs szükség, a személyeket eltávolítják a létesítmény belépési listájáról
34.	12.6. A fizikai belépés ellenőrzése	K12.006_P[1]	meghatározták annak a létesítménynek a belépési és kilépési pontjait, amelyben a rendszer található
35.		K12.006_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {a K12.006_P[3] által meghatározott rendszerek vagy eszközök, őrök}
36.		K12.006_P[3]	meghatározottak a létesítménybe való be- és kilépés ellenőrzésére használt fizikai beléptető rendszerek vagy eszközök
37.		K12.006_P[4]	meghatározták azokat a belépési vagy kilépési pontokat, amelyekre vonatkozóan fizikai belépési naplót vezetnek
38.		K12.006_P[5]	meghatározásra kerültek a létesítményen belül a nyilvánosság számára hozzáférhetőnek minősített területekhez való hozzáférés ellenőrzésére szolgáló fizikai hozzáférés-ellenőrzések

39.		K12.006_P[6]	meghatározásra kerültek a látogatók kíséretét és a látogatók tevékenységének figyelemmel kísérését szükségessé tevő körülmények
40.		K12.006_P[7]	meghatározásra kerültek a leltározandó fizikai belépést ellenőrző eszközök
41.		K12.006_P[8]	meghatározták a fizikai belépést ellenőrző eszközök nyilvántartása frissítésének gyakoriságát
42.		K12.006_P[9]	meghatározásra került a hozzáférési kódok cseréjének gyakorisága
43.		K12.006_P[10]	meghatározásra került a kulcsok cseréjének gyakorisága
44.		K12.006_O.12.6.1.1	a fizikai belépési jogosultságokat a K12.006_P[1] által meghatározott belépési és kilépési pontokon úgy érvényesítik, hogy a létesítménybe való belépés engedélyezése előtt ellenőrzik az egyéni belépési jogosultságokat
45.		K12.006_O.12.6.1.2	a fizikai belépési jogosultságokat a K12.006_P[1] által meghatározott belépési és kilépési pontokon a létesítménybe való be- és kilépés ellenőrzésével, a K12.006_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK segítségével érvényesítik
46.		K12.006_O.12.6.2	a K12.006_P[4] által meghatározott belépési vagy kilépési pontokhoz fizikai hozzáférési ellenőrzési naplót vezetnek
47.		K12.006_O.12.6.3	a létesítményen belül a nyilvánosan hozzáférhetőnek minősített területekhez való hozzáférést a K12.006_P[5] által meghatározott fizikai hozzáférés-ellenőrzés végrehajtásával tartják fenn
48.		K12.006_O.12.6.4.(a)	a látogatókat kísérik
49.		K12.006_O.12.6.4.(b)	a látogatói tevékenységet a K12.006_P[6] által meghatározott körülmények esetén figyelemmel kísérik
50.		K12.006_O.12.6.5.(a)	a kulcsokat biztonságosan tárolják
51.		K12.006_O.12.6.5.(b)	a hozzáférési kódokat biztonságosan tárolják
52.		K12.006_O.12.6.5.(c)	az egyéb fizikai hozzáférést biztosító eszközöket biztonságosan tárolják
53.		K12.006_O.12.6.6	vezetik a K12.006_P[7] által meghatározott fizikai belépést ellenőrző eszközök nyilvántartását, mely a K12.006_P[8] által meghatározott gyakorisággal frissítésre kerül
54.		K12.006_O.12.6.7.(a)	a hozzáférési kódok megváltoztatásra kerülnek a K12.006_P[9] által meghatározott gyakorisággal, amikor a hozzáférési kód kompromittálódik, vagy amikor a hozzáférési kódokat birtokló személyeket áthelyezik vagy megszüntetik a jogosultságukat
55.		K12.006_O.12.6.7.(b)	a kulcsok megváltoztatása a K12.006_P[10] által meghatározott gyakorisággal történik a kulcsok elvesztése, a kulcsokat birtokló személyek áthelyezése vagy jogosultságuk megszűnése esetén
56.	12.7. A fizikai belépés ellenőrzése – Rendszer hozzáférés	K12.007_P[1]	meghatározták a rendszer egy vagy több elemét tartalmazó fizikai helyiségeket
57.		K12.007_O.12.7.(a)	a rendszerhez történő fizikai hozzáférési jogosultságok kiadása engedélyezéshez kötött
58.		K12.007_O.12.7.(b)	a létesítmény fizikai hozzáférés-ellenőrzése a K12.007_P[1] által meghatározott fizikai helyiségeiben érvényesül

59.	12.14. Hozzáférés az adatátviteli eszközökhöz és csatornákhoz	K12.014_P[1]	meghatározásra kerültek a fizikai hozzáférés ellenőrzését igénylő rendszerelosztó és -átviteli vezetékek
60.		K12.014_P[2]	meghatározták a szervezeti létesítményen belül a rendszerelosztó és -átviteli vezetékekhez való fizikai hozzáférés ellenőrzése érdekében végrehajtandó biztonsági követelményeket
61.		K12.014_O.12.14	a K12.014_P[1] által meghatározott rendszerelosztó és -átviteli vezetékekhez való fizikai hozzáférést a szervezeti létesítményeken belül a K12.014_P[2] által meghatározott biztonsági követelmények alkalmazásával ellenőrzik
62.	12.15. A kimeneti eszközök hozzáférés-ellenőrzése	K12.015_P[1]	meghatározták az olyan kimeneti eszközöket, amelyek fizikai hozzáférés-ellenőrzést igényelnek az előállított kimenethez
63.		K12.015_O.12.15	a K12.015_P[1] által meghatározott kimeneti eszközök kimenetéhez való fizikai hozzáférést ellenőrzik annak érdekében, hogy megakadályozzák, hogy jogosulatlan személyek férjenek hozzá az előállított kimenetekhez
64.	12.17. A fizikai hozzáférések felügyelete	K12.017_P[1]	meghatározták a fizikai hozzáférési naplók felülvizsgálatának gyakoriságát
65.		K12.017_P[2]	meghatározták a fizikai hozzáférési naplók felülvizsgálatát igénylő eseményeket vagy az eseményekre utaló potenciális jeleket
66.		K12.017_O.12.7.1	a fizikai biztonsági események észlelése és az azokra való reagálás érdekében ellenőrzi a fizikai hozzáférést ahhoz a létesítményhez, ahol az EIR található
67.		K12.017_O.12.7.2.(a)	a fizikai hozzáférési naplók felülvizsgálata a K12.017_P[1] által meghatározott gyakorisággal történik
68.		K12.017_O.12.7.2.(b)	a fizikai hozzáférési naplókat a K12.017_P[2] által meghatározott események bekövetkezésekor felülvizsgálják
69.		K12.017_O.12.7.3.(a)	az ellenőrzések eredményeit összehangolják a szervezeti eseménykezelési képességekkel
70.		K12.017_O.12.7.3.(b)	a vizsgálatok eredményeit összehangolják a szervezeti eseménykezelési képességekkel
71.	12.18. A fizikai hozzáférések felügyelete – Behatolásjelző és megfigyelő berendezések	K12.018_O.12.18.(a)	a rendszer helyszínéül szolgáló létesítménybe való fizikai bejutást fizikai behatolásjelzőkkel ellenőrzik
72.		K12.018_O.12.18.(b)	a rendszer helyszínéül szolgáló létesítménybe való fizikai bejutást felügyeleti berendezések alkalmazásával ellenőrzik
73.	12.21. A fizikai hozzáférések felügyelete – Rendszerekhez való fizikai hozzáférés-ellenőrzése	K12.021_P[1]	meghatározták az EIR egy vagy több elemét tartalmazó fizikai helyiségeket
74.		K12.021_O.12.21	a rendszerhez való fizikai hozzáférést a K12.021_P[1] által meghatározott fizikai helyiségeknél a létesítmény fizikai hozzáférésének ellenőrzésén túlmenően felügyelik
75.	12.22. Látogatói hozzáférési naplók	K12.022_P[1]	meghatározták azt az időtartamot, amely alatt a látogatói belépési nyilvántartást vezetni kell arra a létesítményre vonatkozóan, ahol a rendszer található
76.		K12.022_P[2]	meghatározásra került a látogatói belépési nyilvántartás felülvizsgálatának gyakorisága

77.		K12.022_P[3]	meghatározottak azok a személyek vagy szerepkörök, akinek a látogatói belépési nyilvántartás rendellenességeit jelenteni kell
78.		K12.022_O.12.22.1	a K12.022_P[1] által meghatározott időtartamra vonatkozóan látogatói belépési nyilvántartást vezetnek arról a létesítményről, ahol az EIR található
79.		K12.022_O.12.22.2	a látogatói belépési nyilvántartás felülvizsgálata a K12.022_P[2] által meghatározott gyakorisággal történik
80.		K12.022_O.12.22.3	a látogatói belépési nyilvántartás rendellenességeit jelentik a K12.022_P[3] által meghatározott személyeknek vagy szerepköröknek
81.	12.23. Látogatói hozzáférési naplók – Nyilvántartások automatizált karbantartása és felülvizsgálata	K12.023_P[1]	meghatározásra kerültek a látogatók belépési nyilvántartásának kezelésére használt automatizált mechanizmusok
82.		K12.023_P[2]	meghatározásra kerültek a látogatók belépési nyilvántartásának átvizsgálására használt automatizált mechanizmusok
83.		K12.023_O.12.23.(a)	a látogatók belépési nyilvántartását a K12.023_P[1] által meghatározott automatizált mechanizmusok segítségével kezelik
84.		K12.023_O.12.23.(b)	a látogatók belépési nyilvántartását a K12.023_P[2] által meghatározott automatizált mechanizmusok segítségével átvizsgálják
85.	12.24. Áramellátó berendezések és kábelezés	K12.024_O.12.24.(a)	az EIR áramellátását biztosító berendezései védettek a károsodástól és a megsemmisüléstől
86.		K12.024_O.12.24.(b)	az EIR áramellátását biztosító kábelezése védett a károsodástól és a megsemmisüléstől
87.	12.27. Vészkikapcsolás	K12.027_P[1]	meghatározásra került olyan EIR vagy egyes rendszerelemek, amelyeknek vészhelyzetben le kell tudni kapcsolni az áramellátást
88.		K12.027_P[2]	a vészlezáró kapcsolók vagy készülékek helye rendszerenként vagy rendszerelemenként került meghatározásra
89.		K12.027_O.12.27.1	a K12.027_P[1] által meghatározott rendszer vagy egyes rendszerelemek áramellátásának vészhelyzetben történő kikapcsolására van lehetőség
90.		K12.027_O.12.27.2	a vészlezáró kapcsolók vagy készülékek a K12.027_P[2] által meghatározott helyen vannak elhelyezve, hogy megkönnyítsék a hozzáférést az arra jogosult személyzet számára
91.		K12.027_O.12.27.3	a vészhelyzeti kikapcsolási lehetőség védett a jogosulatlan aktiválással szemben
92.	12.28. Vészhelyzeti tápellátás	K12.028_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {rendszer leállítása; hosszútávú tartalék áramellátásra történő átkapcsolás}
93.		K12.028_O.12.28	szünetmentes áramellátást biztosítanak, amely megkönnyíti a K12.028_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK működésének fenntartását az elsődleges áramforrás kiesése esetén

94.	12.29. Vészhelyzeti tápellátás – Tartalék áramellátás – Minimális működési képesség	K12.029_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy került kiválasztásra: {manuálisan, automatikusan}
95.		K12.029_O.12.29.(a)	a rendszer számára biztosított alternatív áramellátás aktiválódik a K12.029_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK szerint
96.		K12.029_O.12.29.(b)	a rendszer számára biztosított alternatív áramellátás képes fenntartani a minimálisan szükséges működési képességet az elsődleges áramforrás hosszabb ideig tartó kiesése esetén
97.	12.31. Vészvilágítás	K12.031_O.12.31.(a)	a rendszerhez automatikus vészvilágítást alkalmaznak, amely áramkimaradás vagy áramszünet esetén aktiválódik
98.		K12.031_O.12.31.(b)	a rendszerhez automatikus vészvilágítást tartanak karban, amely áramkimaradás vagy áramszünet esetén aktiválódik
99.		K12.031_O.12.31.(c)	a rendszer automatikus vészvilágítása a létesítményen belüli vészkijáratokra terjed ki
100.		K12.031_O.12.31.(d)	a rendszer automatikus vészvilágítása a létesítményen belüli menekülési útvonalakra terjed ki
101.	12.33. Tűzvédelem	K12.033_O.12.33.(a)	tűzérzékelő rendszereket alkalmaznak
102.		K12.033_O.12.33.(b)	az alkalmazott tűzérzékelő rendszereket független energiaforrás támogatja
103.		K12.033_O.12.33.(c)	az alkalmazott tűzérzékelő rendszereket karbantartják
104.		K12.033_O.12.33.(d)	tűzoltó rendszereket alkalmaznak
105.		K12.033_O.12.33.(e)	az alkalmazott tűzoltó rendszereket független energiaforrás támogatja
106.		K12.033_O.12.33.(f)	az alkalmazott tűzoltó rendszereket karbantartják
107.	12.34. Tűzvédelem – Érzékelőrendszerek – Automatikus élesítés és értesítés	K12.034_P[1]	meghatározták a tűz esetén értesítendő személyeket vagy szerepköröket
108.		K12.034_P[2]	meghatározták a tűz esetén értesítendő vészhelyzeti reagálókat
109.		K12.034_O.12.34.(a)	tűz esetén automatikusan működésbe lépő tűzjelző rendszereket alkalmaznak
110.		K12.034_O.12.34.(b)	tűzjelző rendszereket alkalmaznak, amelyek tűz esetén automatikusan értesítik a K12.034_P[1] által meghatározott személyeket vagy szerepköröket
111.		K12.034_O.12.34.(c)	tűzjelző rendszereket alkalmaznak, amelyek tűz esetén automatikusan értesítik a K12.034_P[2] által meghatározott vészhelyzeti reagálókat
112.	12.35. Tűzvédelem – Tűzoltó berendezések – Automatikus élesítés és értesítés	K12.035_P[1]	meghatározták a tűz esetén értesítendő személyeket vagy szerepköröket
113.		K12.035_P[2]	meghatározták a tűz esetén értesítendő vészhelyzeti reagálókat
114.		K12.035_O.12.35.1.(a)	automatikusan működésbe lépő tűzoltó rendszereket alkalmaznak

115.		K12.035_O.12.35.1.(b)	a K12.035_P[1] által meghatározott személyeket vagy szerepköröket automatikusan értesítő tűzoltó rendszereket alkalmaznak
116.		K12.035_O.12.35.1.(c)	a K12.035_P[2] által meghatározott vészhelyzeti reagálókat automatikusan értesítő tűzoltó rendszereket alkalmaznak
117.		K12.035_O.12.35.2	automatikus tűzoltó berendezést alkalmaznak, ha a létesítményben nincs állandó személyzet
118.	12.37. Környezeti védelmi intézkedések	K12.037_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {hőmérséklet; páratartalom; légnyomás; sugárzás; a K12.037_P[2] által meghatározott környezeti védelmi intézkedések}
119.		K12.037_P[2]	meghatározzák azokat a környezeti védelmi intézkedéseket, amelyeknek egy meghatározott szintet kell fenntartaniuk abban a létesítményben, ahol az EIR található
120.		K12.037_P[3]	meghatározták a környezeti tulajdonságok elfogadható szintjeit
121.		K12.037_P[4]	meghatározták a környezeti szabályozási szintek ellenőrzésének gyakoriságát
122.		K12.037_O.12.37.1	a K12.037_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK szintjei a K12.037_P[3] által meghatározott elfogadható szinten vannak tartva azon a létesítményen belül, ahol az EIR található
123.		K12.037_O.12.37.2	a környezeti szabályozási szinteket a K12.037_P[4] által meghatározott gyakorisággal felügyelik
124.	12.40. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	K12.040_O.12.40.(a)	az EIR-t a vízszivárgásból eredő károktól főelzáró vagy elzáró szelepek biztosításával védik
125.		K12.040_O.12.40.(b)	a főelzáró vagy elzáró szelepek hozzáférhetőek
126.		K12.040_O.12.40.(c)	a főelzáró vagy elzáró szelepek működőképesek
127.		K12.040_O.12.40.(d)	a főelzáró vagy elzáró szelepeket a kulcsszemélyzet ismeri
128.	12.41. Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem – Automatizálás támogatása	K12.041_P[1]	meghatározásra kerültek az EIR közelében megjelenő víz jelenlétének észlelésekor riasztandó személyek vagy szerepkörök
129.		K12.041_P[2]	meghatározásra kerültek az EIR közelében megjelenő víz jelenlétének észlelésekor használt automatizált mechanizmusok
130.		K12.041_O.12.41.(a)	az EIR közelében megjelenő víz jelenléte automatikusan érzékelhető
131.		K12.041_O.12.41.(b)	a K12.041_P[1] által meghatározott személyeket vagy szerepköröket a K12.041_P[2] által meghatározott automatizált mechanizmusok alkalmazásával riasztják
132.	12.42. Be- és kiszállítás	K12.042_P[1]	meghatározták a létesítménybe való belépéskor engedélyezendő és felügyelendő rendszerelemek típusait
133.		K12.042_P[2]	meghatározták a létesítménybe való kilépéskor engedélyezendő és felügyelendő rendszerelemek típusait
134.		K12.042_O.12.42.1.(a)	a K12.042_P[1] által meghatározott rendszerelemek típusai engedélyezettek a létesítménybe való belépéskor

135.		K12.042_O.12.42.1.(b)	a K12.042_P[1] által meghatározott rendszerelemek típusait ellenőrzik a létesítménybe való belépéskor
136.		K12.042_O.12.42.1.(c)	a K12.042_P[2] által meghatározott rendszerelemek típusai engedélyezettek a létesítmény elhagyásakor
137.		K12.042_O.12.42.1.(d)	a K12.042_P[2] által meghatározott rendszerelemek típusait ellenőrzik a létesítmény elhagyásakor
138.		K12.042_O.12.42.2	a rendszerelemekről nyilvántartást vezetnek
139.	12.43. Munkavégzésre kijelölt alternatív helyszín	K12.043_P[1]	meghatározták a munkavállalók által használható alternatív munkavégzési helyeket
140.		K12.043_P[2]	meghatározták az alternatív munkavégzési helyeken alkalmazandó védelmi intézkedéseket
141.		K12.043_O.12.43.1	a K12.043_P[1] szerinti alternatív munkavégzési helyek meghatározása és dokumentálása megtörtént
142.		K12.043_O.12.43.2	a K12.043_P[2] által meghatározott védelmi intézkedéseket alkalmaznak az alternatív munkavégzési helyeken
143.		K12.043_O.12.43.3	az alternatív munkavégzési helyeken végzett védelmi intézkedések hatékonyságát értékelik
144.		K12.043_O.12.43.4	a munkavállalók számára biztosított a lehetőség, hogy események bekövetkezése esetén kommunikálhassanak az információbiztonsággal foglalkozó személyekkel
145.	12.44. Az elektronikus információs rendszer elemeinek elhelyezése	K12.044_P[1]	meghatározták azokat a fizikai és környezeti veszélyeket, amelyek a létesítményen belüli rendszerelemek potenciális károsodását eredményezhetik
146.		K12.044_O.12.44	a rendszerelemeket úgy helyezik el a létesítményen belül, hogy minimalizálják a K12.044_P[1] által meghatározott fizikai és környezeti veszélyekből eredő lehetséges károkat, valamint a jogosulatlan hozzáférés lehetőségét

13. Tervezés

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	13.1. Szabályzat és eljárásrendek	K13.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a biztonságtervezési szabályzatot meg kell ismertetni
3.		K13.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a biztonságtervezési eljárásokat meg kell ismertetni
4.		K13.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K13.001_P[4]	meghatározott, hogy a biztonságtervezési szabályzat és eljárások irányítására egy meghatározott személy kijelölésre került

6.		K13.001_P[5]	meghatározásra került a biztonságtervezési szabályzat felülvizsgálatának és frissítésének gyakorisága
7.		K13.001_P[6]	meghatározták azokat az eseményeket, amelyek a biztonságtervezési szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K13.001_P[7]	meghatározták a biztonságtervezési eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K13.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a biztonságtervezési eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K13.001_O_13.1.1.(a)	biztonságtervezési szabályzatot dolgoztak ki és dokumentáltak
11.		K13.001_O_13.1.1.(b)	a biztonságtervezési szabályzatot megismertették a K13.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K13.001_O_13.1.1.(c)	a biztonságtervezési szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő biztonságtervezési eljárások kidolgozása és dokumentálása megtörtént
13.		K13.001_O_13.1.1.(d)	a biztonságtervezési eljárásokat megismertették a K13.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K13.001_O_13.1.2	a K13.001_P[4] által meghatározott személyt kijelölték a biztonságtervezési szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítására
15.		K13.001_O_13.1.3.(a)	a biztonságtervezési szabályzatot felülvizsgálják és frissítik a K13.001_P[5] által meghatározott gyakorisággal
16.		K13.001_O_13.1.3.(b)	a biztonságtervezési szabályzatot felülvizsgálják és frissítik a K13.001_P[6] által meghatározott eseményeket követően
17.		K13.001_O_13.1.3.(c)	a biztonságtervezési eljárásokat felülvizsgálják és frissítik a K13.001_P[7] által meghatározott gyakorisággal
18.		K13.001_O_13.1.3.(d)	a biztonságtervezési eljárásokat felülvizsgálják és frissítik a K13.001_P[8] által meghatározott eseményeket követően
19.		K13.001_O_13.1.1.1.1.(a)	a biztonságtervezési szabályzat célja rögzítésre került a K13.001_P[3] által meghatározottak szerint
20.		K13.001_O_13.1.1.1.1.(b)	a biztonságtervezési szabályzat hatálya rögzítésre került a K13.001_P[3] által meghatározottak szerint
21.		K13.001_O_13.1.1.1.1.(c)	a biztonságtervezési szabályzathoz kapcsolódó szerepkörök rögzítésre kerültek a K13.001_P[3] által meghatározottak szerint
22.		K13.001_O_13.1.1.1.1.(d)	a biztonságtervezési szabályzathoz kapcsolódó felelősségek rögzítésre kerültek a K13.001_P[3] által meghatározottak szerint
23.		K13.001_O_13.1.1.1.1.(e)	a biztonságtervezési szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K13.001_P[3] által meghatározottak szerint
24.		K13.001_O_13.1.1.1.1.(f)	a biztonságtervezési szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés rögzítésre került a K13.001_P[3] által meghatározottak szerint

25.		K13.001_O_13.1.1.1.1.(g)	a biztonságtervezési szabályzathoz kapcsolódó megfelelőségi kritériumok rögzítésre kerültek a K13.001_P[3] által meghatározottak szerint
26.		K13.001_O_13.1.1.1.2.	a biztonságtervezési szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	13.2. Rendszerbiztonsági terv	K13.002_P[1]	meghatározásra kerültek olyan személyek vagy csoportok, akik az EIR-t érintő, tervezést és koordinációt igénylő, a biztonsággal kapcsolatos tevékenységeket végzik
28.		K13.002_P[2]	meghatározásra kerültek a rendszerbiztonsági terv megismerésére jogosult személyek vagy szerepkörök
29.		K13.002_P[3]	meghatározásra került a rendszerbiztonsági terv felülvizsgálatának gyakorisága
30.		K13.002_O.13.2.1.1	a szervezet felépítésével összhangban álló biztonsági tervet dolgoztak ki a rendszerre
31.		K13.002_O.13.2.1.2	az EIR biztonsági terve meghatározza az EIR alkotóelemeit
32.		K13.002_O.13.2.1.3	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely leírja az EIR működési környezetét az ügymeneti és üzleti folyamatok szempontjából
33.		K13.002_O.13.2.1.4	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely meghatározza az EIR szerepeit és felelősségi köreit betöltő személyeket
34.		K13.002_O.13.2.1.5	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely meghatározza az EIR által feldolgozott, tárolt és továbbított információtípusokat
35.		K13.002_O.13.2.1.6	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely tartalmazza az EIR biztonsági osztályát, beleértve az azt alátámasztó indoklást is
36.		K13.002_O.13.2.1.7	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely leírja az EIR-t fenyegető veszélyeket
37.		K13.002_O.13.2.1.8	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely leírja az EIR működési környezetét és a más rendszerektől vagy rendszerelemektől való függőségeket vagy kapcsolatokat
38.		K13.002_O.13.2.1.9	az EIR biztonsági tervének kidolgozása megtörtént, amely áttekintést nyújt az EIR-rel szemben támasztott biztonsági követelményekről
39.		K13.002_O.13.2.1.10	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely adott esetben meghatározza a vonatkozó alapkövetelményeket vagy átfedéseket
40.		K13.002_O.13.2.1.11	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely leírja a biztonsági követelmények teljesítése érdekében alkalmazott vagy tervezett védelmi intézkedéseket, beleértve a testreszabási döntések indoklását is
41.		K13.002_O.13.2.1.12	az EIR-re vonatkozóan biztonsági tervet dolgoztak ki, amely tartalmazza az EIR-t érintő, biztonsággal kapcsolatos olyan tevékenységeket, amelyek tervezést és koordinációt igényelnek a K13.002_P[1] által meghatározott személyekkel vagy csoportokkal

42.		K13.002_O.13.2.1.14	az EIR-re biztonsági tervet dolgoztak ki, amelyet az engedélyezésre jogosult tisztviselő vagy kijelölt képviselője a terv végrehajtása előtt áttekint és jóváhagy
43.		K13.002_O.13.2.2.(a)	a rendszerbiztonsági terv a K13.002_P[2] által meghatározott személyekkel vagy a szerepkörökkel megismertetésre került
44.		K13.002_O.13.2.2.(b)	a rendszerbiztonsági terv módosításait közölték a K13.002_P[2] által meghatározott személyekkel vagy szerepkörökkel
45.		K13.002_O.13.2.3	a rendszerbiztonsági terv felülvizsgálatra kerül a K13.002_P[3] által meghatározott gyakorisággal
46.		K13.002_O.13.2.4.(a)	a rendszerbiztonsági terv az EIR és a működési környezet változásainak figyelembevételével kerül frissítésre
47.		K13.002_O.13.2.4.(b)	a rendszerbiztonsági tervet a terv végrehajtása során feltárt problémák kezelése érdekében aktualizálják
48.		K13.002_O.13.2.4.(c)	a rendszerbiztonsági tervet a terv értékelése során feltárt problémák kezelése érdekében aktualizálják
49.		K13.002_O.13.2.5.(a)	a rendszerbiztonsági terv védett a jogosulatlan megismeréssel szemben
50.		K13.002_O.13.2.5.(b)	a rendszerbiztonsági terv védett a jogosulatlan módosítással szemben
51.	13.3. Viselkedési szabályok	K013.003_P[1]	meghatározásra került a viselkedési szabályok felülvizsgálatának és frissítésének gyakorisága
52.		K013.003_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {a K013.003_P[3] által meghatározott gyakoriság; amikor a szabályok felülvizsgálatra vagy frissítésre kerülnek}
53.		K013.003_P[3]	meghatározott a viselkedési szabályok elolvasásának és újbóli megismerésének gyakorisága a személyek számára
54.		K013.003_O.13.3.1.(a)	az EIR-hez való hozzáférést igénylő személyek számára olyan szabályokat állapítanak meg, amelyek leírják az információ- és rendszerhasználattal, a biztonsággal és a magánélet védelmével kapcsolatos felelősséget és elvárt viselkedést
55.		K013.003_O.13.3.1.(b)	az EIR-hez való hozzáférést igénylő személyek számára olyan szabályokat biztosítanak, amelyek leírják az információ- és rendszerhasználattal, a biztonsággal és a magánélet védelmével kapcsolatos felelősséget és elvárt viselkedést
56.		K013.003_O.13.3.2	az információkhoz és az EIR-hez való hozzáférés engedélyezése előtt a személyektől dokumentált visszaigazolást kapnak arról, hogy elolvasták, megértették és elfogadják a viselkedési szabályokat
57.		K013.003_O.13.3.3	a viselkedési szabályokat felülvizsgálják és frissítik a K13.003_P[1] által meghatározott gyakorisággal
58.		K013.003_O.13.3.4	azok a személyek, akik a viselkedési szabályok egy korábbi változatát ismerték meg, a megváltozott szabályokat kötelesek elolvasni és újra annak megismerését elismerni a K13.003_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK szerint
59.	13.4. Viselkedési szabályok – Közösségi média és külső	K13.004_O.13.4.1	a viselkedési szabályok közé tartoznak a közösségi média, a közösségi oldalak és a külső oldalak, illetve alkalmazások használatára vonatkozó korlátozások

60.	webhelyek, alkalmazások használatára vonatkozó korlátozások	K13.004_O.13.4.2	a viselkedési szabályok között szerepelnek a szervezeti információk nyilvános honlapokon való közzétételére vonatkozó korlátozások
61.		K13.004_O.13.4.3	a viselkedési szabályok tartalmazzák a szervezet által biztosított azonosítók (pl. e-mail címek) és hitelesítési adatok (pl. jelszavak) használatának korlátozását külső webhelyeken, illetve alkalmazásokon történő fiókok létrehozásához
62.	13.6. Információbiztonsági architektúra leírás	K13.006_P[1]	meghatározásra került a vállalati architektúrában bekövetkezett változásoknak megfelelő felülvizsgálat és frissítés gyakorisága
63.		K13.006_O.13.6.1.1	az EIR biztonsági architektúrája leírja a szervezeti információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelmére vonatkozó követelményeket és megközelítést
64.		K13.006_O.13.6.1.2	az EIR biztonsági architektúrája leírja, hogy az architektúra hogyan illeszkedik a vállalati architektúrába, és hogyan támogatja azt
65.		K13.006_O.13.6.1.3	az EIR biztonsági architektúrája leírja a külső rendszerekkel és szolgáltatásokkal kapcsolatos feltételezéseket és függőségeket
66.		K13.006_O.13.6.2	a vállalati architektúrában bekövetkezett változásokat felülvizsgálják és frissítik a K13.006_P[1] által meghatározott, a vállalati architektúrában bekövetkezett változások tükrözése érdekében
67.		K13.006_O.13.6.3.(a)	a tervezett architektúra-változtatások tükröződnek a rendszerbiztonsági tervben
68.		K13.006_O.13.6.3.(b)	a tervezett architektúra-változtatások tükröződnek a műveleti koncepcióban
69.		K13.006_O.13.6.3.(c)	a tervezett architektúra-változtatások tükröződnek a beszerzésekben
70.	13.10. Biztonsági követelmények kiválasztása	K13.010_O.13.10	kiválasztásra kerültek a rendszer MKr. szerinti biztonsági követelményei
71.	13.11. Biztonsági követelmények testre szabása	K13.011_O.13.11	a kiválasztott biztonsági követelmények testre szabottak

14. Személyi biztonság

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	14.1. Szabályzat és eljárásrendek	K14.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a személyi biztonságra vonatkozó szabályzatot meg kell ismertetni
3.		K14.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a személyi biztonságra vonatkozó eljárásokat meg kell ismertetni

4.		K14.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K14.001_P[4]	meghatározott, hogy a személyi biztonságra vonatkozó szabályzat és eljárások irányítására egy meghatározott személyt kell kijelölni
6.		K14.001_P[5]	meghatározásra került a személyi biztonságra vonatkozó szabályzat felülvizsgálatának és frissítésének gyakorisága
7.		K14.001_P[6]	meghatározták azokat az eseményeket, amelyek a személyi biztonságra vonatkozó szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K14.001_P[7]	meghatározták a személyi biztonságra vonatkozó eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K14.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a személyi biztonságra vonatkozó eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K14.001_O_14.1.1.(a)	a személyi biztonságra vonatkozó szabályzatot dolgoztak ki és dokumentáltak
11.		K14.001_O_14.1.1.(b)	a személyi biztonságra vonatkozó szabályzatot megismertették a K14.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K14.001_O_14.1.1.(c)	a személyi biztonságra vonatkozó szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő személyi biztonságra vonatkozó eljárások kidolgozása és dokumentálása megtörtént
13.		K14.001_O_14.1.1.(d)	a személyi biztonságra vonatkozó eljárásokat megismertették a K14.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K14.001_O_14.1.2	a K14.001_P[4] által meghatározott személy kijelölésre került a személyi biztonságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának és ismertetésének irányítására
15.		K14.001_O_14.1.3.(a)	a személyi biztonságra vonatkozó szabályzatot felülvizsgálják és frissítik a K14.001_P[5] által meghatározott gyakorisággal
16.		K14.001_O_14.1.3.(b)	a személyi biztonságra vonatkozó szabályzatot felülvizsgálják és frissítik a K14.001_P[6] által meghatározott eseményeket követően
17.		K14.001_O_14.1.3.(c)	a személyi biztonságra vonatkozó eljárásokat felülvizsgálják és frissítik a K14.001_P[7] által meghatározott gyakorisággal
18.		K14.001_O_14.1.3.(d)	a személyi biztonságra vonatkozó eljárásokat felülvizsgálják és frissítik a K14.001_P[8] által meghatározott eseményeket követően
19.		K14.001_O_14.1.1.1.1.(a)	a személyi biztonságra vonatkozó szabályzat célja rögzítésre került a K14.001_P[3] által meghatározottak szerint
20.		K14.001_O_14.1.1.1.1.(b)	a személyi biztonságra vonatkozó szabályzat hatálya rögzítésre került a K14.001_P[3] által meghatározottak szerint
21.		K14.001_O_14.1.1.1.1.(c)	a személyi biztonságra vonatkozó szabályzathoz kapcsolódó szerepkörök rögzítésre kerültek a K14.001_P[3] által meghatározottak szerint

22.		K14.001_O_14.1.1.1.1.(d)	a személyi biztonságra vonatkozó szabályzathoz kapcsolódó felelősségek rögzítésre kerültek a K14.001_P[3] által meghatározottak szerint
23.		K14.001_O_14.1.1.1.1.(e)	a személyi biztonságra vonatkozó szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K14.001_P[3] által meghatározottak szerint
24.		K14.001_O_14.1.1.1.1.(f)	a személyi biztonságra vonatkozó szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés rögzítésre került a K14.001_P[3] által meghatározottak szerint
25.		K14.001_O_14.1.1.1.1.(g)	a személyi biztonságra vonatkozó szabályzathoz kapcsolódó megfelelőségi kritériumok rögzítésre kerültek a K14.001_P[3] által meghatározottak szerint
26.		K14.001_O_14.1.1.1.2.	a személyi biztonságra vonatkozó szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	14.2. Munkakörök biztonsági szempontú besorolása	K14.002_P[1]	meghatározták, hogy milyen gyakorisággal kell felülvizsgálni és frissíteni a munkakörök kockázati besorolását
28.		K14.002_O.14.2.1	minden szervezeti munkakörhöz kockázati besorolást rendeltek
29.		K14.002_O.14.2.2	a szervezeti munkaköröket betöltő személyekre vonatkozó átvilágítási kritériumokat állapítottak meg
30.		K14.002_O.14.2.3	a munkakörök kockázati besorolását felülvizsgálják és frissítik a K14.002_P[1] által meghatározott gyakorisággal
31.	14.3. Személyek háttérellenőrzése	K14.003_P[1]	meghatározták az egyének ismételt ellenőrzését igénylő feltételeket
32.		K14.003_P[2]	meghatározták az egyének ismételt ellenőrzésének gyakoriságát ott, ahol ez szükséges
33.		K14.003_O.14.3.1	az EIR-hez való hozzáférés engedélyezése előtt az egyéneket ellenőrzik
34.		K14.003_O.14.3.2.(a)	az egyéneket a K14.003_P[1] által meghatározott ismételt ellenőrzést igénylő feltételekkel összhangban újra átvilágítják
35.		K14.003_O.14.3.2.(b)	ha ismételt ellenőrzés szükséges, az egyének ismételt ellenőrzése a K14.003_P[2] által meghatározott gyakorisággal történik
36.	14.5. Személyek munkaviszonyának megszűnése	K14.005_P[1]	meghatározták azt az időtartamot, amelyen belül a rendszerhez való hozzáférést le kell tiltani
37.		K14.005_P[2]	meghatározták a kilépési interjúk során megvitatandó információbiztonsági témákat
38.		K14.005_O.14.5.1	a munkaviszony megszűnésekor a rendszerhez való hozzáférés a K14.005_P[1] által meghatározott időtartamon belül letiltásra kerül
39.		K14.005_O.14.5.2	a munkaviszony megszűnésekor minden hitelesítő eszköz és jogosultság megszűnik vagy visszavonásra kerül
40.		K14.005_O.14.5.3	a munkaviszony megszűnésekor a rendszerhez való hozzáférés a K14.005_P[2] által meghatározott információbiztonsági témák megvitatására is kiterjedő kilépési interjúkra kerül sor

41.		K14.005_O.14.5.4	a munkaviszony megszűnésekor az összes, a biztonsággal kapcsolatos szervezeti EIR-rel kapcsolatos eszköz visszavételre kerül
42.		K14.005_O.14.5.5	a munkavállaló munkaviszonyának megszűnésekor a korábban általa ellenőrzött szervezeti információkhoz és EIR-ekhez való hozzáférés megmarad
43.	14.7. Személyek munkaviszonyának megszűnése – Automatizált intézkedések	K14.007_P[1]	meghatározásra kerültek az automatizált mechanizmusok a személyek vagy a szerepkörök egyéni kilépési tevékenységeiről való értesítésére, illetve az EIR erőforrásaihoz való hozzáférés letiltására
44.		K14.007_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {a K14.007_P[3] által meghatározott személyek vagy szerepkörök értesítése az egyes kilépési tevékenységekről; a rendszer erőforrásaihoz való hozzáférés letiltása}
45.		K14.007_P[3]	meghatározták azokat a személyeket vagy szerepköröket, akiknek az egyén kilépése esetén értesítést kell küldeni
46.		K14.007_O.14.7	a K14.007_P[1] által meghatározott automatizált mechanizmusokat alkalmaznak a K14.007_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK szerint
47.	14.8. Az áthelyezések, átirányítások és kirendelések kezelése	K14.008_P[1]	meghatározásra kerültek az áthelyezést vagy átirányítást követően kezdeményezendő áthelyezési vagy átirányítási intézkedéseket
48.		K14.008_P[2]	meghatározták azt az időtartamot, amelyen belül az áthelyezést vagy átirányítást követően az áthelyezési vagy átirányítási intézkedéseknek meg kell történniük
49.		K14.008_P[3]	meghatározásra kerültek a szervezeten belül az egyének áthelyezésekor vagy más pozícióba történő áthelyezésekor értesítendő személyek vagy szerepkörök
50.		K14.008_P[4]	meghatározták azt az időtartamot, amelyen belül értesíteni kell a szervezet által meghatározott személyeket vagy szerepköröket arról, ha az egyéneket átirányítják vagy áthelyezik más pozícióba a szervezeten belül
51.		K14.008_O.14.8.1	a rendszerekhez és létesítményekhez való aktuális logikai és fizikai hozzáférési jogosultságok folyamatos működési szükségességét felülvizsgálják és megerősítik, amikor az egyéneket áthelyezik vagy átirányítják a szervezeten belül más pozícióba
52.		K14.008_O.14.8.2	a K14.008_P[1] által meghatározott áthelyezési vagy átirányítási intézkedéseket a hivatalos áthelyezési vagy átirányítási intézkedést követően a K14.008_P[2] által meghatározott időtartamon belül kezdeményezik
53.		K14.008_O.14.8.3	a hozzáférési jogosultságot szükség szerint módosítják, hogy megfeleljen a működési szükségletekben az áthelyezés vagy átirányítás miatt bekövetkező változásoknak
54.		K14.008_O.14.8.4	a K14.008_P[3] által meghatározott személyeket vagy szerepköröket a K14.008_P[4] által meghatározott időtartamon belül értesítik
55.	14.9. Hozzáférési megállapodások	K14.009_P[1]	meghatározták a hozzáférési megállapodások felülvizsgálatának és frissítésének gyakoriságát
56.		K14.009_P[2]	meghatározták, hogy milyen gyakorisággal kell újra aláírni a hozzáférési megállapodásokat a szervezeti információkhoz való hozzáférés fenntartása érdekében

57.		K14.009_O.14.9.1	a szervezeti rendszerekhez hozzáférési megállapodásokat dolgoztak ki és dokumentáltak
58.		K14.009_O.14.9.2	a hozzáférési megállapodásokat felülvizsgálják és frissítik a K14.009_P[1] által meghatározott gyakorisággal
59.		K14.009_O.14.9.3.1	a szervezeti információkhoz és EIR-ekhez való hozzáférést igénylő személyek a hozzáférés engedélyezése előtt aláírták a megfelelő hozzáférési megállapodásokat
60.		K14.009_O.14.9.3.2	a szervezeti információkhoz és EIR-ekhez való hozzáférést igénylő személyek újra aláírják a hozzáférési megállapodásokat a szervezeti rendszerekhez való hozzáférés fenntartása érdekében változás esetén vagy a K14.009_P[2] által meghatározott gyakorisággal
61.	14.11. Külső személyekhez kapcsolódó biztonsági követelmények	K14.011_P[1]	meghatározásra kerültek a szervezeti hitelesítő eszközzel, illetve belépőkártyával rendelkező, vagy rendszerjogosultsággal rendelkező külső személyek bármely áthelyezéséről vagy kilépéséről értesítendő személyek vagy szerepkörök
62.		K14.011_P[2]	meghatározták azt az időtartamot, amelyen belül a külső szolgáltatóknak értesíteniük kell a szervezet által meghatározott személyeket vagy szerepköröket a szervezeti hitelesítő eszközzel, illetve belépőkártyával vagy rendszerjogosultsággal rendelkező külső személyek bármely áthelyezéséről vagy kilépéséről
63.		K14.011_O.14.11.1	meghatározásra kerültek a személyi biztonsági követelmények, beleértve a külső szolgáltatók biztonsági feladatait és felelősségi körét
64.		K14.011_O.14.11.2	meghatározásra került, hogy a külső szolgáltatóknak meg kell felelniük a szervezet által meghatározott személyi biztonsági szabályoknak és eljárásoknak
65.		K14.011_O.14.11.3	a személyi biztonsági követelmények dokumentáltak
66.		K14.011_O.14.11.4	rögzítésre került, hogy a külső szolgáltatók kötelesek értesíteni a K14.011_P[1] által meghatározott személyeket vagy szerepköröket a K14.011_P[2] által meghatározott időtartamon belül a szervezeti hitelesítő eszközzel, illetve belépőkártyával rendelkező vagy rendszerjogosultsággal rendelkező külső személyek bármely áthelyezéséről vagy kilépéséről
67.		K14.011_O.14.11.5	megállapodás alapján a szervezet ellenőrzi, hogy a szolgáltató megfelel-e a személyi biztonsági követelményeknek
68.	14.12. Fegyelmi intézkedések	K14.012_P[1]	meghatározásra kerültek a fegyelmi eljárás megindítása esetén értesítendő személyek vagy szerepkörök
69.		K14.012_P[2]	meghatározták azt az időtartamot, amelyen belül a szervezet által meghatározott személyeket vagy szerepköröket értesíteni kell a fegyelmi eljárás megindításáról
70.		K14.012_O.14.12.1	fegyelmi eljárást kezdeményeznek azon egyének esetében, akik nem tartják be a megállapított információbiztonsági szabályokat és eljárásokat
71.		K14.012_O.14.12.2	a K14.012_P[1] által meghatározott személyeket vagy szerepköröket a K14.012_P[2] által meghatározott időtartamon belül értesítik, ha fegyelmi eljárás indul, megjelölve a fegyelmi eljárás alá vont személyt és az eljárás okát

72.	14.13. Munkaköri leírások	K14.013_O.14.13	a biztonsági szerepek és felelősségi körök beépülnek a szervezeti munkaköri leírásokba

15. Kockázatkezelés

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	15.1. Szabályzat és eljárásrendek	K15.001_P[1]	meghatározásra kerültek azok a személyek vagy szerepkörök, akikkel a kockázatmenedzsment szabályzatot meg kell ismertetni
3.		K15.001_P[2]	meghatározásra kerültek azok a személyek vagy szerepkörök, akikkel a kockázatmenedzsment eljárásokat meg kell ismertetni
4.		K15.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kerül kiválasztásra {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K15.001_P[4]	a kockázatmenedzsment szabályzat és eljárások irányítására egy meghatározott személy került kijelölésre
6.		K15.001_P[5]	a kockázatmenedzsment szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K15.001_P[6]	meghatározásra kerültek azok az események, amelyek a kockázatmenedzsment szabályzat felülvizsgálatát és aktualizálását szükségessé teszik
8.		K15.001_P[7]	meghatározásra került a kockázatmenedzsment eljárások felülvizsgálatának és frissítésének gyakorisága
9.		K15.001_P[8]	meghatározásra kerültek azok az események, amelyek miatt a kockázatmenedzsment eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K15.001_O_15.1.1.(a)	kidolgozásra és dokumentálásra került a kockázatmenedzsment szabályzat
11.		K15.001_O_15.1.1.(b)	a kockázatmenedzsment szabályzat a K15.001_P[1] által meghatározott személyekkel vagy szerepkörökkel ismertetésre került
12.		K15.001_O_15.1.1.(c)	megtörtént a kockázatmenedzsment szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő kockázatmenedzsment eljárások kidolgozása és dokumentálása
13.		K15.001_O_15.1.1.(d)	sor került a kockázatmenedzsment eljárások megismertetésére a K15.001_P[2] által meghatározott személyekkel vagy szerepkörökkel
14.		K15.001_O_15.1.1.1.1.(a)	a kockázatmenedzsment szabályzat célja rögzítésre került a K15.001_P[3] által meghatározottak szerint
15.		K15.001_O_15.1.1.1.1.(b)	a kockázatmenedzsment szabályzat hatálya rögzítésre került a K15.001_P[3] által meghatározottak szerint

16.		K15.001_O_15.1.1.1.1.(c)	a kockázatmenedzsment szabályzathoz kapcsolódó szerepkörök rögzítésre kerültek a K15.001_P[3] által meghatározottak szerint
17.		K15.001_O_15.1.1.1.1.(d)	a kockázatmenedzsment szabályzathoz kapcsolódó felelősségek rögzítésre kerültek a K15.001_P[3] által meghatározottak szerint
18.		K15.001_O_15.1.1.1.1.(e)	a kockázatmenedzsment szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K15.001_P[3] által meghatározottak szerint
19.		K15.001_O_15.1.1.1.1.(f)	a kockázatmenedzsment szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés rögzítésre került a K15.001_P[3] által meghatározottak szerint
20.		K15.001_O_15.1.1.1.1.(g)	a kockázatmenedzsment szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K15.001_P[3] által meghatározottak szerint
21.		K15.001_O_15.1.1.1.2.	a kockázatmenedzsment szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
22.		K15.001_O_15.1.2	kijelölésre került a K15.001_P[4] által meghatározott személy a kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítására
23.		K15.001_O_15.1.3.(a)	a kockázatmenedzsment szabályzat felülvizsgálatra és frissítésre kerül a K15.001_P[5] által meghatározott gyakorisággal
24.		K15.001_O_15.1.3.(b)	a kockázatmenedzsment szabályzat felülvizsgálatra és frissítésre kerül a K15.001_P[6] által meghatározott eseményeket követően
25.		K15.001_O_15.1.3.(c)	a kockázatmenedzsment eljárások felülvizsgálatra és frissítésre kerülnek a K15.001_P[7] által meghatározott gyakorisággal
26.		K15.001_O_15.1.3.(d)	a kockázatmenedzsment eljárások felülvizsgálatra és frissítésre kerülnek a K15.001_P[8] által meghatározott eseményeket követően
27.	15.2. Biztonsági osztályba sorolás	K15.002_O.15.2.1	sor került a rendszer és az általa feldolgozott, tárolt és továbbított információk biztonsági osztályba sorolására
28.		K15.002_O.15.2.2	a biztonsági osztályba sorolás eredményei, beleértve az azt alátámasztó indoklást is, dokumentálásra kerültek a rendszer biztonsági tervében
29.		K15.002_O.15.2.3	az engedélyezésre jogosult tisztviselő vagy az engedélyezésre jogosult tisztviselő kijelölt képviselője felülvizsgálta és jóváhagyta a biztonsági osztályba sorolásról szóló döntést
30.	15.4. Kockázatelemzés	K15.004_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy került kiválasztásra: {biztonsági és adatvédelmi tervek; kockázatelemzési jelentés; a K15.004_P[2] által meghatározott dokumentum}
31.		K15.004_P[2]	megalkotásra került az a dokumentum, amelyben a kockázatelemzés eredményeit dokumentálni kell, ha azt nem a biztonsági és adatvédelmi tervekben vagy a kockázatelemzési jelentésben dokumentálják (ha alkalmazható)

32.		K15.004_P[3]	a kockázatelemzési eredmények felülvizsgálatának gyakorisága meghatározásra került
33.		K15.004_P[4]	meghatározásra kerültek azok a személyek vagy szerepkörök, akikkel a kockázatelemzés eredményeit meg kell ismertetni
34.		K15.004_P[5]	meghatározásra került a kockázatelemzés frissítésének gyakorisága
35.		K15.004_O.15.4.1.1	kockázatelemzésre került sor az EIR-re vonatkozó fenyegetések és sérülékenységek azonosítása érdekében
36.		K15.004_O.15.4.1.2	kockázatelemzésre került sor az EIR, az általa feldolgozott, tárolt vagy továbbított információk, valamint a kapcsolódó információk jogosulatlan hozzáférése, használata, közzététele, megzavarása, módosítása vagy megsemmisítése által okozott kár valószínűségének és hatásának meghatározására
37.		K15.004_O.15.4.1.3	kockázatelemzésre került sor a személyazonosításra alkalmas információk feldolgozásából eredő, az egyénekre gyakorolt káros hatások valószínűségének és hatásának meghatározása érdekében
38.		K15.004_O.15.4.2	a kockázatelemzés eredményei és a kockázatkezelési döntések a szervezeti célok vagy az üzleti folyamatok szempontjából integrálódnak a rendszerszintű kockázatelemzésekbe
39.		K15.004_O.15.4.3	a kockázatelemzés eredményei a K15.004_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK alapján kerültek dokumentálásra
40.		K15.004_O.15.4.4	a kockázatelemzés eredményei a K15.004_P[3] által meghatározott gyakorisággal felülvizsgálatra kerültek
41.		K15.004_O.15.4.5	a kockázatelemzés eredményei a K15.004_P[4] által meghatározott személyekkel vagy szerepkörökkel ismertetésre kerültek
42.		K15.004_O.15.4.6	a kockázatelemzés frissítésre kerül a K15.004_P[5] által meghatározott gyakorisággal, vagy amikor az EIR-ben, annak működési környezetében vagy más olyan körülményekben jelentős változások történnek, amelyek hatással lehetnek az EIR biztonsági állapotára
43.	15.5. Kockázatelemzés – Ellátási lánc	K15.005_P[1]	az ellátási lánc kockázatainak értékelésére meghatározásra kerültek az EIR-ek, rendszerelemek és rendszerszolgáltatások
44.		K15.005_P[2]	meghatározásra került, hogy milyen gyakorisággal kell frissíteni az ellátási lánc kockázatelemzését
45.		K15.005_O.15.5.1	a K15.005_P[1] által meghatározott rendszerekhez, rendszerelemekhez és rendszerszolgáltatásokhoz kapcsolódó ellátási lánc kockázatai felmérésre kerültek
46.		K15.005_O.15.5.2	az ellátási lánc kockázatelemzése frissítésre kerül a K15.005_P[2] által meghatározott gyakorisággal, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor az EIR, a működési környezet vagy más körülmények változása szükségessé teheti az ellátási lánc megváltoztatását
47.	15.9. Sérülékenységek ellenőrzése	K15.009_P[1]	meghatározásra került az EIR-ek és alkalmazások sérülékenységi ellenőrzésének gyakorisága
48.		K15.009_P[2]	meghatározásra került az EIR-ek és alkalmazások sérülékenységi azonosításának gyakorisága

49.		K15.009_P[3]	meghatározásra került az a válaszidő, amelyen belül a szervezeti kockázatkezelésnek megfelelően kijavításra kell, hogy kerüljenek a valós sérülékenységek
50.		K15.009_O.15.9.1.(a)	az EIR-ek és alkalmazások a K15.009_P[1] által meghatározott gyakorisággal, illetve eseti jelleggel ellenőrzésre kerülnek a sérülékenységek tekintetében a szervezet által meghatározott folyamatnak megfelelően, és amikor az EIR-t potenciálisan érintő új sérülékenységeket azonosítanak és jelentenek
51.		K15.009_O.15.9.1.(b)	az EIR-ek és alkalmazások a K15.009_P[2] által meghatározott gyakorisággal, illetve eseti jelleggel azonosításra kerülnek a sérülékenységek tekintetében a szervezet által meghatározott folyamatnak megfelelően, és amikor az EIR-t potenciálisan érintő új sérülékenységeket azonosítanak és jelentenek
52.		K15.009_O.15.9.2	a valós sérülékenységek kijavítására a K15.009_P[3] által meghatározott válaszidőn belül került sor a szervezeti kockázatkezelési eljárásoknak megfelelően
53.	15.10. Sérülékenység-menedzsment	K15.010_P[1]	meghatározásra került a rendszerek és alkalmazások sérülékenységi ellenőrzésének gyakorisága
54.		K15.010_P[2]	meghatározásra került a rendszerek és alkalmazások sérülékenységi azonosításának gyakorisága
55.		K15.010_P[3]	meghatározott az a válaszidő, amelyen belül a valós sérülékenységek kijavításának a szervezeti kockázatkezelésnek megfelelően meg kell történnie
56.		K15.010_P[4]	meghatározottak azok a személyek vagy szerepkörök, akikkel a sérülékenységi vizsgálatból és az ellenőrzési értékelésekből származó információkat meg kell ismertetni
57.		K15.010_O.15.10.1.(a)	az EIR-eket és alkalmazásokat a K15.010_P[1] által meghatározott gyakorisággal, illetve eseti jelleggel ellenőrzik a sérülékenységek tekintetében a szervezet által meghatározott folyamatnak megfelelően, és akkor, amikor az EIR-t potenciálisan érintő új sérülékenységeket azonosítanak és jelentenek
58.		K15.010_O.15.10.1.(b)	az EIR-eket és alkalmazásokat a K15.010_P[2] által meghatározott gyakorisággal, illetve eseti jelleggel azonosítják a sérülékenységek tekintetében a szervezet által meghatározott folyamatnak megfelelően, és akkor, amikor az EIR-t potenciálisan érintő új sérülékenységeket azonosítanak és jelentenek
59.		K15.010_O.15.10.2	sérülékenységi felügyeleti eszközöket és technikákat alkalmaznak az eszközök közötti átjárhatóság megkönnyítése érdekében
60.		K15.010_O.15.10.2.1	a sérülékenységet figyelő eszközöket és technikákat a sérülékenységi folyamat egyes részeinek automatizálására használják a platformok, szoftverhibák és helytelen konfigurációk felsorolására szolgáló szabványok alkalmazásával
61.		K15.010_O.15.10.2.2	a sérülékenységet figyelő eszközöket és technikákat az eszközök közötti átjárhatóság elősegítésére és a sérülékenységkezelési folyamat egyes részeinek automatizálására alkalmazzák azáltal, hogy szabványokat használnak az ellenőrző listák és a tesztelési eljárások formázására
62.		K15.010_O.15.10.2.3	sérülékenységet figyelő eszközöket és technikákat alkalmaznak az eszközök közötti átjárhatóság elősegítésére és a sérülékenységkezelési folyamat egyes részeinek automatizálására a sérülékenységi hatások mérésére szolgáló szabványok alkalmazásával

63.		K15.010_O.15.10.3	a sérülékenységi vizsgálatok jelentéseit és a sérülékenységi megfigyelés eredményeit elemzik
64.		K15.010_O.15.10.4	a valós sérülékenységek kijavítása a K15.010_P[3] által meghatározott válaszidőn belül megtörtént a szervezeti kockázatkezelési eljárásoknak megfelelően
65.		K15.010_O.15.10.5	a sérülékenység-menedzsment folyamatból és az ellenőrzési értékelésekből származó információkat megosztják a K15.010_P[4] által meghatározott személyekkel vagy szerepkörökkel, hogy segítsék a hasonló sérülékenységek kiküszöbölését más rendszerekben
66.		K15.010_O.15.10.6	olyan sérülékenység-menedzsment eszközöket alkalmaznak, amelyek képesek a vizsgálandó sérülékenységek egyszerű frissítésére
67.	15.11. Sérülékenység-menedzsment – Sérülékenységi adatbázis frissítése	K15.011_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {a K05.011_P[2] által meghatározott gyakoriság; új vizsgálat megkezdése előtt; új sérülékenységek azonosításakor és bejelentésekor}
68.		K15.011_P[2]	a vizsgálandó rendszer sérülékenységek frissítésének gyakorisága meghatározott
69.		K15.011_O.15.11	a vizsgálandó EIR-t frissítik a K05.011_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK alapján
70.	15.13. Sérülékenység-menedzsment – Felfedezhető információk	K15.013_P[1]	az EIR-rel kapcsolatos információk felfedezhetősége esetén végrehajtandó korrekciós intézkedések meghatározottak
71.		K15.013_O.15.13.(a)	az EIR-re vonatkozó információk felderíthetőek
72.		K15.013_O.15.13.(b)	a K15.013_P[1] által meghatározott korrekciós intézkedések megtételére akkor kerül sor, amikor az EIR-re vonatkozó információ felfedezhetőnek bizonyul
73.	15.14. Sérülékenység-menedzsment – Privilegizált hozzáférés	K15.014_P[1]	meghatározottak azon rendszerelemek, amelyekhez a kiválasztott sérülékenységvizsgálati tevékenységekhez privilegizált hozzáférés engedélyezett
74.		K15.014_P[2]	meghatározottak azok a sérülékenységvizsgálati tevékenységek, amelyeket a rendszerelemeken le kell folytatni
75.		K15.014_O.15.14	a K15.014_P[1] által meghatározott rendszerelemekhez való hozzáférés biztosított a K15.014_P[2] által meghatározott sérülékenységvizsgálat elvégzéséhez
76.	15.18. Sérülékenység-menedzsment – Sérülékenységi információk fogadása	K15.018_O.15.18	az EIR-ek és rendszerelemek sérülékenységéről szóló jelentések fogadására nyilvános jelentéstételi csatornát hoztak létre
77.	15.20. Kockázatokra adott válasz	K15.020_O.15.20.(a)	a biztonsági értékelések megállapításaira a szervezeti kockázattűrő képességnek megfelelően reagálnak
78.		K15.020_O.15.20.(b)	a biztonsági ellenőrzések megállapításaira a szervezeti kockázattűrő képességnek megfelelően reagálnak
79.		K15.020_O.15.20.(c)	a biztonsági vizsgálatok megállapításaira a szervezeti kockázattűrő képességnek megfelelően reagálnak

80.	15.21. Rendszerelemek kritikusságának elemzése	K15.021_P[1]	a kritikusság szempontjából elemzendő EIR-ek, rendszerelemek vagy rendszerszolgáltatások meghatározásra kerültek
81.		K15.021_P[2]	meghatározták a rendszerfejlesztési életciklus azon döntési pontjait, amikor kritikussági elemzést kell végezni
82.		K15.021_O.15.21	a kritikus rendszerelemeket és funkciókat a K15.021_P[1] által meghatározott EIR-ekre, rendszerelemekre vagy rendszerszolgáltatásokra vonatkozó kritikussági elemzés elvégzésével azonosították a rendszerfejlesztési életciklus K15.021_P[2] által meghatározott döntési pontjain

16. Rendszer- és szolgáltatásbeszerzés

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	16.1. Szabályzat és eljárásrendek	K16.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a beszerzési szabályzatot meg kell ismertetni
3.		K16.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a beszerzési eljárásokat meg kell ismertetni
4.		K16.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több került kiválasztásra: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K16.001_P[4]	a beszerzési szabályzat és eljárások irányítására egy meghatározott személy került kijelölésre
6.		K16.001_P[5]	a beszerzési szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K16.001_P[6]	meghatározták azokat az eseményeket, amelyek a beszerzési szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K16.001_P[7]	meghatározták a beszerzési eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K16.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a beszerzési eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K16.001_O_16.1.1.(a)	beszerzési szabályzatot dolgoztak ki és dokumentáltak
11.		K16.001_O_16.1.1.(b)	a beszerzési szabályzatot megismertetették a K16.001_P[1] által meghatározott személyekkel vagy szerepkörökkel
12.		K16.001_O_16.1.1.(c)	a beszerzési szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő beszerzési eljárások kidolgozásra és dokumentálásra kerültek
13.		K16.001_O_16.1.1.(d)	a beszerzési eljárásokat megismertetették a K16.001_P[2] szerinti személyekkel vagy szerepkörökkel
14.		K16.001_O_16.1.2	a K16.001_P[4] által meghatározott személyt kijelölték a beszerzési szabályzat és eljárások kidolgozásának, dokumentálásának és megismertetésének irányítására
15.		K16.001_O_16.1.3.(a)	a beszerzési szabályzatot felülvizsgálják és frissítik a K16.001_P[5] szerinti gyakorisággal

16.		K16.001_O_16.1.3.(b)	a beszerzési szabályzatot felülvizsgálják és frissítik a K16.001_P[6] szerinti eseményeket követően
17.		K16.001_O_16.1.3.(c)	a beszerzési eljárásokat felülvizsgálják és frissítik a K16.001_P[7] szerinti gyakorisággal
18.		K16.001_O_16.1.3.(d)	a beszerzési eljárásokat felülvizsgálják és frissítik a K16.001_P[8] szerinti eseményeket követően
19.		K16.001_O_16.1.1.1.1.(a)	a beszerzési szabályzat célja meghatározásra került a K16.001_P[3] szerint
20.		K16.001_O_16.1.1.1.1.(b)	a beszerzési szabályzat hatálya meghatározásra került a K16.001_P[3] szerint
21.		K16.001_O_16.1.1.1.1.(c)	a beszerzési szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K16.001_P[3] szerint
22.		K16.001_O_16.1.1.1.1.(d)	a beszerzési szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K16.001_P[3] szerint
23.		K16.001_O_16.1.1.1.1.(e)	a beszerzési szabályzatban foglalt célok iránti vezetői elkötelezettség rögzítésre került a K16.001_P[3] szerint
24.		K16.001_O_16.1.1.1.1.(f)	a beszerzési szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K16.001_P[3] szerint
25.		K16.001_O_16.1.1.1.1.(g)	a beszerzési szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K16.001_P[3] szerint
26.		K16.001_O_16.1.1.1.2.	a beszerzési szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	16.2. Erőforrások rendelkezésre állása	K16.002_O.16.2.1	a rendszerre vagy a rendszerszolgáltatásra vonatkozó magas szintű információbiztonsági követelményeket az üzletmenet és az üzleti folyamatok tervezése során határozták meg
28.		K16.002_O.16.2.2.(a)	a rendszer vagy a rendszerszolgáltatás védelméhez szükséges erőforrásokat a beruházás tervezés folyamat részeként határozták meg és dokumentálták
29.		K16.002_O.16.2.2.(b)	a rendszer vagy a rendszerszolgáltatás védelméhez szükséges erőforrásokat a beruházás tervezés folyamat részeként elosztják
30.		K16.002_O.16.2.3	a szervezeti programozási és költségvetési dokumentációban külön tételt hoztak létre az információbiztonságra
31.	16.3. A rendszer fejlesztési életciklusa	K16.003_P[1]	a rendszerfejlesztési életciklus meghatározásra került
32.		K16.003_O.16.3.1	a rendszer beszerzése, fejlesztése és kezelése a K16.003_P[1] szerinti rendszerfejlesztési életciklus alkalmazásával történik, amely magában foglalja az információbiztonsági megfontolásokat
33.		K16.003_O.16.3.2	az információbiztonsági szerepek és felelősségi körök meghatározásra és dokumentálásra kerültek a rendszerfejlesztési életciklus során
34.		K16.003_O.16.3.3	az információbiztonsági szerepkörrel és felelősségi körrel rendelkező személyek azonosításra kerültek
35.		K16.003_O.16.3.4	a szervezeti információbiztonsági kockázatmenedzsment folyamatok beépülnek a rendszerfejlesztési életciklus tevékenységeibe

36.	16.7. Beszerzések	K16.007_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {egységesített szerződés nyelvezet; a K16.007_P[1] szerinti szerződés nyelvezete}
37.		K16.007_O.16.7.1	a biztonsági funkcionális követelmények, leírások és kritériumok kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
38.		K16.007_O.16.7.2	a mechanizmusok erősségére vonatkozó követelmények, leírások és kritériumok kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
39.		K16.007_O.16.7.3	a biztonsági garanciális követelmények, leírások és kritériumok kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
40.		K16.007_O.16.7.4	a biztonsági követelmények, leírások és kritériumok teljesítéséhez szükséges védelmi intézkedések kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
41.		K16.007_O.16.7.5	a biztonsági dokumentáció követelményei, leírásai és kritériumai kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
42.		K16.007_O.16.7.6	a biztonsági dokumentáció védelmére vonatkozó követelmények, leírások és kritériumok kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
43.		K16.007_O.16.7.7	a rendszerfejlesztési környezet és annak a környezetnek a leírása, amelyben a rendszert működtetni kívánják kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
44.		K16.007_O.16.7.8.(a)	az információbiztonsági követelményekért, leírásokért és kritériumokért felelős felek felelősségi köre vagy azonosítása kifejezetten vagy hivatkozással szerepel a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
45.		K16.007_O.16.7.8.(b)	az ellátási lánc kockázatkezelési követelményekért, leírásokért és kritériumokért felelős felek felelősségi köre vagy azonosítása kifejezetten vagy hivatkozással szerepel a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
46.		K16.007_O.16.7.9	a teljesítési kritériumok leírásai kifejezetten vagy hivatkozással szerepelnek a K16.007_P[1] szerinti PARAMÉTER-ÉRTÉKEK használatával a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó beszerzési szerződésben
47.	16.8. Beszerzések – Alkalmazandó védelmi	K16.008_O.16.8	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírják, hogy adja meg a megvalósítandó védelmi intézkedések funkcionális tulajdonságainak leírását

	intézkedések funkcionális tulajdonságai		
48.	16.9. Beszerzések – Tervezési és megvalósítási információk a védelmi intézkedések teljesüléséhez	K16.009_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {biztonság szempontjából releváns külső rendszerinterfészek; magas szintű rendszerterv; alacsony szintű rendszerterv; forráskód vagy hardversémák; a K16.009_P[2] szerinti tervezési és megvalósítási információk}
49.		K16.009_P[2]	a tervezési és megvalósítási információk meghatározása (ha alkalmazható)
50.		K16.009_P[3]	a részletesség szintje meghatározott
51.		K16.009_O.16.9	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztőjét kötelezték olyan tervezési és megvalósítási információk szolgáltatására a védelmi intézkedésekhez, amelyek tartalmazzák a K16.009_P[1] szerinti PARAMÉTER-ÉRTÉKEK-et és a K16.009_P[3] szerinti részletességi szintű használatot
52.	16.11. Beszerzések - Rendszer, rendszerelem és szolgáltatás konfigurációk	K16.011_P[1]	a rendszer, rendszerelem vagy szolgáltatás biztonsági konfigurációi meghatározásra kerültek
53.		K16.011_O.16.11.1	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszert, rendszerelemet vagy szolgáltatást a K16.011_P[1] szerinti biztonsági konfigurációkkal együtt szállítsa
54.		K16.011_O.16.11.2	a konfigurációkat minden későbbi rendszer, rendszerelem vagy szolgáltatás újratelepítésénél vagy frissítésénél alapértelmezettként használják
55.	16.13. Beszerzések – Használatban lévő funkciók, portok, protokollok és szolgáltatások	K16.013_O.16.13.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy azonosítsa a szervezeti használatra szánt funkciókat
56.		K16.013_O.16.13.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy azonosítsa a szervezeti használatra szánt portokat
57.		K16.013_O.16.13.(c)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy azonosítsa a szervezeti használatra szánt protokollokat
58.		K16.013_O.16.13.(d)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy azonosítsa a szervezeti használatra szánt szolgáltatásokat
59.	16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció	K16.015_P[1]	a rendszer, a rendszerelem vagy a rendszerszolgáltatás dokumentációjának elérhetetlensége vagy hiánya esetén végrehajtandó lépések meghatározásra kerültek
60.		K16.015_P[2]	meghatározottak azok a személyek vagy szerepkörök, amelyekkel a rendszerdokumentáció megosztásra kerül
61.		K16.015_O.16.15.1.1.(a)	beszerzésre vagy kidolgozásra került a rendszer, rendszerelem vagy rendszerszolgáltatás rendszergazdai dokumentációja, amely leírja a rendszer, a rendszerelem vagy a szolgáltatás biztonságos konfigurációját
62.		K16.015_O.16.15.1.1.(b)	beszerzésre vagy kidolgozásra került a rendszer, rendszerelem vagy rendszerszolgáltatás rendszergazdai dokumentációja, amely leírja a rendszer, a rendszerelem vagy a szolgáltatás biztonságos telepítését
63.		K16.015_O.16.15.1.1.(c)	beszerzésre vagy kidolgozásra került a rendszer, rendszerelem vagy rendszerszolgáltatás rendszergazdai dokumentációja, amely leírja a rendszer, a rendszerelem vagy a szolgáltatás biztonságos üzemeltetését

64.		K16.015_O.16.15.1.2.(a)	beszerzésre vagy kidolgozásra került a rendszer, rendszerelem vagy rendszerszolgáltatás rendszergazdai dokumentációja, amely leírja a biztonsági funkciók és mechanizmusok hatékony használatát
65.		K16.015_O.16.15.1.2.(b)	beszerzésre vagy kidolgozásra került a rendszer, rendszerelem vagy rendszerszolgáltatás rendszergazdai dokumentációja, amely leírja a biztonsági funkciók és mechanizmusok hatékony karbantartását
66.		K16.015_O.16.15.1.3.(a)	beszerzésre vagy kidolgozásra került a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó rendszergazdai dokumentáció, amely ismerteti a rendszergazdai vagy privilegizált funkciók konfigurációjára vonatkozó ismert sérülékenységeket
67.		K16.015_O.16.15.1.3.(b)	beszerzésre vagy kidolgozásra került a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó rendszergazdai dokumentáció, amely ismerteti a rendszergazdai vagy privilegizált funkciókra vonatkozó ismert sérülékenységeket
68.		K16.015_O.16.15.2.1.(a)	beszerzésre vagy kidolgozásra került a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációja, amely leírja a felhasználó számára hozzáférhető biztonsági funkciókat és mechanizmusokat
69.		K16.015_O.16.15.2.1.(b)	beszerzésre vagy kidolgozásra került a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentáció, amely leírja, hogyan lehet hatékonyan használni a felhasználó által hozzáférhető biztonsági funkciókat és mechanizmusokat
70.		K16.015_O.16.15.2.2	beszerzésre vagy kidolgozásra került a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentáció, amely leírja a felhasználói interakció módszereit, amelyek lehetővé teszik az egyének számára a rendszer, rendszerelem vagy szolgáltatás biztonságosabb használatát
71.		K16.015_O.16.15.2.3	beszerzésre vagy kidolgozásra került a rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentáció, amely leírja a rendszer, rendszerelem vagy szolgáltatás biztonságának fenntartásával kapcsolatos felhasználói felelősséget
72.		K16.015_O.16.15.3.(a)	dokumentálták a rendszer, a rendszerelem vagy a rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, ha ilyen dokumentáció nem áll rendelkezésre vagy nem létezik
73.		K16.015_O.16.15.3.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérletek után, amikor az ilyen dokumentáció nem áll rendelkezésre vagy nem létezik, a K16.015_P[1] szerinti intézkedések kerültek végrehajtásra
74.		K16.015_O.16.15.4	a rendszerdokumentációt a K16.015_P[2] szerinti személyeknek és szerepköröknek eljuttatták
75.	16.16. Biztonságtervezési elvek	K16.016_P[1]	a rendszer biztonságtervezési elvei meghatározásra kerültek
76.		K16.016_O.16.16.(a)	a K16.016_P[1] szerinti rendszer és a rendszerelemek specifikációja során a rendszer biztonságtervezési elveit alkalmazzák
77.		K16.016_O.16.16.(b)	a K16.016_P[1] szerinti rendszer és a rendszerelemek tervezése során a rendszer biztonságtervezési elveit alkalmazzák

78.		K16.016_O.16.16.(c)	a K16.016_P[1] szerinti rendszer és a rendszerelemek fejlesztése során a rendszer biztonságtervezési elveit alkalmazzák
79.		K16.016_O.16.16.(d)	a K16.016_P[1] szerinti rendszer és a rendszerelemek megvalósítása során a rendszer biztonságtervezési elveit alkalmazzák
80.		K16.016_O.16.16.(e)	a K16.016_P[1] szerinti rendszer és a rendszerelemek módosítása során a rendszer biztonságtervezési elveit alkalmazzák
81.	16.49. Külső elektronikus információs rendszerek szolgáltatásai	K16.049_P[1]	a külső rendszerszolgáltatók által alkalmazandó védelmi intézkedések meghatározásra kerültek
82.		K16.049_P[2]	a külső szolgáltatók által végzett védelmi intézkedések megfelelőségének ellenőrzésére alkalmazott folyamatok, módszerek és technikák meghatározásra kerültek
83.		K16.049_O.16.49.1.(a)	a külső rendszerszolgáltatók megfelelnek a szervezeti biztonsági követelményeknek
84.		K16.049_O.16.49.1.(b)	a külső rendszerszolgáltatók a K16.049_P[1] szerinti védelmi intézkedéseket alkalmazzák
85.		K16.049_O.16.49.2.(a)	a külső rendszerszolgáltatókkal kapcsolatos szervezeti felügyeletet meghatározták és dokumentálták
86.		K16.049_O.16.49.2.(b)	a külső rendszerszolgáltatásokkal kapcsolatos felhasználói szerepek és felelősségi körök meghatározásra és dokumentálásra kerültek
87.		K16.049_O.16.49.3	a K16.049_P[2] szerinti folyamatokat, módszereket és technikákat alkalmaznak a külső szolgáltatók által végzett védelmi intézkedések betartásának folyamatos ellenőrzésére
88.	16.51. Külső információs rendszerek szolgáltatásai – Funkciók, portok, protokollok és szolgáltatások azonosítása	K16.051_O.16.51.(a)	a szervezet a rendszerszolgáltatások szolgáltatóinak előírta, hogy azonosítaniuk kell az ilyen szolgáltatások használatához szükséges funkciókat, portokat, protokollokat és egyéb szolgáltatásokat
89.		K16.051_O.16.51.(b)	a K16.051_O.16.51.(a)-val összhangban a szolgáltatások használatához szükséges funkciók, portok, protokollok és egyéb szolgáltatások azonosítottak
90.	16.58. Fejlesztői változáskövetés	K16.058_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {tervezés; fejlesztés; bevezetés; üzemeltetés; kivonás}
91.		K16.058_P[2]	a konfigurációkezelés alá tartozó konfigurációs elemek meghatározásra kerültek
92.		K16.058_P[3]	meghatározottak azok a személyek, akiknek a rendszerben, rendszerelemben vagy szolgáltatásban előforduló biztonsági hibákat és hibaelhárításokat jelentik
93.		K16.058_O.16.58.1	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy konfigurációkezelési folyamatokat alkalmazzon a rendszer, rendszerelem vagy szolgáltatás tekintetében a K16.058_P[1] szerinti PARAMÉTER-ÉRTÉKEK szerint
94.		K16.058_O.16.58.2.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője köteles dokumentálni a K16.058_P[2] szerinti konfigurációs elemek változásait biztosítva ezek sértetlenségét

95.		K16.058_O.16.58.2.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy kezelje a K16.058_P[2] szerinti konfigurációs elemek változásait biztosítva ezek sértetlenségét
96.		K16.058_O.16.58.2.(c)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy ellenőrizze a K16.058_P[2] szerinti konfigurációs elemek változásait biztosítva ezek sértetlenségét
97.		K16.058_O.16.58.3	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy csak a szervezet által jóváhagyott változtatásokat hajthatja végre a rendszerben, rendszerelemben vagy szolgáltatásban
98.		K16.058_O.16.58.4.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy dokumentálja a szervezet által jóváhagyott változtatásokat a rendszerben, rendszerelemben vagy szolgáltatásban
99.		K16.058_O.16.58.4.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy dokumentálja a szervezet által jóváhagyott változtatások lehetséges biztonsági hatásait a rendszerben, rendszerelemben vagy szolgáltatásban
100.		K16.058_O.16.58.5.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy nyomon kövesse a rendszerben, rendszerelemben vagy szolgáltatásban található biztonsági hibákat
101.		K16.058_O.16.58.5.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy nyomon kövesse a rendszerben, rendszerelemben vagy szolgáltatásban található biztonsági hibák javításait
102.		K16.058_O.16.58.5.(c)	a rendszer, a rendszerelem vagy a rendszerszolgáltatás fejlesztője számára előírták, hogy jelentse az észrevételeit a K16.058_P[3] által meghatározott személyeknek
103.	16.66. Fejlesztői biztonsági tesztelés	K16.066_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {egység-, integrációs-, rendszer-, illetve regressziós tesztelés}
104.		K16.066_P[2]	meghatározták a tesztelés, illetve értékelés elvégzésének gyakoriságát
105.		K16.066_P[3]	a K16.066_P[1] szerinti teszttípus mélysége és lefedettsége meghatározásra kerül
106.		K16.066_O.16.66.1.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában tervet dolgozzon ki a folyamatos biztonsági értékelésekre
107.		K16.066_O.16.66.1.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában hajtsa végre a tervet a folyamatos biztonsági értékelésekre
108.		K16.066_O.16.66.2	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden tervezés utáni szakaszában a K16.066_P[1] szerinti PARAMÉTER-ÉRTÉKEK szerint a K16.066_P[2] szerinti gyakorisággal a K16.066_P[3] szerinti mélységű és lefedettségű tesztelést, illetve értékelést végezzen
109.		K16.066_O.16.66.3.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában bizonyítékot szolgáltasson a biztonságértékelési terv végrehajtásáról

110.		K16.066_O.16.66.3.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában a tesztelés és értékelés eredményeit dokumentálja
111.		K16.066_O.16.66.4	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában ellenőrizhető hibajavítási folyamatot hajtson végre
112.		K16.066_O.16.66.5	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus minden, a tervezést követő szakaszában javítsa ki a tesztelés és értékelés során azonosított hibákat
113.	16.76. Fejlesztési folyamat, szabványok és eszközök	K16.076_P[1]	meghatározták, hogy milyen gyakorisággal kell felülvizsgálni a fejlesztési folyamatot, a szabványokat, az eszközöket, az eszközopciókat és az eszközkonfigurációkat
114.		K16.076_P[2]	a folyamat, a szabványok, az eszközök, az eszközopciók és az eszközkonfigurációk által teljesítendő biztonsági követelmények meghatározásra kerültek
115.		K16.076_O.16.76.2.1	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan dokumentált fejlesztési folyamatot kövessen, amely kifejezetten foglalkozik a biztonsági követelményekkel
116.		K16.076_O.16.76.2.2.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan dokumentált fejlesztési folyamatot kövessen, amely meghatározza a fejlesztési folyamat során alkalmazott szabványokat
117.		K16.076_O.16.76.2.2.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan dokumentált fejlesztési folyamatot kövessen, amely meghatározza a fejlesztési folyamat során alkalmazott eszközöket
118.		K16.076_O.16.76.2.3.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan dokumentált fejlesztési folyamatot kövessen, amely dokumentálja a fejlesztési folyamatban használt speciális eszközöket
119.		K16.076_O.16.76.2.3.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan dokumentált fejlesztési folyamatot kövessen, amely dokumentálja a fejlesztési folyamat során használt speciális eszközkonfigurációkat
120.		K16.076_O.16.76.2.4	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan dokumentált fejlesztési folyamatot kövessen, amely dokumentálja, kezeli és biztosítja a fejlesztés során alkalmazott folyamat, illetve eszközök változásainak sértetlenségét
121.		K16.076_O.16.76.3	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan dokumentált fejlesztési folyamatot kövessen, amelyben a fejlesztési folyamatot, szabványokat, eszközöket, eszközopciókat és eszközkonfigurációkat a K16.076_P[1] szerinti gyakorisággal felülvizsgálják annak megállapítása érdekében, hogy a kiválasztott és alkalmazott folyamat, szabványok, eszközök, eszközopciók és eszközkonfigurációk megfelelnek-e a K16.076_P[2] szerinti biztonsági követelményeknek
122.	16.79. Fejlesztési folyamat, szabványok és eszközök – Kritikussági elemzés	K16.079_P[1]	a rendszerfejlesztési életciklus döntési pontjai meghatározásra kerültek
123.		K16.079_P[2]	a kritikussági elemzés terjedelme meghatározásra került
124.		K16.079_P[3]	a kritikussági elemzés mélysége meghatározásra került

125.		K16.079_O.16.79.1	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a rendszerfejlesztési életciklus a K16.079_P[1] szerinti döntési pontjain kritikussági elemzést végezzen
126.		K16.079_O.16.79.2.(a)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a kritikussági elemzést a K16.079_P[3] szerinti mélységi szinten elvégezze a K16.079_P[2] szerinti terjedelem szerint
127.		K16.079_O.16.79.2.(b)	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a kritikussági elemzést a K16.079_P[3] szerinti mélységi szinten végezze el a K16.079_P[3] szerinti mélységben
128.	16.86. Szoftverfejlesztők oktatása	K16.086_P[1]	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője által biztosított biztonsági funkciók, szabályozások, illetve mechanizmusok helyes használatára és működtetésére vonatkozó képzés meghatározásra került
129.		K16.086_O.16.86	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy a K16.086_P[1] szerinti képzést biztosítson a bevezetett biztonsági funkciók, szabályozások, illetve mechanizmusok helyes használatáról és működtetéséről
130.	16.87. Fejlesztői biztonsági architektúra és tervezés	K16.087_O.16.87.1	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan tervezési specifikációt és biztonsági architektúrát készítsen, amely összhangban van a szervezet biztonsági architektúrájával, amely a szervezet vállalati architektúrájának szerves részét képezi
131.		K16.087_O.16.87.2	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan tervezési specifikációt és biztonsági architektúrát készítsen, amely pontosan és teljes körűen leírja a szükséges biztonsági funkciókat és a védelmi intézkedések fizikai és logikai összetevők közötti megosztását
132.		K16.087_O.16.87.3	a rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője számára előírták, hogy olyan tervezési specifikációt és biztonsági architektúrát készítsen, amely tartalmazza, hogy az egyes biztonsági funkciók, mechanizmusok és szolgáltatások hogyan működnek együtt a szükséges biztonsági követelmények és a védelem egységes megközelítése érdekében
133.	16.98. Külső fejlesztők háttérellenőrzése	K16.098_P[1]	meghatározott az a rendszer, rendszerelem, illetve rendszerszolgáltatás, amelyhez a fejlesztő hozzáférhet
134.		K16.098_P[2]	a fejlesztőre bízott feladatok meghatározásra kerültek
135.		K16.098_P[3]	átvilágítási kritériumokat határoztak meg a fejlesztő számára
136.		K16.098_O.16.98.1	a K16.098_P[1] szerinti rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője kizárólag a kijelölt K16.098_P[2] szerinti feladatoknak megfelelő hozzáférési jogosultságokkal rendelkezik
137.		K16.098_O.16.98.2	a K16.098_P[1] szerinti rendszer, rendszerelem vagy rendszerszolgáltatás fejlesztője megfelel a K16.098_P[3] szerinti további átvilágítási kritériumoknak
138.	16.99. Támogatással nem rendelkező rendszerelemek	K16.099_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {házon belüli támogatás; a K16.099_P[2] szerinti külső szolgáltatók általi támogatás}
139.		K16.099_P[2]	a támogatással már nem rendelkező rendszerelemekhez alternatív támogatást nyújtó külső szolgáltatók meghatározottak

140.		K16.099_O.16.99.1	a rendszerelemek cseréjére akkor kerül sor, ha a fejlesztő, a szállító vagy a gyártó már nem nyújt támogatást a rendszerelemekhez
141.		K16.099_O.16.99.2	a K16.099_P[1] szerinti PARAMÉTER-ÉRTÉKEK szerinti erőforrásokat biztosít a nem támogatott rendszerelemek folyamatos támogatására

17. Rendszer- és kommunikációvédelem

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	17.1. Szabályzat és eljárásrendek	K17.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a rendszer- és kommunikációvédelmi szabályzatot meg kell ismertetni
3.		K17.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a rendszer- és kommunikációvédelmi eljárásokat meg kell ismertetni
4.		K17.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K17.001_P[4]	a rendszer- és kommunikációvédelmi szabályzat és eljárások irányítására egy meghatározott személyt kijelölésre került
6.		K17.001_P[5]	a rendszer- és kommunikációvédelmi szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K17.001_P[6]	meghatározták azokat az eseményeket, amelyek a rendszer- és kommunikációvédelmi szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K17.001_P[7]	meghatározták a rendszer- és kommunikációvédelmi eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K17.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a rendszer- és kommunikációvédelmi eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K17.001_O_17.1.1.(a)	rendszer- és kommunikációvédelmi szabályzatot dolgoztak ki és dokumentáltak
11.		K17.001_O_17.1.1.(b)	a rendszer- és kommunikációvédelmi szabályzatot megismertették a K17.001_P[1] szerinti személyekkel vagy szerepkörökkel
12.		K17.001_O_17.1.1.(c)	a rendszer- és kommunikációvédelmi szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő rendszer- és kommunikációvédelmi eljárások kidolgozásra és dokumentálásra kerültek

13.		K17.001_O_17.1.1.(d)	a rendszer- és kommunikációvédelmi eljárások ismertetésre kerültek a K17.001_P[2] szerinti személyekkel vagy szerepkörökkel
14.		K17.001_O_17.1.2	a K17.001_P[4] szerinti személyt kijelölték a rendszer- és kommunikációvédelmi szabályzat és eljárások kidolgozásának, dokumentálásának és ismertetésének irányítására
15.		K17.001_O_17.1.3.(a)	a rendszer- és kommunikációvédelmi szabályzatot felülvizsgálják és frissítik a K17.001_P[5] szerinti gyakorisággal
16.		K17.001_O_17.1.3.(b)	a rendszer- és kommunikációvédelmi szabályzatot felülvizsgálják és frissítik a K17.001_P[6] szerinti eseményeket követően
17.		K17.001_O_17.1.3.(c)	a rendszer- és kommunikációvédelmi eljárásokat felülvizsgálják és frissítik a K17.001_P[7] szerinti gyakorisággal
18.		K17.001_O_17.1.3.(d)	a rendszer- és kommunikációvédelmi eljárásokat felülvizsgálják és frissítik a K17.001_P[8] szerinti eseményeket követően
19.		K17.001_O_17.1.1.1.1.(a)	a rendszer- és kommunikációvédelmi szabályzat célja meghatározásra került a K17.001_P[3] szerint
20.		K17.001_O_17.1.1.1.1.(b)	a rendszer- és kommunikációvédelmi szabályzat hatálya meghatározásra került a K17.001_P[3] szerint
21.		K17.001_O_17.1.1.1.1.(c)	a rendszer- és kommunikációvédelmi szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K17.001_P[3] szerint
22.		K17.001_O_17.1.1.1.1.(d)	a rendszer- és kommunikációvédelmi szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K17.001_P[3] szerint
23.		K17.001_O_17.1.1.1.1.(e)	a rendszer- és kommunikációvédelmi szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K17.001_P[3] szerint
24.		K17.001_O_17.1.1.1.1.(f)	a rendszer- és kommunikációvédelmi szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K17.001_P[3] szerint
25.		K17.001_O_17.1.1.1.1.(g)	a rendszer- és kommunikációvédelmi szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K17.001_P[3] által meghatározottak szerint
26.		K17.001_O_17.1.1.1.2.	a rendszer- és kommunikációvédelmi szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	17.2. Rendszer és felhasználói funkciók szétválasztása	K17.002_O.17.2	a felhasználói funkciók, beleértve a felhasználói interfész-szolgáltatásokat is, elkülönülnek a rendszer üzemeltetési funkcióktól
28.	17.4. Biztonsági funkciók elkülönítése	K17.004_O.17.4	a biztonsági funkciók el különítésre kerültek a nem biztonsági funkcióktól
29.	17.10. Információk az osztott használatú rendszererőforrásokban	K17.010_O.17.10.(a)	a szervezet megakadályozza a jogosulatlan információátvitelt a megosztott rendszererőforrásokon keresztül
30.		K17.010_O.17.10.(b)	a szervezet megakadályozza a véletlen információátvitelt a megosztott rendszererőforrásokon keresztül

31.	17.12. Szolgáltatás-megtagadással járó támadások elleni védelem	K17.012_P[1]	meghatározottak a szolgáltatásmegtagadási események típusai, amelyek ellen védelmet vagy korlátozást kell alkalmazni
32.		K17.012_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került:{védekezés; korlátozás}
33.		K17.012_P[3]	a szolgáltatásmegtagadás elleni védelmi cél eléréséhez szükséges védelmi intézkedések a szolgáltatásmegtagadási esemény típusa szerint kerülnek meghatározásra
34.		K17.012_O.17.12.1	a szervezet a K17.012_P[1] által meghatározott típusú szolgáltatásmegtagadási események hatásaival szemben a K17.012_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK szerint védekezik
35.		K17.012_O.17.12.2	a K17.012_P[3] szerinti szolgáltatásmegtagadási esemény típusa szerinti védelmi intézkedéseket alkalmaznak a szolgáltatásmegtagadási védelmi cél elérése érdekében
36.	17.17. A határok védelme	K17.017_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került:{fizikailag; logikailag}
37.		K17.017_O.17.17.1.(a)	a rendszer külső interfészeinek kommunikációját ellenőrzik
38.		K17.017_O.17.17.1.(b)	a rendszeren belüli kulcsfontosságú belső interfészek kommunikációját ellenőrzik
39.		K17.017_O.17.17.2	a nyilvánosan hozzáférhető rendszerelemek alhálózatai a K17.017_P[1] szerinti PARAMÉTER-ÉRTÉKEK szerint elkülönülnek a belső szervezeti hálózatoktól
40.		K17.017_O.17.17.3	külső hálózatokhoz vagy rendszerekhez csak a szervezeti biztonsági architektúrával összhangban elhelyezett határvédelmi eszközökből álló menedzselt interfészeken keresztül lehet csatlakozni
41.	17.18. A határok védelme – Hozzáférési pontok	K17.018_O.17.18	a rendszerhez csatlakoztatható külső hálózati kapcsolatok száma korlátozott
42.	17.19. A határok védelme – Külső infokommunikációs szolgáltatások	K17.019_P[1]	meghatározták, hogy milyen gyakorisággal kell felülvizsgálni a forgalmi áramlási szabályzat alóli kivételeket
43.		K17.019_O.17.19.1	minden egyes külső infokommunikációs szolgáltatáshoz egy kezelt interfészt alkalmaznak
44.		K17.019_O.17.19.2	minden egyes kezelt interfészhez forgalomáramlási házirendet alkalmaznak
45.		K17.019_O.17.19.3.(a)	az egyes interfészeken keresztül továbbított információk bizalmassága védett
46.		K17.019_O.17.19.3.(b)	az egyes interfészeken keresztül továbbított információk sértetlensége védett
47.		K17.019_O.17.19.4	a forgalomáramlási szabályzat alóli minden egyes kivételt dokumentáltak az azt alátámasztó működési vagy üzleti igény és az igény időtartamának megjelölésével
48.		K17.019_O.17.19.5.(a)	a forgalomáramlási szabályzat alóli kivételek felülvizsgálata a K17.019_P[1] szerinti gyakorisággal történik
49.		K17.019_O.17.19.5.(b)	a forgalomáramlási szabályzat alóli azon kivételek, amelyeket már nem támogat kifejezett működési vagy üzleti igény, eltávolításra kerülnek
50.		K17.019_O.17.19.6	a vezérlőadat forgalmának külső hálózatokkal való illetéktelen cseréje megakadályozásra kerül

51.		K17.019_O.17.19.7	információkat tesznek közzé, hogy a távoli hálózatok számára lehetővé tegyék a belső hálózatokból érkező, nem engedélyezett vezérlőadat forgalom észlelését
52.		K17.019_O.17.19.8	a külső hálózatokból kiszűrésre kerül a nem engedélyezett vezérlőadat forgalom
53.	17.20. A határok védelme – Alapértelmezés szerinti elutasítás és kivétel alapú engedélyezés	K17.020_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {menedzselt interfészeken; a K17.020_P[2] szerinti rendszerek esetében}
54.		K17.020_P[2]	meghatározásra kerültek azok a rendszerek, amelyek esetében a hálózati kommunikációs forgalom alapértelmezés szerint nem engedélyezett, illetve amelyek esetében a hálózati kommunikációs forgalom kivételesen engedélyezett (ha alkalmazható)
55.		K17.020_O.17.20.(a)	a hálózati kommunikációs forgalom alapértelmezés szerint elutasításra kerül a K17.020_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK szerint
56.		K17.020_O.17.20.(b)	a hálózati kommunikációs forgalom kivételesen engedélyezett a K17.020_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK szerint
57.	17.21. A határok védelme – Megosztott csatornahasználat távoli eszközök esetén	K17.021_P[1]	a megosztott csatorna biztonságos konfigurálásához szükséges védelmi intézkedéseket meghatározták
58.		K17.021_O.17.21	a szervezeti rendszerekhez csatlakozó távoli eszközök esetében a megosztott csatorna létrehozása nem lehetséges, kivéve, ha a megosztott csatorna biztonságos módon, a K17.021_P[1] szerinti védelmi intézkedésekkel van biztosítva
59.	17.22. A határok védelme – A forgalom átirányítása hitelesített proxykiszolgálókra	K17.022_P[1]	a külső hálózatok felé továbbítandó belső kommunikációs forgalom meghatározásra került
60.		K17.022_P[2]	meghatározták azokat a külső hálózatokat, amelyek felé a belső kommunikációs forgalmat továbbítani kell
61.		K17.022_O.17.22	a K17.022_P[1] szerinti belső kommunikációs forgalmat a K17.022_P[2] szerinti külső hálózatok felé a menedzselt interfészek hitelesített proxy-kiszolgálóin keresztül irányítják
62.	17.32. A határok védelme – Biztonságos állapot fenntartása	K17.032_O.17.32	a rendszereket megakadályozzák abban, hogy egy határvédelmi berendezés működési hibája esetén nem biztonságos állapotba kerüljenek
63.	17.35. A határok védelme – Rendszerelemek elkülönítése	K17.035_P[1]	a határvédelmi mechanizmusok által elkülönítendő rendszerelemeket meghatározták
64.		K17.035_P[2]	a határvédelmi mechanizmusokkal elkülönített rendszerelemek által támogatandó célok, illetve üzleti funkciók meghatározásra kerültek
65.		K17.035_O.17.35	határvédelmi mechanizmusokat alkalmaznak a K17.035_P[1] szerinti rendszerelemek elkülönítésére, amelyek a K17.035_P[2] által meghatározott célokat, illetve üzleti funkciókat támogatják
66.	17.40. Az adatátvitel bizalmassága és sértetlensége	K17.040_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {bizalmasság; sértetlenség}
67.		K17.040_O.17.40	a továbbított információk a K17.040_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK szerint védettek

68.	17.41. Az adatátvitel bizalmassága és sértetlensége – Kriptográfiai védelem	K17.041_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {az információ jogosulatlan nyilvánosságra hozatalának megelőzése; az információban bekövetkezett módosítások észlelése}
69.		K17.041_O.17.41	a K17.041_P[1] szerinti PARAMÉTER-ÉRTÉKEK átvitele során kriptográfiai mechanizmusokat alkalmaznak
70.	17.46. A hálózati kapcsolat megszakítása	K17.046_P[1]	meghatározták azt az inaktivitási időtartamot, amely után a rendszer megszakítja a kommunikációs munkaszakaszhoz kapcsolódó hálózati kapcsolatot
71.		K17.046_O.17.46	a kommunikációs munkaszakaszhoz kapcsolódó hálózati kapcsolat a munkaszakasz befejezésekor vagy a K17.046_P[1] szerinti inaktivitás után megszakad
72.	17.49. Kriptográfiai kulcs előállítása és kezelése	K17.049_P[1]	a kriptográfiai kulcsok előállítására, szétosztására, tárolására, hozzáférésére és megsemmisítésére vonatkozó követelmények meghatározásra kerültek
73.		K17.049_O.17.49.(a)	a kriptográfiai kulcsok a K17.049_P[1] szerinti követelményeknek megfelelően kerülnek előállításra
74.		K17.049_O.17.49.(b)	a kriptográfiai kulcsokat a K17.049_P[1] szerinti követelményeknek megfelelően kezelik
75.	17.50. Kriptográfiai kulcs előállítása és kezelése – Rendelkezésre állás	K17.050_O.17.50	az információk rendelkezésre állása megmarad abban az esetben is, ha a felhasználók elveszítik a kriptográfiai kulcsokat
76.	17.53. Kriptográfiai védelem	K17.053_P[1]	kriptográfiai felhasználási módok meghatározásra kerültek
77.		K17.053_P[2]	a szervezet által támogatott kriptográfia megoldások meghatározottak
78.		K17.053_O.17.53.2	a szervezet a K17.053_P[2] szerinti kriptográfiai megoldásokat alkalmazza a K17.053_P[1] felhasználási módokon
79.	17.54. Együttműködésen alapuló informatikai eszközök	K17.054_P[1]	meghatározták azokat a kivételeket, amelyek esetében a távoli aktiválást engedélyezni kell
80.		K17.054_O.17.54.1	az együttműködésen alapuló informatikai eszközök és alkalmazások távoli aktiválása nem lehetséges, kivéve a K17.054_P[1] szerinti kivételeket, ahol a távoli aktiválás megengedett
81.		K17.054_O.17.54.2	az eszközöknél fizikailag jelen lévő felhasználók számára a távoli aktiválásról visszajelzés küldésére kerül sor
82.	17.62. Nyilvános kulcsú infrastruktúra tanúsítványok	K17.062_P[1]	a nyilvános kulcsú tanúsítványok kiállítására a vonatkozó tanúsítványkiadási szabályok szerint került sor
83.		K17.062_O.17.62.1	a nyilvános kulcsú tanúsítványokat a K17.062_P[1] szerinti tanúsítványkiadási szabályok szerint állítják ki, vagy a nyilvános kulcsú tanúsítványokat bizalmi szolgáltatótól szerzik be
84.		K17.062_O.17.62.2	csak jóváhagyott hitelesített tanúsítványok szerepelnek a szervezet által kezelt tanúsítványtárolókban
85.	17.63. Mobilkód korlátozása	K17.063_O.17.63.1.(a)	az elfogadható mobilkód meghatározásra került
86.		K17.063_O.17.63.1.(b)	a nem elfogadható mobilkód meghatározásra került
87.		K17.063_O.17.63.1.(c)	az elfogadható mobilkód technológia meghatározásra került
88.		K17.063_O.17.63.1.(d)	a nem elfogadható mobilkód technológia meghatározásra került

89.		K17.063_O.17.63.2.(a)	a mobilkód használata engedélyezett a rendszerben
90.		K17.063_O.17.63.2.(b)	a mobilkód használatát a rendszerben felügyelik
91.		K17.063_O.17.63.2.(c)	a mobilkód használatát a rendszerben ellenőrzik
92.	17.69. Biztonságos név/cím feloldási szolgáltatás (hiteles forrás)	K17.069_O.17.69.1.(a)	további adatok eredetének hitelesítése a hiteles névfeloldási adatokkal együtt történik, amelyeket a rendszer a külső név-, illetve címfeloldási lekérdezésekre adott válaszként ad vissza
93.		K17.069_O.17.69.1.(b)	a tartalom sértetlenségére vonatkozó kiegészítő adatok a hiteles névfeloldási adatokkal együtt kerülnek rendelkezésre bocsátásra, amelyeket a rendszer a külső név-, illetve címfeloldási lekérdezésekre adott válaszként ad vissza
94.		K17.069_O.17.69.2.(a)	ha az EIR elosztott, hierarchikus névtér részeként működik, a gyermektartományok biztonsági állapota jelzett
95.		K17.069_O.17.69.2.(b)	a szülő- és a gyermektartományok közötti bizalmi lánc ellenőrzését biztonságos névfeloldási szolgáltatások támogatják.
96.	17.71. Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)	K17.071_O.17.71.(a)	a rendszer a hiteles forrásokból érkező név-, illetve címfeloldási válaszokhoz kéri az adatok eredetének hitelesítését
97.		K17.071_O.17.71.(b)	a rendszer a hiteles forrásokból érkező név-, illetve címfeloldási válaszokon elvégzi az adatok eredetének hitelesítését
98.		K17.071_O.17.71.(c)	a rendszer a hiteles forrásokból érkező név-, illetve címfeloldási válaszokon kéri az adatok sértetlenségének ellenőrzését
99.		K17.071_O.17.71.(d)	a rendszer a hiteles forrásokból érkező név-, illetve címfeloldási válaszokon elvégzi az adatok sértetlenségének ellenőrzését
100.	17.72. Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	K17.072_O.17.72.(a)	a név-, illetve címfeloldási szolgáltatásokat együttesen biztosító rendszerek hibatűrőek
101.		K17.072_O.17.72.(b)	azok a rendszerek, amelyek együttesen nyújtanak név-, illetve címfeloldási szolgáltatásokat a szervezet számára, belső szerepkörök szétválasztását hajtják végre
102.		K17.072_O.17.72.(c)	azok a rendszerek, amelyek együttesen nyújtanak név-, illetve címfeloldási szolgáltatásokat a szervezet számára, külső szerepkörök szétválasztását hajtják végre
103.	17.73. Munkaszakasz hitelessége	K17.073_O.17.73	a kommunikációs munkaszakaszok hitelessége védett
104.	17.77. Ismert állapotba való visszatérés	K17.077_P[1]	meghatározásra kerültek a rendszer meghibásodásainak típusai, amelyek esetében a rendszerelemek ismert állapotba kerülnek
105.		K17.077_P[2]	meghatározott az a rendszerállapot, amelybe a rendszerelemek rendszerhiba esetén visszaállnak
106.		K17.077_P[3]	a rendszer meghibásodása esetén megőrzendő rendszerállapot információkat meghatározták

107.		K17.077_O.17.77	a K17.077_P[1] által meghatározott típusú rendszerhibák esetén a rendszerelemek a K17.077_P[2] által meghatározott ismert rendszerállapot szerinti, a K17.077_P[3] szerinti rendszerállapotra vonatkozó információkat a megőrzik
108.	17.81. Tárolt (at rest) adatok védelme	K17.081_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {bizalmasság; sértetlenség}
109.		K17.081_P[2]	a védelmet igénylő, tárolt, illetve archivált (at rest) állapotban lévő információk meghatározásra kerültek
110.		K17.081_O.17.81	a K17.081_P[1] által meghatározott PARAMÉTER-ÉRTÉKEK szerint a K17.081_P[2] által meghatározott tárolt, illetve archivált (at rest) információk védettek
111.	17.82. Tárolt (at rest) adatok védelme – Kriptográfiai védelem	K17.082_P[1]	a kriptográfiai védelmet igénylő információk meghatározásra kerültek
112.		K17.082_P[2]	a kriptográfiai védelmet igénylő rendszerelemek vagy adathordozók meghatározásra kerültek
113.		K17.082_O.17.82.(a)	a K17.082_P[1] szerinti rendszerelemeken vagy adathordozókon tárolt, a K17.082_P[2] szerinti információk jogosulatlan felfedésének megelőzésére kriptográfiai mechanizmusokat alkalmaznak
114.		K17.082_O.17.82.(b)	a K17.082_P[1] szerinti rendszerelemeken vagy adathordozókon tárolt, a K17.082_P[2] szerinti információk jogosulatlan módosításának megelőzésére kriptográfiai mechanizmusokat alkalmaznak
115.	17.108. A folyamatok elkülönítése	K17.108_O.17.108	minden egyes végrehajtó rendszerfolyamathoz külön végrehajtási tartományt tartanak fenn

18. Rendszer- és információsértetlenség

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmények**
2.	18.1. Szabályzat és eljárásrendek	K18.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a rendszer- és információsértetlenségi szabályzatot meg kell ismertetni
3.		K18.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel a rendszer- és információsértetlenségi eljárásokat meg kell ismertetni
4.		K18.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K18.001_P[4]	a rendszer- és információsértetlenségi szabályzat és eljárások irányítására egy meghatározott személy került kijelölésre
6.		K18.001_P[5]	a rendszer- és információsértetlenségi szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került

7.		K18.001_P[6]	meghatározták azokat az eseményeket, amelyek a rendszer- és információsértetlenségi szabályzat felülvizsgálatát és aktualizálását teszik szükségessé
8.		K18.001_P[7]	meghatározták a rendszer- és információsértetlenségi eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K18.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt a rendszer- és információsértetlenségi eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K18.001_O_18.1.1.(a)	rendszer- és információsértetlenségi szabályzatot dolgoztak ki és dokumentáltak
11.		K18.001_O_18.1.1.(b)	a rendszer- és információsértetlenségi szabályzatot megismertették a K18.001_P[1] szerinti személyekkel vagy szerepkörökkel
12.		K18.001_O_18.1.1.(c)	a rendszer- és információsértetlenségi szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő rendszer- és információsértetlenségi eljárások kidolgozásra és dokumentálásra kerültek
13.		K18.001_O_18.1.1.(d)	a rendszer- és információsértetlenségi eljárások ismertetésre kerültek a K18.001_P[2] szerinti személyekkel vagy szerepkörökkel
14.		K18.001_O_18.1.2	a K18.001_P[4] szerinti személyt kijelölték a rendszer- és információsértetlenségi szabályzat és eljárások kidolgozásának, dokumentálásának és ismertetésének irányítására
15.		K18.001_O_18.1.3.(a)	a rendszer- és információsértetlenségi szabályzatot felülvizsgálják és frissítik a K18.001_P[5] szerinti gyakorisággal
16.		K18.001_O_18.1.3.(b)	a rendszer- és információsértetlenségi szabályzatot felülvizsgálják és frissítik a K18.001_P[6] szerinti eseményeket követően
17.		K18.001_O_18.1.3.(c)	a rendszer- és információsértetlenségi eljárásokat felülvizsgálják és frissítik a K18.001_P[7] szerinti gyakorisággal
18.		K18.001_O_18.1.3.(d)	a rendszer- és információsértetlenségi eljárásokat felülvizsgálják és frissítik a K18.001_P[8] szerinti eseményeket követően
19.		K18.001_O_18.1.1.1.1.(a)	a rendszer- és információsértetlenségi szabályzat célja meghatározásra került a K18.001_P[3] szerint
20.		K18.001_O_18.1.1.1.1.(b)	a rendszer- és információsértetlenségi szabályzat hatálya meghatározásra került a K18.001_P[3] szerint
21.		K18.001_O_18.1.1.1.1.(c)	a rendszer- és információsértetlenségi szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K18.001_P[3] szerint
22.		K18.001_O_18.1.1.1.1.(d)	a rendszer- és információsértetlenségi szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K18.001_P[3 szerint
23.		K18.001_O_18.1.1.1.1.(e)	a rendszer- és információsértetlenségi szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K18.001_P[3] szerint
24.		K18.001_O_18.1.1.1.1.(f)	a rendszer- és információsértetlenségi szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K18.001_P[3] szerint

25.		K18.001_O_18.1.1.1.1.(g)	a rendszer- és információsértetlenségi szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K18.001_P[3] szerint
26.		K18.001_O_18.1.1.1.2.	a rendszer- és információsértetlenségi szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	18.2. Hibajavítás	K18.002_P[1]	meghatározták azt az időtartamot, amelyen belül a biztonsági szempontból fontos szoftverfrissítéseket a frissítések kiadását követően telepíteni kell
28.		K18.002_O.18.2.1.(a)	a rendszer hibáinak azonosítása megtörtént
29.		K18.002_O.18.2.1.(b)	a rendszer hibáinak jelentése megtörtént
30.		K18.002_O.18.2.1.(c)	a rendszer hibáinak javítása megtörtént
31.		K18.002_O.18.2.2.(a)	a hibajavítással kapcsolatos szoftverfrissítések hatékonyságát a telepítés előtt tesztelték
32.		K18.002_O.18.2.2.(b)	a hibajavításhoz kapcsolódó szoftverfrissítéseket telepítés előtt tesztelték a lehetséges mellékhatások szempontjából
33.		K18.002_O.18.2.3	a biztonság szempontjából releváns szoftverfrissítéseket a frissítések kiadásától számított a K18.002_P[1] szerinti időtartamon belül telepítették
34.	18.3. Hibajavítás – Automatizált hibaelhárítás állapota	K18.003_P[1]	automatizált mechanizmusokat határoztak meg annak megállapítására, hogy a rendszerelemekre telepítve vannak-e a vonatkozó biztonsági szempontból releváns szoftver- és firmware-frissítések
35.		K18.003_P[2]	meghatározták, hogy milyen gyakorisággal kell megállapítani, hogy a rendszerelemekre telepítve vannak-e a biztonság szempontjából releváns szoftver- és firmware-frissítések
36.		K18.003_O.18.3	a rendszerelemek a vonatkozó biztonsági szempontból releváns szoftver- és firmware-frissítésekkel rendelkeznek, amelyeket a K18.003_P[2] szerinti gyakorisággal telepítenek a K18.003_P[1] szerinti automatizált mechanizmusokat alkalmazásával
37.	18.8. Kártékony kódok elleni védelem	K18.008_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {aláírás-alapú; nem aláírás-alapú}
38.		K18.008_P[2]	meghatározott, hogy a kártékony kódok elleni védelmi vizsgálati mechanizmusokat milyen gyakorisággal alkalmazzák
39.		K18.008_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {végpont; hálózati belépési és kilépési pontok}
40.		K18.008_P[4]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {blokkolja a kártékony kódot; karanténba helyezi a kártékony kódot; megteszi a K18.008_P[5] szerinti egyéb intézkedéseket}
41.		K18.008_P[5]	a kártékony kód észlelésére válaszul végrehajtandó művelet meghatározásra került
42.		K18.008_P[6]	a kártékony kód észlelésekor riasztandó személyek vagy szerepkörök meghatározásra kerültek

43.		K18.008_O.18.8.1.(a)	a K18.008_P[1] szerinti PARAMÉTER-ÉRTÉKEK szerint a kártékony kódok elleni védelmi mechanizmusokat alkalmaznak a rendszer belépési és kilépési pontjain a rosszindulatú kódok észlelésére
44.		K18.008_O.18.8.1.(b)	a rendszer belépési és kilépési pontjain a szervezet a K18.008_P[1] szerinti PARAMÉTER-ÉRTÉKEK szerinti mechanizmusokat alkalmazza
45.		K18.008_O.18.8.2	a kártékony kódok elleni védelmi mechanizmusok automatikusan frissülnek, amint új verziók állnak rendelkezésre a szervezeti konfigurációkezelési irányelvekkel és eljárásokkal összhangban
46.		K18.008_O.18.8.3.1.(a)	a kártékony kódok elleni védelmi mechanizmusok úgy vannak konfigurálva, hogy a rendszer a K18.008_P[2] szerinti gyakorisággal időszakos vizsgálatokat végezzen
47.		K18.008_O.18.8.3.1.(b)	a kártékony kódok elleni védelmi mechanizmusok úgy vannak konfigurálva, hogy a külső forrásból származó fájlok valós idejű vizsgálatát a K18.008_P[3] szerinti PARAMÉTER-ÉRTÉKEK szerinti időpontban végzik, amikor a fájlokat a szervezeti irányelveknek megfelelően letöltik, megnyitják vagy futtatják
48.		K18.008_O.18.8.3.2.(a)	a kártékony kódok elleni védelmi mechanizmusok úgy vannak konfigurálva, hogy a rosszindulatú kód észlelésére válaszul reagálnak a K18.008_P[4] szerinti PARAMÉTER-ÉRTÉKEK szerint
49.		K18.008_O.18.8.3.2.(b)	a kártékony kódok elleni védelmi mechanizmusok úgy vannak konfigurálva, hogy rosszindulatú kód észlelése esetén riasztásokat küldjenek a K18.008_P[6] szerinti személyeknek vagy szerepköröknek
50.		K18.008_O.18.8.4	a kártékony kódok észlelése és megsemmisítése során kapott téves pozitív eredmények és az ebből eredő, a rendszer rendelkezésre állására gyakorolt lehetséges hatások kezelésre kerülnek
51.	18.13. Az EIR monitorozása	K18.013_P[1]	az EIR elleni támadások és a potenciális támadások jeleinek észlelésére irányuló felügyeleti célok meghatározásra kerültek
52.		K18.013_P[2]	az EIR jogosulatlan használatának azonosítására használt technikák és módszerek meghatározásra kerültek
53.		K18.013_P[3]	a személyek vagy a szerepkörök számára nyújtandó rendszerfelügyeleti információk meghatározásra kerültek
54.		K18.013_P[4]	meghatározták azokat a személyeket vagy szerepköröket, akiknek a rendszerfelügyeleti információkat át kell adni
55.		K18.013_P[5]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {a K18.013_P[6] szerinti gyakoriság}
56.		K18.013_P[6]	a személyek vagy a szerepkörök számára történő rendszerfelügyelet biztosításának gyakorisága meghatározott
57.		K18.013_O.18.13.1.1	az EIR-t a K18.013_P[1] szerinti felügyeleti célokkal összhangban a támadások és a lehetséges támadásokra utaló jelek észlelése érdekében monitorozzák
58.		K18.013_O.18.13.1.2.(a)	az EIR-t az engedély nélküli helyi kapcsolatok észlelése érdekében monitorozzák
59.		K18.013_O.18.13.1.2.(b)	az EIR-t az engedély nélküli hálózati kapcsolatok észlelése érdekében monitorozzák
60.		K18.013_O.18.13.1.2.(c)	az EIR-t az engedély nélküli távoli kapcsolatok észlelése érdekében monitorozzák
61.		K18.013_O.18.13.2	az EIR jogosulatlan használatát a K18.013_P[2] szerinti technikák és módszerek segítségével azonosítják

62.		K18.013_O.18.13.3.1	belső felügyeleti képességeket hívnak életre, vagy felügyeleti eszközöket helyeznek el az EIR-en belül a szervezet által meghatározott alapvető információk összegyűjtésére
63.		K18.013_O.18.13.3.2	belső felügyeleti képességeket hívnak életre, vagy felügyeleti eszközöket helyeznek el az EIR-en belüli ad hoc helyekre, hogy nyomon kövessék a tranzakciók bizonyos típusait
64.		K18.013_O.18.13.4.(a)	az észlelt eseményeket elemzik
65.		K18.013_O.18.13.4.(b)	az észlelt rendellenességeket elemzik
66.		K18.013_O.18.13.5	a rendszerfelügyeleti tevékenység szintjét módosítják, ha a szervezeti műveletekre és eszközökre, egyénekre vagy a külső szervezetekre vonatkozó kockázat megváltozik
67.		K18.013_O.18.13.6	jogi állásfoglalást szereznek be a rendszerfelügyeleti tevékenységekkel kapcsolatban
68.		K18.013_O.18.13.7	a szervezet a K18.013_P[3] szerinti rendszerfelügyeleti információkat K18.013_P[4] szerinti személyek és szerepkörök számára a K18.013_P[5] által meghatározott PARAMÉTER-ÉRTÉKEK szerint biztosítja
69.	18.15. Az EIR monitorozása – Automatizált eszközök és mechanizmusok valós idejű elemzéshez	K18.015_O.18.15	automatizált eszközöket és mechanizmusokat alkalmaznak az események közel valós idejű elemzésének támogatására
70.	18.17. Az EIR monitorozása – Bejövő és kimenő kommunikációs forgalom	K18.017_P[1]	meghatározták azt a gyakoriságot, amellyel a bejövő kommunikációs forgalmat szokatlan vagy nem engedélyezett tevékenységek vagy körülmények szempontjából ellenőrizni szükséges
71.		K18.017_P[2]	a bejövő kommunikációs forgalomban azonosítandó szokatlan vagy nem engedélyezett tevékenységek vagy körülmények meghatározásra kerültek
72.		K18.017_P[3]	meghatározták azt a gyakoriságot, amellyel a kimenő kommunikációs forgalmat szokatlan vagy nem engedélyezett tevékenységek vagy körülmények szempontjából ellenőrizni szükséges
73.		K18.017_P[4]	a kimenő kommunikációs forgalomban azonosítandó szokatlan vagy nem engedélyezett tevékenységek vagy körülmények meghatározásra kerültek
74.		K18.017_O.18.17.1.(a)	a bejövő kommunikációs forgalomra vonatkozó szokatlan vagy nem engedélyezett tevékenységekre vagy feltételekre vonatkozó kritériumok meghatározásra kerültek
75.		K18.017_O.18.17.1.(b)	a kimenő kommunikációs forgalomra vonatkozó szokatlan vagy nem engedélyezett tevékenységekre vagy feltételekre vonatkozó kritériumok meghatározásra kerültek
76.		K18.017_O.18.17.2.(a)	a bejövő kommunikációs forgalmat a K18.017_P[1] szerinti gyakorisággal ellenőrzik a K18.017_P[2] szerinti szokatlan vagy nem engedélyezett tevékenységek vagy feltételek szempontjából
77.		K18.017_O.18.17.2.(b)	a kimenő kommunikációs forgalmat a K18.017_P[3] szerinti gyakorisággal ellenőrzik a K18.017_P[4] szerinti szokatlan vagy nem engedélyezett tevékenységek vagy feltételek szempontjából
78.		K18.018_P[1]	a kompromittálódásra utaló jelek esetén riasztandó személyek vagy szerepkörök meghatározásra kerültek

79.	18.18. Az EIR monitorozása – Rendszer által generált riasztások	K18.018_P[2]	az indikátorok meghatározásra kerültek
80.		K18.018_O.18.18	a K18.018_P[1] szerinti személyek vagy szerepkörök riasztást kapnak, amikor a rendszer által generált a K18.018_P[2] szerinti indikátorok jelennek meg
81.	18.21. Az EIR monitorozása – A titkosított kommunikáció láthatósága	K18.021_P[1]	a titkosított kommunikációs forgalom a rendszerfelügyeleti eszközök és mechanizmusok számára látható
82.		K18.021_P[2]	a rendszerfelügyeleti eszközökhöz és a titkosított kommunikációs forgalomhoz való hozzáférést biztosító mechanizmusok meghatározásra kerülnek
83.		K18.021_O.18.21	gondoskodnak arról, hogy a K18.021_P[1] szerinti kommunikációs forgalom látható legyen a K18.021_P[2] szerinti rendszerfelügyeleti eszközök és mechanizmusok számára
84.	18.23. Az EIR monitorozása – Automatikusan generált szervezeti riasztások	K18.023_P[1]	a biztonsági vonatkozású, nem megfelelő vagy szokatlan tevékenységre utaló jelek esetén riasztandó személyek vagy szerepkörök meghatározásra kerültek
85.		K18.023_P[2]	a személyek vagy a szerepkörök riasztására használt automatizált mechanizmusok meghatározásra kerültek
86.		K18.023_P[3]	a riasztást kiváltó vagy meghatározott tevékenységek meghatározásra kerültek
87.		K18.023_O.18.23	a K18.023_P[1] szerinti személyeket vagy szerepköröket a K18.023_P[2] szerinti automatizált mechanizmusok alkalmazásával riasztják, ha a K18.023_P[3] szerinti riasztást kiváltó tevékenységek nem megfelelő vagy szokatlan, biztonsági vonatkozású tevékenységekre utalnak
88.	18.25. Az EIR monitorozása – Vezeték nélküli behatolást érzékelő rendszer	K18.025_O.18.25.(a)	egy vezeték nélküli behatolásérzékelő rendszert alkalmaznak a nem engedélyezett vezeték nélküli eszközök észlelésére
89.		K18.025_O.18.25.(b)	egy vezeték nélküli behatolásérzékelő rendszert alkalmaznak a rendszer elleni támadási kísérletek észlelésére
90.		K18.025_O.18.25.(c)	egy vezeték nélküli behatolásérzékelő rendszert alkalmaznak a rendszer esetleges kompromittálásának vagy sérülésének észlelésére
91.	18.31. Az EIR monitorozása – Privilegizált felhasználók	K18.031_P[1]	a privilegizált felhasználók kiegészítő felügyelete meghatározásra került
92.		K18.031_O.18.31	a K18.031_P[1] szerinti privilegizált felhasználók kiegészítő felügyelete megvalósul
93.	18.33. Az EIR monitorozása – Engedély nélküli hálózati szolgáltatások	K18.033_P[1]	a hálózati szolgáltatásokra vonatkozó engedélyezési vagy jóváhagyási folyamatok meghatározásra kerültek
94.		K18.033_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {naplózás; a K18.033_P[3] szerinti riasztandó személyek vagy szerepkörök}
95.		K18.033_P[3]	az engedélyezési vagy jóváhagyási folyamatok által nem engedélyezett vagy jóváhagyott hálózati szolgáltatások észlelésekor riasztandó személyek vagy szerepkörök meghatározásra kerültek
96.		K18.033_O.18.33.1	a K18.033_P[1] szerinti engedélyezési vagy jóváhagyási folyamatok által nem engedélyezett vagy jóváhagyott hálózati szolgáltatások észlelése biztosított

97.		K18.033_O.18.33.2	a K18.033_P[2] szerinti PARAMÉTER-ÉRTÉKEK alkalmazásra kerülnek, ha olyan hálózati szolgáltatásokat észlelnek, amelyeket az engedélyezési vagy jóváhagyási folyamatok nem engedélyeztek vagy hagytak jóvá
98.	18.37. Biztonsági riasztások és tájékoztatások	K18.037_P[1]	meghatározták azokat a külső szervezeteket, amelyektől a rendszerbiztonsági figyelmeztetéseket, tanácsokat és utasításokat folyamatosan fogadni kell
99.		K18.037_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {a K18.037_P[3] szerinti személyek vagy szerepkörök; a K18.037_P[4] szerinti szervezeti elemek; a K18.037_P[5] szerinti külső szervezetek}
100.		K18.037_P[3]	meghatározottak azok a személyek vagy szerepkörök, akiknek a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat terjeszteni kell
101.		K18.037_P[4]	meghatározásra kerültek a szervezeten belüli azon elemek, amelyek számára a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat terjeszteni kell
102.		K18.037_P[5]	meghatározták azokat a külső szervezeteket, amelyek számára a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat terjeszteni kell
103.		K18.037_O.18.37.1	a K18.037_P[1] szerinti külső szervezetektől folyamatosan rendszerbiztonsági figyelmeztetések, tanácsok és iránymutatások érkeznek
104.		K18.037_O.18.37.2	szükség esetén belső biztonsági riasztásokat, tanácsokat és iránymutatásokat generálnak
105.		K18.037_O.18.37.3	a biztonsági riasztások, tanácsok és iránymutatások a K18.037_P[2] szerinti PARAMÉTER-ÉRTÉKEK szerint kerülnek kiadásra
106.		K18.037_O.18.37.4	a biztonsági iránymutatások végrehajtása meghatározott paraméterek mentén történik
107.	18.38. Biztonsági riasztások és tájékoztatások – Automatizált figyelmeztetések és tanácsok	K18.038_P[1]	a biztonsági riasztási és tanácsadói információk szervezeten belüli továbbítására használt automatizált mechanizmusok meghatározásra kerültek
108.		K18.038_O.18.38	a K18.038_P[1] szerinti automatizált mechanizmusokat használják a biztonsági riasztási és tanácsadói információk szervezeten belüli továbbítására
109.	18.39. Biztonsági funkciók ellenőrzése	K18.039_P[1]	a helyes működés szempontjából ellenőrizendő biztonsági funkciókat meghatározták
110.		K18.039_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {a K18.039_P[3] szerinti átmeneti állapotok; a megfelelő jogosultsággal rendelkező felhasználók utasítására; a K18.039_P[4] szerinti gyakorisággal}
111.		K18.039_P[3]	a biztonsági funkciók ellenőrzését igénylő rendszerátmeneti állapotok meghatározásra kerültek
112.		K18.039_P[4]	a biztonsági funkciók helyes működésének ellenőrzésére szolgáló gyakoriság meghatározásra került (ha alkalmazható)
113.		K18.039_P[5]	meghatározásra kerültek azok a személyek vagy szerepkörök, akiket figyelmeztetni kell a sikertelen biztonsági ellenőrzés esetén

114.		K18.039_P[6]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {a rendszer leállítása; a rendszer újraindítása; a K18.039_P[7] szerinti alternatív intézkedések}
115.		K18.039_P[7]	a rendellenességek észlelésekor végrehajtandó alternatív intézkedések meghatározásra kerültek
116.		K18.039_O.18.39.1	a K18.039_P[1] szerinti biztonsági funkciók helyes működésének ellenőrzése megvalósul
117.		K18.039_O.18.39.2	a K18.039_P[1] szerinti biztonsági funkciók ellenőrzése a K18.039_P[3] által meghatározott PARAMÉTER-ÉRTÉKEK szerint megvalósul
118.		K18.039_O.18.39.3	a K18.039_P[5] szerinti személyeket vagy szerepköröket figyelmeztetik a sikertelen biztonsági ellenőrzés esetén
119.		K18.039_O.18.39.4	a K18.039_P[6] szerinti PARAMÉTER-ÉRTÉKEK alkalmazása rendellenességek észlelésekor kerül végrehajtásra
120.	18.42. Szoftver- és információsértetlenség	K18.042_P[1]	rendelkezésre áll olyan szoftver, amely a jogosulatlan változtatások észleléséhez sértetlenség-ellenőrző eszközöket alkalmaz
121.		K18.042_P[2]	rendelkezésre áll olyan firmware, amely a jogosulatlan változtatások észleléséhez sértetlenség-ellenőrző eszközöket alkalmaz
122.		K18.042_P[3]	meghatározottak azon információk, amelyek jogosulatlan változtatása észleléséhez a szervezet sértetlenség-ellenőrző eszközöket alkalmaz
123.		K18.042_P[4]	a szoftver engedély nélküli megváltoztatásának észlelésekor végrehajtandó intézkedések meghatározásra kerültek
124.		K18.042_P[5]	a firmware engedély nélküli megváltoztatásának észlelésekor végrehajtandó intézkedések meghatározásra kerültek
125.		K18.042_P[6]	az információk engedély nélküli megváltoztatásának észlelésekor végrehajtandó intézkedések meghatározásra kerültek
126.		K18.042_O.18.42.1.(a)	a K18.042_P[1] szerinti szoftver jogosulatlan megváltoztatásának észlelésére sértetlenség-ellenőrző eszközöket alkalmaznak
127.		K18.042_O.18.42.1.(b)	a K18.042_P[2] szerinti firmware jogosulatlan megváltoztatásának észlelésére sértetlenség-ellenőrző eszközöket alkalmaznak
128.		K18.042_O.18.42.1.(c)	a K18.042_P[3] szerinti információk jogosulatlan megváltoztatásának észlelésére sértetlenség-ellenőrző eszközöket alkalmaznak
129.		K18.042_O.18.42.2.(a)	a K18.042_P[4] szerinti intézkedésekre kerül sor, ha a szoftver engedély nélküli megváltoztatását észlelik
130.		K18.042_O.18.42.2.(b)	a K18.042_P[5] szerinti intézkedésekre kerül sor, ha a firmware engedély nélküli megváltoztatását észlelik
131.		K18.042_O.18.42.2.(c)	a K18.042_P[6] szerinti intézkedésekre kerül sor, ha az információk engedély nélküli megváltoztatását észlelik
132.		K18.043_P[1]	meghatározták azt a szoftvert, amelyen sértetlenség-ellenőrzést kell végrehajtani

133.	18.43. Szoftver-, firmware- és információsértetlenség – Sértetlenség ellenőrzése	K18.043_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {indításkor; a K18.043_P[3] szerinti átmeneti állapotoknál vagy a biztonsági szempontból releváns események esetén; a K18.043_P[4] szerinti gyakorisággal}
134.		K18.043_P[3]	meghatározásra kerültek azok az átmeneti állapotok vagy biztonság szempontjából releváns események, amelyek sértetlenség-ellenőrzést igényelnek
135.		K18.043_P[4]	a sértetlenség-ellenőrzés szoftveren történő végrehajtásának gyakorisága meghatározásra került
136.		K18.043_P[5]	meghatározták azt a firmware-t, amelyen sértetlenség-ellenőrzést kell végrehajtani
137.		K18.043_P[6]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {indításkor; a K18.043_P[7] szerinti átmeneti állapotoknál vagy a biztonsági szempontból releváns események esetén; a K18.043_P[8] szerinti gyakorisággal}
138.		K18.043_P[7]	meghatározásra kerültek azok az átmeneti állapotok vagy biztonság szempontjából releváns események, amelyek sértetlenség-ellenőrzést igényelnek a firmware-en (ha alkalmazható)
139.		K18.043_P[8]	a sértetlenség-ellenőrzés firmware-en történő végrehajtásának gyakorisága meghatározásra került
140.		K18.043_P[9]	meghatározták azokat az információkat, amelyeken sértetlenség-ellenőrzést kell végrehajtani
141.		K18.043_P[10]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {indításkor; a K18.043_P[11] szerinti átmeneti állapotoknál vagy a biztonsági szempontból releváns események esetén; a K18.043_P[12] szerinti gyakorisággal}
142.		K18.043_P[11]	meghatározásra kerültek azok az átmeneti állapotok vagy biztonság szempontjából releváns események, amelyek sértetlenség-ellenőrzést igényelnek az információkon (ha alkalmazható)
143.		K18.043_P[12]	a sértetlenség-ellenőrzés információkon történő végrehajtásának gyakorisága meghatározásra került
144.		K18.043_O.18.43.(a)	a K18.043_P[1] szerinti szoftver sértetlenség-ellenőrzése a K18.043_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK szerint történik
145.		K18.043_O.18.43.(b)	a K18.043_P[5] szerinti firmware sértetlenség-ellenőrzése a K18.043_P[6] által meghatározott PARAMÉTER-ÉRTÉKEK szerint történik
146.		K18.043_O.18.43.(c)	a K18.043_P[9] szerinti információk sértetlenség-ellenőrzése a K18.043_P[10] által meghatározott PARAMÉTER-ÉRTÉKEK szerint történik
147.	18.44. Szoftver-, firmware- és információsértetlenség – Automatikus értesítések a sértetlenség megszűnéséről	K18.044_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akiket értesíteni kell, ha a sértetlenség ellenőrzése során eltérést észlelnek
148.		K18.044_O.18.44	olyan automatizált eszközöket alkalmaznak, amelyek értesítik a K18.044_P[1] szerinti személyeket vagy szerepköröket, ha a sértetlenség ellenőrzése során eltéréseket észlelnek

149.	18.46. Szoftver- és információsértetlenség – Automatikus reagálás	K18.046_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {a rendszer leállítása; a rendszer újraindítása; a K18.046_P[2] szerinti intézkedések végrehajtása}
150.		K18.046_P[2]	a sértetlenség megsértésének észlelésekor automatikusan végrehajtandó intézkedések meghatározásra kerültek (ha alkalmazható)
151.		K18.046_O.18.46	a K18.046_P[1] szerinti PARAMÉTER-ÉRTÉKEK automatikusan végrehajtásra kerülnek, ha a sértetlenség megsértését észlelik
152.	18.48. Szoftver- és információsértetlenség – Észlelés és a válaszadás integrálása	K18.048_P[1]	a rendszer biztonsági szempontból jogosulatlan változtatásait meghatározták
153.		K18.048_O.18.48	a K18.048_P[1] szerinti jogosulatlan változtatások észlelése beépül a szervezeti eseménykezelési képességbe
154.	18.53. Szoftver-, firmware- és információsértetlenség – Kódok hitelesítése	K18.053_P[1]	a telepítés előtt kriptográfiai mechanizmusokkal hitelesített szoftver- vagy firmware-elemeket határoztak meg
155.		K18.053_O.18.53	a K18.053_P[1] szerinti szoftver- vagy firmware-elemek telepítés előtti hitelesítésére kriptográfiai mechanizmusokat alkalmaznak
156.	18.56. Kéretlen üzenetek elleni védelem	K18.056_O.18.56.1.(a)	a rendszer belépési pontjain levélszemét elleni védelmi mechanizmusokat alkalmaznak a kéretlen üzenetek észlelésére
157.		K18.056_O.18.56.1.(b)	a rendszer kilépési pontjain levélszemét elleni védelmi mechanizmusokat alkalmaznak a kéretlen üzenetek észlelésére
158.		K18.056_O.18.56.1.(c)	a rendszer belépési pontjain levélszemét elleni védelmi mechanizmusokat alkalmaznak a kéretlen üzenetek kezelésére
159.		K18.056_O.18.56.1.(d)	a rendszer kilépési pontjain levélszemét elleni védelmi mechanizmusokat alkalmaznak a kéretlen üzenetek kezelésére
160.		K18.056_O.18.56.2	a levélszemét elleni védelmi mechanizmusokat a szervezeti konfigurációkezelési szabályoknak megfelelően frissítik, amikor új verziók válnak elérhetővé
161.	18.57. Kéretlen üzenetek elleni védelem – Automatikus frissítések	K18.057_P[1]	a levélszemét elleni védelmi mechanizmusok automatikus frissítésének gyakorisága meghatározott
162.		K18.057_O.18.57	a levélszemét elleni védelmi mechanizmusok automatikusan frissülnek a K18.057_P[1] szerinti gyakorisággal
163.	18.59. Bemeneti információ ellenőrzés	K18.059_P[1]	a rendszerbe bevitt, érvényességi ellenőrzést igénylő információk meghatározásra kerültek
164.		K18.059_O.18.59	a K18.059_P[1] szerinti beviteli információk érvényességét ellenőrzik
165.	18.66. Hibakezelés	K18.066_P[1]	meghatározásra kerültek azok a személyek vagy szerepkörök, amelyek számára a hibaüzeneteket elérhetővé kell tenni
166.		K18.066_O.18.66.1	olyan hibaüzeneteket állítanak elő, amelyek a javító intézkedésekhez szükséges információkat szolgáltatják anélkül, hogy olyan információkat tárnának fel, amelyeket ki lehetne használni

167.		K18.066_O.18.66.2	a hibaüzenetek csak a K18.066_P[1] szerinti személyek vagy szerepkörök számára érhetőek el
168.	18.67. Információ kezelése és megőrzése	K18.067_O.18.67.(a)	a rendszerben lévő információkat a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal, ajánlásokkal és működési követelményekkel összhangban kezelik
169.		K18.067_O.18.67.(b)	a rendszerben lévő információk a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal, ajánlásokkal és működési követelményekkel összhangban kerülnek megőrzésre
170.		K18.067_O.18.67.(c)	a rendszerből kikerülő információkat a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal, ajánlásokkal és működési követelményekkel összhangban kezelik
171.		K18.067_O.18.67.(d)	a rendszerből kikerülő információk a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal, ajánlásokkal és működési követelményekkel összhangban kerülnek megőrzésre
172.	18.78. Memóriavédelem	K18.078_P[1]	a rendszermemória jogosulatlan kódfuttatása elleni védelem érdekében végrehajtandó védelmi intézkedések meghatározásra kerülnek
173.		K18.078_O.18.78	a K18.078_P[1] szerinti védelmi intézkedések a rendszermemória jogosulatlan kódfuttatással szembeni védelmét szolgálják

19. Ellátási lánc kockázatkezelése

	A	B	C
1.	**MKr. 2. melléklete szerinti követelménycsoport**	**Hivatkozási kód**	**Elemi követelmény**
2.	19.1. Szabályzat és eljárásrendek	K19.001_P[1]	meghatározták azokat a személyeket vagy szerepköröket, akikkel az ellátási láncra vonatkozó kockázatmenedzsment szabályzatot meg kell ismertetni
3.		K19.001_P[2]	meghatározták azokat a személyeket vagy szerepköröket, akikkel az ellátási láncra vonatkozó kockázatmenedzsment eljárásokat meg kell ismertetni
4.		K19.001_P[3]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {szervezeti szint; küldetés/üzleti folyamat-szint; rendszerszint}
5.		K19.001_P[4]	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat és eljárások irányítására kijelöltek egy meghatározott személyt
6.		K19.001_P[5]	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat felülvizsgálatának és frissítésének gyakorisága meghatározásra került
7.		K19.001_P[6]	meghatározták azokat az eseményeket, amelyek az ellátási láncra vonatkozó kockázatmenedzsment szabályzat felülvizsgálatát és aktualizálását teszik szükségessé

8.		K19.001_P[7]	meghatározták az ellátási láncra vonatkozó kockázatmenedzsment eljárások felülvizsgálatának és frissítésének gyakoriságát
9.		K19.001_P[8]	meghatározták azokat az eseményeket, amelyek miatt az ellátási láncra vonatkozó kockázatmenedzsment eljárásokat felül kell vizsgálni és aktualizálni kell
10.		K19.001_O_19.1.1.(a)	ellátási láncra vonatkozó kockázatmenedzsment szabályzatot dolgoztak ki és dokumentáltak
11.		K19.001_O_19.1.1.(b)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzatot megismertették a K19.001_P[1] szerinti személyekkel vagy szerepkörökkel
12.		K19.001_O_19.1.1.(c)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat és a kapcsolódó hozzáférés-ellenőrzések végrehajtását elősegítő ellátási láncra vonatkozó kockázatmenedzsment eljárások kidolgozása és dokumentálása megtörtént
13.		K19.001_O_19.1.1.(d)	az ellátási láncra vonatkozó kockázatmenedzsment eljárások ismertetésre kerültek a K19.001_P[2] szerinti személyekkel vagy szerepkörökkel
14.		K19.001_O_19.1.2	a K19.001_P[4] szerinti személyt kijelölték az ellátási láncra vonatkozó kockázatmenedzsment szabályzat és eljárások kidolgozásának, dokumentálásának és ismertetésének irányítására
15.		K19.001_O_19.1.3.(a)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzatot felülvizsgálják és frissítik a K19.001_P[5] szerinti gyakorisággal
16.		K19.001_O_19.1.3.(b)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzatot felülvizsgálják és frissítik a K19.001_P[6] szerinti eseményeket követően
17.		K19.001_O_19.1.3.(c)	az ellátási láncra vonatkozó kockázatmenedzsment eljárásokat felülvizsgálják és frissítik a K19.001_P[7] szerinti gyakorisággal
18.		K19.001_O_19.1.3.(d)	az ellátási láncra vonatkozó kockázatmenedzsment eljárásokat felülvizsgálják és frissítik a K19.001_P[8] szerinti eseményeket követően
19.		K19.001_O_19.1.1.1.1.(a)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat célja meghatározásra került a K19.001_P[3] szerint
20.		K19.001_O_19.1.1.1.1.(b)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat hatálya meghatározásra került a K19.001_P[3] szerint
21.		K19.001_O_19.1.1.1.1.(c)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzathoz kapcsolódó szerepkörök meghatározásra kerültek a K19.001_P[3] szerint
22.		K19.001_O_19.1.1.1.1.(d)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzathoz kapcsolódó felelősségek meghatározásra kerültek a K19.001_P[3] szerint
23.		K19.001_O_19.1.1.1.1.(e)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzathoz kapcsolódó vezetői elkötelezettség rögzítésre került a K19.001_P[3] szerint

24.		K19.001_O_19.1.1.1.1.(f)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzathoz kapcsolódó szervezeti egységek közötti együttműködés meghatározásra került a K19.001_P[3] szerint
25.		K19.001_O_19.1.1.1.1.(g)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzathoz kapcsolódó megfelelőségi kritériumok meghatározásra kerültek a K19.001_P[3] szerint
26.		K19.001_O_19.1.1.1.2.	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat összhangban van a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, politikákkal, szabványokkal és iránymutatásokkal
27.	19.2. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat	K19.002_P[1]	meghatározásra kerültek olyan rendszerek, rendszerelemek vagy rendszerszolgáltatások, amelyekre ellátási láncra vonatkozó kockázatmenedzsment szabályzatot dolgoznak ki
28.		K19.002_P[2]	meghatározták az ellátási láncra vonatkozó kockázatmenedzsment szabályzat felülvizsgálatának és frissítésének gyakoriságát
29.		K19.002_O.19.2.1.(a)	szabályzatot dolgoztak ki az ellátási lánc kockázatainak kezelésére
30.		K19.002_O.19.2.1.(b)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások kutatásával és fejlesztésével kapcsolatos kockázatokkal foglalkozik
31.		K19.002_O.19.2.1.(c)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások tervezésével kapcsolatos kockázatokkal foglalkozik
32.		K19.002_O.19.2.1.(d)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások gyártásával kapcsolatos kockázatokkal foglalkozik
33.		K19.002_O.19.2.1.(e)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások beszerzésével kapcsolatos kockázatokkal foglalkozik
34.		K19.002_O.19.2.1.(f)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások szállításával kapcsolatos kockázatokkal foglalkozik
35.		K19.002_O.19.2.1.(g)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások integrációjával kapcsolatos kockázatokkal foglalkozik
36.		K19.002_O.19.2.1.(h)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások üzemeltetésével kapcsolatos kockázatokkal foglalkozik
37.		K19.002_O.19.2.1.(i)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat a K19.002_P[1] szerinti rendszerek, rendszerelemek vagy rendszerszolgáltatások selejtezésével kapcsolatos kockázatokkal foglalkozik
38.		K19.002_O.19.2.2	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat felülvizsgálata és frissítése a K19.002_P[2] szerinti gyakorisággal vagy szükség szerint történik
39.		K19.002_O.19.2.3.(a)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat védett a jogosulatlan közzététellel szemben
40.		K19.002_O.19.2.3.(b)	az ellátási láncra vonatkozó kockázatmenedzsment szabályzat védett a jogosulatlan módosítással szemben

41.	19.4. Ellátási láncra vonatkozó követelmények és folyamatok	K19.004_P[1]	meghatározták azt a rendszert vagy rendszerelemet, amely a gyengeségek vagy hiányosságok azonosításához és kezeléséhez folyamatot vagy folyamatokat igényel
42.		K19.004_P[2]	meghatározottak az ellátási láncban részt vevő azon személyek, akikkel együttműködve kell az ellátási lánc elemeiben és folyamataiban lévő gyengeségeket vagy hiányosságokat azonosítani és kezelni
43.		K19.004_P[3]	a rendszert, rendszerelemet vagy rendszerszolgáltatást érintő ellátási lánc kockázatok elleni védelemre, valamint az ellátási lánccal kapcsolatos eseményekből eredő károk vagy következmények csökkentésére alkalmazott kontrollok meghatározásra kerültek
44.		K19.004_P[4]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került:{biztonsági szabályzatban; ellátási lánc kockázatmenedzsment szabályzatban; egyéb, a szervezet által meghatározott dokumentumban}
45.		K19.004_O.19.4.1.(a)	folyamatot vagy folyamatokat hoznak létre a K19.004_P[1] szerinti rendszer vagy rendszerelem ellátási láncában lévő elemei és folyamatai gyengeségeinek vagy hiányosságainak azonosítására és kezelésére
46.		K19.004_O.19.4.1.(b)	a K19.004_P[1] szerinti rendszer vagy rendszerelem ellátási láncában lévő elemei és folyamatai gyengeségeinek vagy hiányosságainak azonosítására és kezelésére szolgáló folyamat vagy folyamatok a K19.004_P[2] szerinti személyekkel együttműködve kerülnek végrehajtásra
47.		K19.004_O.19.4.2	a K19.004_P[3] szerinti kontrollokat a rendszert, rendszerelemet vagy rendszerszolgáltatást érintő ellátási láncbeli kockázatok elleni védelemre, valamint az ellátási lánccal kapcsolatos eseményekből eredő károk vagy következmények csökkentésére alkalmazzák
48.		K19.004_O.19.4.3	a bevezetett és végrehajtott ellátási lánc folyamatokat és kontrollokat a K19.004_P[4] szerinti PARAMÉTER-ÉRTÉKEK szerint dokumentálták
49.	19.7. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók	K19.007_O.19.7	a fővállalkozói szerződésekben szereplő követelmények az alvállalkozói szerződésekben is szerepelnek
50.	19.13. Beszerzési stratégiák, eszközök és módszerek	K19.013_P[1]	meghatározásra kerültek beszerzési stratégiák, szerződéses eszközök és beszerzési módszerek az ellátási lánc kockázatai kezelésére a kockázatok azonosítása és csökkentése érdekében
51.		K19.013_O.19.13.(a)	a K19.013_P[1] szerinti stratégiák, eszközök és módszerek alkalmazása megvalósul az ellátási lánc kockázatai elleni védelem érdekében
52.		K19.013_O.19.13.(b)	a K19.013_P[1] szerinti stratégiák, eszközök és módszerek alkalmazása megvalósul az ellátási lánc kockázatainak azonosítása érdekében
53.		K19.013_O.19.13.(c)	a K19.013_P[1] szerinti stratégiák, eszközök és módszerek alkalmazása megvalósul az ellátási lánc kockázatainak csökkentése érdekében
54.	19.16. Beszállítók értékelése és felülvizsgálata	K19.016_P[1]	meghatározták, hogy milyen gyakorisággal kell értékelni és felülvizsgálni a beszállítókkal vagy szerződéses partnerekkel és az általuk nyújtott rendszerekkel, rendszerelemekkel vagy rendszerszolgáltatásokkal kapcsolatos, az ellátási láncból eredő kockázatokat

55.		K19.016_O.19.16	a beszállítókkal vagy szerződéses partnerekkel és az általuk biztosított rendszerekkel, rendszerelemekkel vagy rendszerszolgáltatásokkal kapcsolatos, ellátási láncból eredő kockázatokat értékelik és felülvizsgálják a K19.016_P[1] szerinti gyakorisággal
56.	19.19. Értesítési megállapodások	K19.019_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {a K19.019_P[2] szerinti értékelések vagy auditok eredményei}
57.		K19.019_P[2]	meghatározzák azokat az információkat, amelyekre vonatkozóan megállapodásokat kell kötni és eljárásokat kell létrehozni (ha alkalmazható)
58.		K19.019_O.19.19	a K19.019_P[1] szerinti PARAMÉTER-ÉRTÉKEK tekintetében a rendszer, a rendszerelemek vagy a rendszerszolgáltatás ellátási láncában részt vevő szervezetekkel megállapodásokat kötnek és eljárásokat hoznak létre
59.	19.20. Hamisítás elleni védelem	K19.020_O.19.20	a rendszer, a rendszerelem vagy a rendszerszolgáltatás hamisítás elleni védelmi programmal van ellátva
60.	19.21. Hamisítás elleni védelem - Rendszerfejlesztési életciklus	K19.021_O.19.21	a hamisítás elleni technológiákat, eszközöket és technikákat a rendszerfejlesztés teljes életciklusa során alkalmazzák
61.	19.22. Rendszerek vagy rendszerelemek vizsgálata	K19.022_P[1]	az ellenőrzést igénylő rendszerek vagy rendszerelemek meghatározásra kerültek
62.		K19.022_P[2]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {eseti jelleggel; a K19.022_P[3] szerinti gyakorisággal; a K19.022_P[4] szerinti esetekben}
63.		K19.022_P[3]	a rendszerek vagy rendszerelemek ellenőrzésének gyakorisága meghatározott
64.		K19.022_P[4]	a rendszerek vagy rendszerelemek ellenőrzésének szükségességére vonatkozó esetek meghatározásra kerülnek
65.		K19.022_O.19.22	a K19.022_P[1] szerinti rendszerek vagy rendszerelemek ellenőrzésre kerülnek a K19.022_P[2] által meghatározott PARAMÉTER-ÉRTÉKEK szerint az esetleges hamisítás felderítése érdekében
66.	19.23. Rendszerelem hitelessége	K19.023_P[1]	a következő PARAMÉTER-ÉRTÉKEK közül egy vagy több kiválasztásra került: {a K19.023_P[2] szerinti külső jelentéstevő szervezetek; a K19.023_P[3] szerinti személyek vagy szerepkörök}
67.		K19.023_P[2]	meghatározták azokat a külső szervezeteket, amelyeknek a hamisított rendszerelemeket jelenteni kell
68.		K19.023_P[3]	meghatározott az a személy vagy szerepkör, akinek a hamisított rendszerelemeket jelenteni kell
69.		K19.023_O.19.23.1.(a)	a hamisítás elleni szabályok kidolgozásra és bevezetésre kerültek
70.		K19.023_O.19.23.1.(b)	a hamisítás elleni eljárások kidolgozásra és bevezetésre kerültek
71.		K19.023_O.19.23.1.(c)	a hamisítás elleni eljárások alkalmazzák a rendszerbe kerülő hamisított rendszerelemek észlelésére szolgáló eszközöket
72.		K19.023_O.19.23.1.(d)	a hamisítás elleni eljárások alkalmazzák azokat az eszközöket, amelyek megakadályozzák, hogy hamisított rendszerelemek kerüljenek a rendszerbe

73.		K19.023_O.19.23.2	a hamisított rendszerelemeket a K19.023_P[1] szerinti PARAMÉTER-ÉRTÉKEK számára kell jelenteni
74.	19.24. Rendszerelem hitelessége – Hamisítás elleni képzés	K19.024_P[1]	a hamisított rendszerelemek – beleértve a hardvert, a szoftvert és a firmware-t – felismerésére képzést igénylő személyek vagy szerepkörök meghatározása megtörtént
75.		K19.024_O.19.24	a K19.024_P[1] szerinti személyek vagy szerepkörök számára képzés került megtartásra a hamisított rendszerelemek – beleértve a hardvert, a szoftvert és a firmware-t – felismerésére
76.	19.25. Rendszerelem hitelessége – Konfigurációfelügyelet	K19.025_P[1]	a konfiguráció felügyeletet igénylő rendszerelemek meghatározásra kerültek
77.		K19.025_O.19.25.(a)	a szervizelésre vagy javításra váró, a K19.025_P[1] szerinti rendszerelemek konfigurációs felügyelete fennmarad
78.		K19.025_O.19.25.(b)	a szervizelt vagy javított K19.025_P[1] szerinti rendszerelemek konfigurációs felügyelete fennmarad az újbóli üzembe helyezésre várva
79.	19.27. Rendszerelem selejtezése, megsemmisítése	K19.027_P[1]	a megsemmisítendő adatok, dokumentációk, eszközök vagy rendszerelemek meghatározásra kerültek
80.		K19.027_P[2]	az adatok, dokumentációk, eszközök vagy rendszerelemek megsemmisítésére szolgáló technikák és módszerek meghatározásra kerültek
81.		K19.027_O.19.27	a K19.027_P[1] szerinti adatok, dokumentációk, eszközök vagy rendszerelemek a K19.027_P[2] szerinti technikák és módszerek alkalmazásával kerülnek selejtezésre, megsemmisítésre

8. melléklet az 1/2025. (I. 31.) SZTFH rendelethez

Az auditjelentés tartalma

1. Az auditjelentés a következőket tartalmazza:

1.1. vezetői összefoglaló, a kiberbiztonsági audit összefoglaló megállapításai,

1.2. auditor megnevezése, székhelyének címe és a Hatóság általi nyilvántartásba vételekor kapott azonosító száma,

1.3. a szervezet megnevezése, székhelyének címe és adószáma,

1.4. a megállapodást megkötő szervezet megnevezése és székhelyének címe, ha az eltér az 1.3. pontban foglaltaktól,

1.5. a megállapodás megkötésének dátuma,

1.6. az auditjelentés kiállításának dátuma,

1.7. a vizsgált EIR azonosító adatai,

1.8. a vizsgált EIR biztonsági osztályba sorolása, és az osztályba sorolás megfelelősége vizsgálatnak főbb megállapításai,

1.9. az alkalmazott, a Kiberbiztonsági tv. 22. § (1) bekezdése szerinti vizsgálati tevékenységekre vonatkozó adatok,

1.10. a 3. § (4) bekezdése szerinti dokumentumok azonosítása (verziószáma, elektronikus dokumentumok fájlneve, hash lenyomata),

1.11. az audit megállapításai:

1.11.1. a 7. melléklet szerinti, az elemi követelményekre vonatkozó „megfelelt", „nem megfelelt" vagy „nem alkalmazható" auditori döntések (AD) minden követelménycsoport esetén,

1.11.2. vizsgált követelménycsoportok értékelése:

1.11.2.1. az elvárás,

1.11.2.2. az alkalmazott vizsgálati módszer,

1.11.2.3. az 5. melléklet 2.2.4.1–2.2.4.1.2.2.5. pontja alapján a követelménycsoport szöveges értékelése, eltérések indokolása,

1.11.2.4. a döntést alátámasztó bizonyíték-hivatkozások,

1.12. összefoglaló megállapítások:

1.12.1. az EIR-re vonatkozó összesített statisztikai adatok megadása a kontrollcsoportok értékelése összesített eredményének, valamint annak ismertetésével, hogy összesen hány kontrollcsoportra lett az értékelés eredménye

1.12.1.1. megfelelt,

1.12.1.2. nem megfelelt, ezen belül az eltérés mértéke:

1.12.1.2.1. elhanyagolható mértékű eltérés,

1.12.1.2.2. kis mértékű eltérés,

1.12.1.2.3. kiemelt mértékű eltérés vagy

1.12.1.2.4 kritikus mértékű eltérés,

1.12.2. minden EIR-re a VMI és szöveges értékelése az 5. melléklet 2.2.5.6. pontja alapján,

1.12.3. a szervezet ellenálló-képességi indexe és annak szöveges értékelése az 5. melléklet 2.3.2. pontja alapján,

1.13. a felhasznált értékelési bizonyítékok rendezett felsorolása.

A Szabályozott Tevékenységek Felügyeleti Hatósága elnökének 2/2025. (I. 31.) SZTFH rendelete a kiberbiztonsági felügyeleti díjról

[1] A Szabályozott Tevékenységek Felügyeleti Hatósága elnöke rendeletének célja a kiberbiztonsági felügyeleti tevékenységért fizetendő kiberbiztonsági felügyeleti díj mértékének és a megfizetésére vonatkozó rendelkezések megállapítása.

[2] A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 81. § (6) bekezdés a) pontjában kapott felhatalmazás alapján,

a 2. § (10) bekezdése és a 4. § tekintetében a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 29. § b) pontjában kapott felhatalmazás alapján,

a 7–10. § tekintetében a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 81. § (6) bekezdés e) pontjában kapott felhatalmazás alapján,

a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § n) és q) pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

1. A kiberbiztonsági felügyeleti díj mértéke

1. § (1) A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 7. § (1) bekezdése szerinti kiberbiztonsági felügyeleti díj (a továbbiakban: kiberbiztonsági felügyeleti díj) éves mértéke

a) a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja szerinti azon szervezet, amely egyúttal a Kiberbiztonsági tv. 2. és 3. melléklete szerinti szervezet is, valamint a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet (a továbbiakban együtt: szervezet) tárgyévet megelőző évben közzétett utolsó, a számvitelről szóló 2000. évi C. törvény (a továbbiakban: Szt.) szerinti beszámolója szerinti nettó árbevételének 0,00015 százaléka, ha a szervezet tárgyévet megelőző éves nettó árbevétele nem éri el a 20 milliárd forintot,

b) a szervezet tárgyévet megelőző évben közzétett utolsó, Szt. szerinti beszámolója szerinti nettó árbevételének 0,0015 százaléka, de legfeljebb 10 millió forint, ha a szervezet tárgyévet megelőző éves nettó árbevétele eléri vagy meghaladja a 20 milliárd forintot.

(2) Az (1) bekezdéstől eltérően, az (1) bekezdés szerinti árbevétel hiányában a kiberbiztonsági felügyeleti díj éves mértéke

a) a szervezet tárgyévi árbevétele egész évre vetített időarányos részének 0,00015 százaléka, ha a szervezet tárgyévi árbevétele egész évre vetített időarányos része nem éri el a 20 milliárd forintot,

b) a szervezet tárgyévi árbevétele egész évre vetített időarányos részének 0,0015 százaléka, de legfeljebb 10 millió forint, ha a szervezet tárgyévi árbevétele egész évre vetített időarányos része eléri vagy meghaladja a 20 milliárd forintot.

(3) A kiberbiztonsági felügyeleti díj számítása, megfizetése, nyilvántartása és elszámolása 1000 forintra kerekítve történik. A kiberbiztonsági felügyeleti díj 1000 forintra kerekített összegét az általános kerekítési szabályok alkalmazásával kell meghatározni.

(4) Ha a szervezet a tárgyévben kerül a Kiberbiztonsági tv. hatálya alá, a hatály alá kerülés Kiberbiztonsági tv. 8. § (6) bekezdése szerinti időpontjától kezdődően a szervezet tárgyévet megelőző évben közzétett utolsó, Szt. szerinti beszámolója szerinti nettó árbevétele – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos része – alapján időarányos mértékű kiberbiztonsági felügyeleti díj fizetésére köteles.

(5) Ha a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: Hatóság) a tárgyévben törli a szervezetet a Kiberbiztonsági tv. 29. § (1) bekezdés a) pontja szerinti nyilvántartásból (a továbbiakban: nyilvántartás), és a szervezet tárgyévre vonatkozó kiberbiztonsági felügyeleti díj fizetési kötelezettségét még nem teljesítette, akkor a szervezet a nyilvántartásból való törlésének napjáig terjedő időszakra vonatkozóan, a tárgyévet megelőző évben közzétett utolsó, Szt. szerinti beszámolója szerinti nettó árbevétele – árbevétel hiányában a tárgyévi árbevételének egész évre vetített időarányos része – alapján időarányos mértékű kiberbiztonsági felügyeleti díj fizetésére köteles.

(6) Ha a tárgyévben fizetendő kiberbiztonsági felügyeleti díj összege nem éri el az 5000 forintot, a kiberbiztonsági felügyeleti díjat nem kell megfizetni. Ebben az esetben a Hatóság a 2. § (3), (6), (7) vagy (9) bekezdése szerinti tájékoztatása tartalmazza, hogy a szervezet kiberbiztonsági felügyeleti díj fizetési kötelezettsége a tárgyévre nem áll fenn.

2. A kiberbiztonsági felügyeleti díj megfizetésének általános szabályai

2. § (1) Ha a szervezet a Polgári Törvénykönyvről szóló törvény szerinti elismert vállalatcsoportban, tényleges vállalatcsoportban vagy az Szt. szerinti anyavállalatot, leányvállalatokat és a konszolidálásba bevont közös vezetésű vállalkozásokat tartalmazó, egy konszolidációs körbe tartozó vállalkozáscsoportban vesz részt, a szervezet a részvételét a Hatóság által e célra rendszeresített elektronikus űrlapon benyújtott – elismert vállalatcsoport esetében az uralkodó taggal közösen megtett – nyilatkozatával igazolja a Hatóság részére a tárgyév január 31. napjáig.

(2) Az 1. § (2) bekezdése szerinti esetben a szervezet a Hatóság által e célra rendszeresített elektronikus űrlapon nyilatkozatot nyújt be a Hatósághoz a tárgyévi árbevétele egész évre vetített időarányos részének összegéről a tárgyév február 28. napjáig.

(3) A Hatóság a (6)–(10) bekezdésben foglalt kivétellel a szervezetet – vagy elismert vállalatcsoportba tartozó szervezet esetében az uralkodó tagot – a tárgyévre fizetendő kiberbiztonsági felügyeleti díj mértékéről és – az 1. § (6) bekezdésében foglalt kivétellel – a megfizetésének módjáról a tárgyévet megelőző évben közzétett utolsó, Szt. szerinti beszámolója alapján a tárgyév március 31. napjáig tájékoztatja.

(4) Ha a Polgári Törvénykönyvről szóló törvény szerinti tényleges vállalatcsoportban vagy az Szt. szerinti anyavállalatot, leányvállalatokat és a konszolidálásba bevont közös vezetésű vállalkozásokat tartalmazó, egy konszolidációs körbe tartozó vállalkozáscsoportban részt vevő szervezetek által – a (3) bekezdés szerinti tájékoztatás alapján – a tárgyévben fizetendő éves kiberbiztonsági felügyeleti díj együttes mértéke meghaladja a Kiberbiztonsági tv. 7. § (2) bekezdése szerinti 50 millió forintot, akkor a szervezetek tárgyév április 30-ig közös nyilatkozatot nyújtanak be a Hatóság részére, amely tartalmazza az egyes szervezetek által megfizetésre kerülő kiberbiztonsági felügyeleti díj összegét, azzal, hogy a megfizetésre kerülő kiberbiztonsági felügyeleti díj együttes mértéke összesen 50 millió forint.

(5) A kiberbiztonsági felügyeleti díjat a (3) és (4) bekezdés szerinti esetben a tárgyév május 31. napjáig kell megfizetni.

(6) Az 1. § (4) bekezdése szerinti szervezetet a Hatóság – a (7) bekezdésben foglalt kivétellel – a nyilvántartásba vételi határozatában tájékoztatja a tárgyévben fizetendő kiberbiztonsági felügyeleti díj mértékéről és – az 1. § (6) bekezdésében foglalt kivétellel – a megfizetésének módjáról.

(7) Ha az 1. § (4) bekezdése szerinti szervezet nem rendelkezik az 1. § (1) bekezdése szerinti árbevétellel, a szervezet a nyilvántartásba vételétől számított 90 napon belül a Hatóság által e célra rendszeresített elektronikus űrlapon nyilatkozatot nyújt be a Hatósághoz a tárgyévi árbevétel egész évre vetített időarányos részének összegéről. A Hatóság a nyilatkozat kézhezvételétől számított 30 napon belül tájékoztatja a szervezetet az általa a tárgyévre fizetendő kiberbiztonsági felügyeleti díj mértékéről és – az 1. § (6) bekezdésében foglalt kivétellel – a megfizetésének módjáról.

(8) Az 1. § (4) bekezdése szerinti szervezet a nyilvántartásba vételi határozat kézhezvételétől – vagy a (7) bekezdés szerinti esetben a Hatóság tájékoztatásától – számított 90 napon belül fizeti meg a kiberbiztonsági felügyeleti díjat.

(9) Az 1. § (5) bekezdése szerinti esetben a Hatóság a nyilvántartásból való törlésről szóló határozatában tájékoztatja a szervezetet a tárgyévben fizetendő időarányos kiberbiztonsági felügyeleti díj mértékéről és – az 1. § (6) bekezdésében foglalt kivétellel – a megfizetésének módjáról.

(10) A (9) bekezdés szerinti esetben a kiberbiztonsági felügyeleti díjat a nyilvántartásból való törlésről szóló határozat kézhezvételétől számított 30 napon belül kell megfizetni.

(11) Ha a Hatóság a tárgyévben törli a szervezetet a nyilvántartásból, és a szervezet tárgyévre vonatkozó kiberbiztonsági felügyeleti díj fizetési kötelezettségét már teljesítette, akkor a Hatóság a nyilvántartásból való törlésről szóló határozatában tájékoztatja a szervezetet a tárgyévben a törlés napjáig időarányosan fizetendő kiberbiztonsági felügyeleti díj és a szervezet által a tárgyévre megfizetett kiberbiztonsági felügyeleti díj különbözetéről. A különbözet visszatérítésére a 4. § (2) bekezdése alkalmazandó.

3. § (1) A szervezet kiberbiztonsági felügyeleti díj fizetési kötelezettségét évente, egy összegben, a Hatóság Magyar Államkincstár által vezetett, 10032000-00362887-00000000 számú előirányzat-felhasználási keretszámlájára átutalással teljesíti.

(2) A kiberbiztonsági felügyeleti díj megfizetésekor a pénzforgalmi szolgáltató által kiállított, az átutalás megindításának megtörténtét tanúsító igazolás közlemény rovatában fel kell tüntetni a „kiberbiztonsági felügyeleti díj” megjegyzést és

a) a 2. § (3) bekezdése szerinti esetben a Hatóság 2. § (3) bekezdése szerinti tájékoztatásának iktatószámát,

b) az 1. § (4) bekezdése szerinti szervezet esetén a nyilvántartásba vételi határozat iktatószámát,

c) az 1. § (5) bekezdése szerinti esetben a nyilvántartásból való törlésről szóló határozat iktatószámát vagy

d) a b) ponttól eltérően, ha az 1. § (4) bekezdése szerinti szervezet nem rendelkezik az 1. § (1) bekezdése szerinti árbevétellel, a Hatóság 2. § (7) bekezdése szerinti tájékoztatásának iktatószámát.

3. Hatósági feladatok

4. § (1) A Hatóság a kiberbiztonsági felügyeleti díjat szervezetenként – ha a szervezet a Polgári Törvénykönyvről szóló törvény szerinti elismert vállalatcsoport ellenőrzött tagja, helyette az uralkodó taghoz rendelten – és elszámolási időszakonként tartja nyilván.

(2) Túlfizetés esetén a Hatóság a kiberbiztonsági felügyeleti díj többletet visszatéríti a szervezet azon bankszámlájára, amelyről a befizetés érkezett, ha a befizetést igazoló iratok alapján megállapítható, hogy a kötelezett az e rendeletben meghatározott mértéket meghaladó összegű díjat fizetett.

4. Záró rendelkezések

5. § (1) Ez a rendelet – a (2) bekezdésben foglalt kivétellel – a kihirdetését követő 3. napon lép hatályba.

(2) Az 1–3. alcím és a 6. § az e rendelet kihirdetését követő 31. napon lép hatályba.

6. § (1) A 2024. évre és a 2025. évre vonatkozó kiberbiztonsági felügyeleti díj mértékére, megfizetésére és kezelésére az 1–3. alcímben foglaltakat az e szakaszban foglalt eltérésekkel, kiegészítésekkel kell alkalmazni.

(2) Az 1. § (1) és (4) bekezdése szerinti esetben a 2024. évre vonatkozó kiberbiztonsági felügyeleti díjat a Hatóság a szervezet 2024. évet megelőző utolsó, Szt. alapján közzétett beszámolóval lezárt üzleti évről szóló beszámolója alapján állapítja meg. A 2024. évre vonatkozó kiberbiztonsági felügyeleti díjat a 2024. október 18-tól 2024. december 31-ig terjedő felügyeleti időszakra kell megfizetni.

(3) Ha az e rendelet hatálybalépésekor a nyilvántartásban szereplő szervezet nem rendelkezik a (2) bekezdés szerinti beszámolóval, a 2024. évre vonatkozóan kiberbiztonsági felügyeleti díj fizetési kötelezettsége nem áll fenn.

(4) A 2024. évre és a 2025. évre vonatkozóan

a) a 2. § (1) bekezdése szerinti nyilatkozatot 2025. március 15. napjáig,

b) a 2. § (4) bekezdése szerinti nyilatkozatot 2025. június 30. napjáig

kell benyújtani.

(5) A 2025. évre vonatkozóan a 2. § (2) bekezdése szerinti nyilatkozatot 2025. március 31. napjáig kell benyújtani.

(6) A 2024. évre és a 2025. évre vonatkozó kiberbiztonsági felügyeleti díj mértékéről és – az 1. § (6) bekezdésében foglalt kivétellel – megfizetésének módjáról a Hatóság a szervezetet – vagy elismert vállalatcsoportba tartozó szervezet esetében az uralkodó tagot – 2025. május 31-ig tájékoztatja.

(7) A (6) bekezdés szerinti kiberbiztonsági felügyeleti díjat 2025. július 31-ig kell megfizetni.

7. § Az érintett szervezetek kiberbiztonsági felügyeleti hatósági nyilvántartásáról szóló 23/2023. (XII. 19.) SZTFH rendelet (a továbbiakban: R.) 1. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A Szabályozott Tevékenységek Felügyeleti Hatósága mint a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági tv.) 23. § (1) bekezdés b) pontja szerinti kiberbiztonsági hatóság (a továbbiakban: felügyeleti hatóság) kiberbiztonsági felügyeleti tevékenysége keretében végzi a Kiberbiztonsági tv. 1. § (1) bekezdés b), d) és e) pontja szerinti szervezet (a továbbiakban együtt: szervezet) vonatkozásában a Kiberbiztonsági tv. 29. § (1) bekezdés a) pontja szerinti nyilvántartás (a továbbiakban: nyilvántartás) vezetését."

8. § (1) Az R. 2. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A szervezetnek a nyilvántartásba történő felvételére irányuló eljárás kérelemre indul, amelyet a szervezet nyújt be a felügyeleti hatósághoz."

(2) Az R. 2. § (2) bekezdés a) pontja helyébe a következő rendelkezés lép:

[Az (1) bekezdés szerinti kérelem tartalmazza]

„a) a szervezet

aa) megnevezését,

ab) adószámát,

ac) cégjegyzékszámát,

ad) székhelyének címét,

ae) alapításának dátumát,

af) a Kiberbiztonsági tv. 2. és 3. melléklete szerinti tevékenységeit,

ag) a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerinti besorolását és előző üzleti évi nettó árbevételét,

ah) elektronikus levelezési címét, amely a felügyeleti hatóság által tájékoztatási célra felhasználható a szervezet kérelemben rögzített hozzájárulása alapján,

ai) Kiberbiztonsági tv. hatálya alá kerülésének Kiberbiztonsági tv. 8. § (6) bekezdése szerinti időpontját,"

(3) Az R. 2. § (2) bekezdése a következő e) ponttal egészül ki:

[Az (1) bekezdés szerinti kérelem tartalmazza]

„e) azon európai uniós tagállamok listáját, amelyekben a szervezet szolgáltatásokat nyújt."

(4) Az R. 2. § (3) bekezdése helyébe a következő rendelkezés lép:

„(3) A felügyeleti hatóság nyilvántartja a (2) bekezdés a) pont ad)–ai) alpontja és (2) bekezdés d) pontja szerinti adatokat, valamint az érintett szervezet nyilvántartásba vételekor kapott azonosító számát."

9. § Az R.

a) 2. § (2) bekezdés b) és d) pontjában az „az érintett szervezet" szövegrész helyébe az „a szervezet" szöveg,

b) 2. § (2) bekezdés c) pontjában a „levelezési címét" szövegrész helyébe a „levelezési címét, valamint – ha az elektronikus információs rendszerek biztonságáért felelős személy nem a szervezet munkavállalója – az elektronikus információs rendszerek biztonságáért felelős személyt foglalkoztató jogi személy megnevezését, adószámát és cégjegyzékszámát," szöveg,

c) 2. § (2) bekezdés d) pont dc) alpontjában a „domainnevet" szövegrész helyébe a „doménnevet" szöveg,

d) 3. § (1) és (2) bekezdésében az „Az érintett szervezet" szövegrész helyébe az „A szervezet" szöveg,

e) 3. § (3) bekezdésében az „az érintett szervezet" szövegrészek helyébe az „a szervezet" szöveg,

f) 4. §-ában az „érintett szervezet" szövegrész helyébe a „szervezet" szöveg

lép.

10. § Hatályát veszti az R. 2. § (2) bekezdés d) pont db) alpontjában a „valamint az ahhoz kapcsolódó szolgáltatás megnevezését," szövegrész.

Dr. Nagy László s. k.,
elnök

V. A Kormány tagjainak rendeletei

Az építési és közlekedési miniszter 2/2025. (I. 31.) ÉKM rendelete a közlekedésért felelős miniszter szabályozási feladatkörébe tartozó forgalmazási követelmények tekintetében eljáró megfelelőségértékelő szervezetek kijelölési eljárásáért fizetendő igazgatási szolgáltatási díjakról

[1] A megfelelőségértékelő szervezetek tevékenységről szóló törvény alapján a kijelölési eljárásért fizetendő díjat rendeletben kell megállapítani, amely törvényi felhatalmazás alapján a rendelet célja a közlekedésért felelős miniszter szabályozási feladatkörébe tartozó forgalmazási követelmények tekintetében eljáró megfelelőségértékelő szervezetek kijelölési eljárásért fizetendő igazgatási szolgáltatási díjak mértékének, megfizetésével összefüggő szabályainak meghatározása.

[2] A megfelelőségértékelő szervezetek tevékenységéről szóló 2009. évi CXXXIII. törvény 13. § (2) bekezdés b) pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 95. § 8. pontjában meghatározott feladatkörömben eljárva – a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 103. § (1) bekezdés 21. pontjában meghatározott feladatkörében eljáró nemzetgazdasági miniszterrel egyetértésben – a következőket rendelem el:

1. § (1) A közlekedésért felelős miniszter szabályozási feladatkörébe tartozó forgalmazási követelmények tekintetében eljáró megfelelőségértékelő szervezetek kijelöléséről szóló 60/2011. (XI. 25.) NFM rendeletben (a továbbiakban: kijelölési rendelet) meghatározott kijelölési eljárásért az e rendeletben meghatározott igazgatási szolgáltatási díjat (a továbbiakban: díj) kell fizetni.

(2) A díjat a kijelölés iránti kérelem benyújtásával egyidejűleg kell az Építési és Közlekedési Minisztérium Magyar Államkincstárnál vezetett, 10032000-00003582-06020015 számú számlájára befizetni.

(3) A befizetett díj az eljáró hatóság bevétele. A befizetett díjat a megfelelőségértékelő szervezetek kijelölésével kapcsolatban felmerülő személyi és tárgyi költségekre kell felhasználni.

(4) A díj mértéke, ha a kérelmezett megfelelőségértékelési terület nem tartozik harmonizációs uniós jogi aktus hatálya alá – a kijelölési rendelet 2. mellékletében meghatározott – megfelelőségértékelési területet szabályozó jogszabályonként

a) 142 760 forint, valamint annyiszor 19 370 forint, ahány megfelelőségértékelési eljárást vagy megfelelőségértékelési tevékenységet, és annyiszor 10 490 forint, ahány terméket foglal magában a kérelmezett megfelelőségértékelési terület;

b) egy adott jogszabály vonatkozásában már kijelölt szervezet esetében 66 290 forint, valamint annyiszor 19 370 forint, ahány további megfelelőségértékelési eljárást vagy megfelelőségértékelési tevékenységet, és annyiszor 10 490 forint, ahány további terméket foglal magában a kérelmezett megfelelőségértékelési terület.

(5) A díj mértéke, ha a kérelmezett megfelelőségértékelési terület harmonizációs uniós jogi aktus hatálya alá tartozik, – a kijelölési rendelet 2. mellékletében meghatározott – megfelelőségértékelési területet szabályozó jogszabályonként

a) 160 520 forint, valamint annyiszor 19 370 forint, ahány megfelelőségértékelési eljárást vagy megfelelőségértékelési tevékenységet, és annyiszor 10 490 forint, ahány terméket foglal magában a kérelmezett megfelelőségértékelési terület;

b) egy adott jogszabály vonatkozásában már kijelölt szervezet esetében 76 770 forint, valamint annyiszor 19 370 forint, ahány további megfelelőségértékelési eljárást vagy megfelelőségértékelési tevékenységet, és annyiszor 10 490 forint, ahány további terméket foglal magában a kérelmezett megfelelőségértékelési terület.

2. § (1) A díjak beszedésére, kezelésére, nyilvántartására, elszámolására és visszatérítésére az államháztartás számviteléről szóló kormányrendelet előírásait kell alkalmazni.

(2) Ha a kérelem és a befizetést igazoló okiratok alapján megállapítható, hogy az ügyfél

a) az e rendeletben meghatározott mértéket meghaladó összegű díjat fizetett, vagy

b) eljárás megindítása nélkül fizetett díjat,

akkor az a) pont szerinti esetben a különbözet összegét, a b) pont szerinti esetben a befizetett összeget vissza kell téríteni.

(3) A visszatérítést a többletbefizetés megállapítását követően haladéktalanul, de legfeljebb 8 napon belül hivatalból el kell rendelni.

(4) Ha a többletbefizetést a kérelmező jelzi az eljáró hatóságnak, a visszatérítésre vonatkozó kérelem beérkezését követően haladéktalanul, de legfeljebb 8 napon belül kell elrendelni a visszatérítést.

(5) A visszatérítés teljesítése iránt a visszatérítés elrendelését követő 30 napon belül intézkedni kell. A visszatérítést arra a bankszámlaszámra kell teljesíteni, amelyről a befizetés érkezett. Az ügyfél nyilatkozatával kérheti ettől eltérő bankszámlaszámra is a visszautalást.

(6) Amennyiben készpénzben történt a befizetés és az ügyfél nem tett nyilatkozatot a bankszámlára történő visszautalásról, a visszatérítést készpénzátutalási megbízással kell teljesíteni.

3. § Az e rendeletben meghatározott díj tekintetében

a) a díjfizetési kötelezettségre az illetékekről szóló 1990. évi XCIII. törvény (a továbbiakban: Itv.) 28. § (2) és (3) bekezdésében foglaltakat,

b) a díjfizetésre kötelezettek körének megállapítására az Itv. 31. § (1) és (2) bekezdésében foglaltakat

kell alkalmazni, azzal, hogy ahol az Itv. illetéket említ, azon e jogszabály tekintetében díjat kell érteni.

4. § Ez a rendelet a kihirdetését követő 31. napon lép hatályba.

5. § E rendelet rendelkezéseit a hatálybalépését követően kezdeményezett eljárásokra kell alkalmazni.

6. § Hatályát veszti a közlekedésért felelős miniszter szabályozási feladatkörébe tartozó forgalmazási követelmények tekintetében eljáró megfelelőségértékelő szervezetek kijelölési eljárásáért fizetendő igazgatási szolgáltatási díjakról szóló 89/2011. (XII. 30.) NFM rendelet.

Lázár János s. k.,
építési és közlekedési miniszter

Az építési és közlekedési miniszter 3/2025. (I. 31.) ÉKM rendelete a hajózási hatósági eljárások díjairól

[1] A víziközlekedésről szóló törvény alapján a hatósági eljárásokért fizetendő díjakat rendeletben kell megállapítani, amely törvényi felhatalmazás alapján a rendelet célja a hajózási hatósági eljárásokért fizetendő igazgatási szolgáltatási díjak mértékének, megfizetésével összefüggő szabályainak meghatározása.

[2] A víziközlekedésről szóló 2000. évi XLII. törvény 88. § (2) bekezdés 20. pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 95. § 8. pontjában meghatározott feladatkörömben eljárva – a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 103. § (1) bekezdés 21. pontjában meghatározott feladatkörében eljáró nemzetgazdasági miniszterrel egyetértésben – a következőket rendelem el:

1. § A hajózási hatóság eljárásáért

a) az úszólétesítményekkel, a kikötőkkel kapcsolatos, valamint hatósági engedélyezési eljárások esetében az 1. mellékletben,

b) az úszólétesítmények lajstromozásával kapcsolatos eljárások esetében a 2. mellékletben,

c) hajózási képesítések megszerzésére irányuló képzésekkel és hajózási hatósági személyi nyilvántartásokkal kapcsolatos eljárások esetében a 3. mellékletben

megállapított hatósági eljárási díjat (a továbbiakban együtt: díj) kell fizetni.

2. § (1) A díjat az eljárás kezdeményezőjének az Építési és Közlekedési Minisztérium Magyar Államkincstárnál vezetett, 10032000-00003582-06020015 számú számlájára az eljárás kezdeményezésével egyidejűleg kell befizetni. A díjak beszedésére, kezelésére, nyilvántartására, elszámolására és visszatérítésére az államháztartás szervezetei beszámolási és könyvvezetési kötelezettségeinek sajátosságairól szóló kormányrendelet előírásait kell alkalmazni.

(2) A hajózási hatósági eljárásokért fizetett díj az Építési és Közlekedési Minisztérium bevétele.

(3) Ha a kérelem és a befizetést igazoló okiratok alapján megállapítható, hogy az ügyfél

a) az e rendeletben meghatározott mértéket meghaladó összegű díjat fizetett, vagy

b) eljárás megindítása nélkül fizetett díjat,

akkor az a) pont szerinti esetben a különbözet összegét, a b) pont szerinti esetben a befizetett összeget vissza kell téríteni.

(4) A visszatérítést a többletbefizetés megállapítását követően haladéktalanul, de legfeljebb 8 napon belül hivatalból el kell rendelni.

(5) Ha a többletbefizetést a kérelmező jelzi az eljáró hatóságnak, a visszatérítésre vonatkozó kérelem beérkezését követően haladéktalanul, de legfeljebb 8 napon belül kell elrendelni a visszatérítést.

(6) A visszatérítés teljesítése iránt a visszatérítés elrendelését követő 30 napon belül intézkedni kell. A visszatérítést arra a bankszámlaszámra kell teljesíteni, amelyről a befizetés érkezett. Az ügyfél nyilatkozatával a visszautalást kérheti attól eltérő bankszámlaszámra, amelyről a befizetés érkezett.

(7) Amennyiben készpénzben történt a befizetés, és az ügyfél nem tett nyilatkozatot a bankszámlára történő visszautalásról, a visszatérítést készpénzátutalási megbízással kell teljesíteni.

3. § (1) Ha a hajózási hatóság a jogszabályban előírt hajózási hatósági eljárást kizárólag külföldön folytathatja le, vagy a hajózási hatósági eljárás lefolytatását a kérelmező külföldön kéri, a díjat a felmerült tényleges költségekkel megemelt összegben kell megfizetni.

(2) A külföldön lefolytatandó hatósági eljárás várható költségeiről a kérelmezőt 8 napon belül tájékoztatni kell, amelynek összegét a kérelmezőnek a kérelem benyújtásától számított 5 napon belül meg kell előlegeznie.

(3) A hatósági eljárás befejezése után az eljáró hajózási hatóság a tényleges költségekkel növelt díjról számlát köteles kiállítani.

(4) A számla alapján a befizetett előleg és a ténylegesen elvégzett hatósági tevékenység díja közti különbözetet,

a) amennyiben az ügyfél által befizetett előleg összege több, a hatóság az ügy érdemében hozott határozat meghozatalát követő 15 napon belül az ügyfél részére visszautalja;

b) amennyiben az ügyfél által befizetett előleg összege kevesebb, az ügyfél az ügy érdemében hozott határozat meghozatalát követő 15 napon belül a hatóság részére befizeti.

4. § A hatósági eljárás során igénybe veendő szemlebizottság szakértői tekintetében az ügyfél két szakértő díját köteles megfizetni a 3. § (4) bekezdése alapján, további szakértő bevonása esetén annak költsége a hajózási hatóságot terheli.

5. § Az e rendeletben meghatározott igazgatási szolgáltatási díjak tekintetében

a) a díjfizetési kötelezettségre az illetékekről szóló 1990. évi XCIII. törvény (a továbbiakban: Itv.) 28. § (2)–(3) bekezdésében foglaltakat,

b) a díjfizetésre kötelezettek körének megállapítására az Itv. 31. § (1) és (2) bekezdésében foglaltakat

kell alkalmazni, azzal, hogy ahol az Itv. illetéket említ, azon e jogszabály tekintetében díjat kell érteni.

6. § Ez a rendelet a kihirdetését követő 31. napon lép hatályba.

7. § E rendelet rendelkezéseit a hatálybalépését követően kezdeményezett eljárásokra kell alkalmazni.

8. § Hatályát veszti a hajózási hatósági eljárások díjairól szóló 29/2001. (IX. 1.) KöViM rendelet.

Lázár János s. k.,
építési és közlekedési miniszter

1. melléklet a 3/2025. (I. 31.) ÉKM rendelethez

Az úszólétesítményekkel, kikötőkkel, valamint hatósági engedélyezéssel kapcsolatos hajózási hatósági eljárások (szolgáltatások) díjai

	A	B
1	Eljárás megnevezése	Díj (Ft)
2	Úszólétesítmények építési, átépítési tervének jóváhagyása nagyhajónál, önjáró úszómunkagépnél, önjáró kompnál, továbbá személyszállításra vagy nagyhajók továbbítására szolgáló kishajónál	200 200
3	Úszólétesítmények építési, átépítési tervének jóváhagyása gépnélküli nagyhajónál, nem önjáró kompnál, nem önjáró úszómunkagépnél, továbbá kereskedelmi céllal üzemeltetett úszóműnél	176 800
4	Úszólétesítmények építési, átépítési tervének jóváhagyása a 2. sorba nem tartozó kishajónál és a 3. sorba nem tartozó úszóműnél	122 200
5	A hajó veszélyes áru szállítására, tárolására való alkalmasságát igazoló tervek jóváhagyása, amennyiben azokat külön eljárásban nyújtják be	120 000
6	A hajó egyes fő részeit érintő átépítési tervek jóváhagyása, valamint jóváhagyás nélkül átdolgozásra visszaküldött részlettervek ismételt felülvizsgálatának díja	108 000
7	Úszólétesítmények üzembe helyezési, időszakos, önkéntes üzemképességi vizsgálata, vagy a hajónak vízből kiemelt, illetve partra vont állapotú vizsgálata nagyhajónál, önjáró úszómunkagépnél, önjáró kompnál, személyszállításra vagy nagyhajók továbbítására szolgáló kishajónál, valamint kereskedelmi céllal üzemeltetett úszóműveknél	196 300
8	Úszólétesítmények üzembe helyezési, időszakos, önkéntes üzemképességi vizsgálata, vagy a hajónak vízből kiemelt, illetve partra vont állapotú vizsgálata gépnélküli nagyhajónál, nem önjáró úszómunkagépnél, felépítménnyel rendelkező úszóműnél	124 800
9	Úszólétesítmények üzembe helyezési, időszakos, önkéntes üzemképességi vizsgálata, vagy a hajónak vízből kiemelt, illetve partra vont állapotú vizsgálata a 7. sorba nem tartozó kishajónál és kompnál, továbbá a 8. sorba nem tartozó úszóműnél	84 500

10	Úszólétesítmények üzembe helyezési, időszakos, önkéntes üzemképességi vizsgálata, vagy a hajónak vízből kiemelt, illetve partra vont állapotú vizsgálata kedvtelési célból üzemeltetett gépi vagy vitorlás meghajtású kishajónál, továbbá motoros vízi sporteszköznél, ha annak hajótesten mért hossza a 9 métert nem éri el	59 800
11	Úszólétesítmények üzembe helyezési, időszakos, önkéntes üzemképességi vizsgálata, vagy a hajónak vízből kiemelt, illetve partra vont állapotú vizsgálata kedvtelési célból üzemeltetett gépi vagy vitorlás meghajtású kishajónál, ha annak hajótesten mért hossza a 9 métert eléri, azonban a 12 métert nem haladja meg	113 100
12	Úszólétesítmények üzembe helyezési, időszakos, önkéntes üzemképességi vizsgálata, vagy a hajónak vízből kiemelt, illetve partra vont állapotú vizsgálata kedvtelési célból üzemeltetett gépi vagy vitorlás meghajtású kishajónál, ha annak hajótesten mért hossza a 12 métert meghaladja	144 300
13	Hajó veszélyes áru szállítására, tárolására történő alkalmasságának vizsgálata, amennyiben azokat külön eljárásban nyújtják be	196 300
14	Tengeri hajó köbözéséért felszámítható díj alapdíja	280 800
15	A felső fedélzet felett zárt helyiség és hajószemélyzet számára szolgáló helyiségek, valamint a géphelyiség felmérésének alapdíja	330 200
16	A Szuezi-, a Sulina- és a Panama-csatorna használatához szükséges köbözés alapdíja	102 700
17	Belvízi hajó köbözése	107 900
18	A belvízi hajónál a centiméterenkénti terhelhetőség megállapítása	93 600
19	Hajóradar, fordulási szögsebesség mérő berendezések és AIS készülék vizsgálata, illetve tájoló kompenzálása, amennyiben a vizsgálat nem esik egybe az üzemképességi vizsgálatokkal	100 100
20	Kikötő létesítésének vagy a fennmaradásának engedélyezése esetén a kikötő létesítési terv felülvizsgálati, engedélyezési eljárásának alapdíja nagyhajók fogadására alkalmas kikötő, valamint ferde pályás hajókiemelő berendezés, hajóállomás, úszóműves kikötőhely esetében	206 000
21	Kikötő létesítésének vagy a fennmaradásának engedélyezése esetén a kikötő létesítési terv felülvizsgálati, engedélyezési eljárásának alapdíja kishajók (csónakok) fogadására alkalmas kikötő esetében	108 000
22	Kikötő létesítésének vagy a fennmaradásának engedélyezése esetén az alapdíjon felül a kikötésre alkalmas part élének hossza, úszóműves kikötőhelynél az úszómű hosszának 2,5-szerese alapján méterenként nagyhajók fogadására alkalmas kikötőnél	2 600
23	Kikötő létesítésének vagy a fennmaradásának engedélyezése esetén az alapdíjon felül a kikötésre alkalmas part élének hossza, úszóműves kikötőhelynél az úszómű hosszának 2,5-szerese alapján méterenként kishajók (csónakok) fogadására alkalmas kikötőnél	1 300
24	Kikötő létesítésének vagy a fennmaradásának engedélyezése esetén a kikötő fennmaradásának engedélyezése	a 20–21., 22–23. és 31–32. sorban megállapított eljárási díj összegének kétszerese
25	Kikötő létesítésének vagy a fennmaradásának engedélyezése esetén a kikötő létesítési terv módosításának engedélyezési díja, illetve a létesítési engedély meghosszabbításának díja	115 700
26	Komp- és révátkelőhely létesítésének engedélyezése	186 000
27	Komp- és révátkelőhely fennmaradásának engedélyezése	274 000
28	Hajóhíd létesítésének használatba vételének engedélyezése, a létesítési vagy üzemben tartási engedély kiadása eljárásonként nemzetközi vízi úton	213 200

29	Hajóhíd létesítésének használatba vételének engedélyezése, a létesítési vagy üzemben tartási engedély kiadása eljárásonként egyéb belvizeken	209 600
30	Hajózási létesítmény elhelyezésének elvi engedélyeztetési díja	108 000
31	Kikötő használatbavétele során a használatbevétel engedélyezése a kikötő part élének hossza alapján	1 300
32	Kikötő használatbavétele során a használatbevétel engedélyezése úszóműves kikötőhelynél az úszómű hosszának 2,5-szerese alapján méterenként	1 300
33	Kikötő használatbavétele során a hajózási létesítmény üzemelési szabályzat megállapítása	43 000
34	Kikötő használatba vétele során kikötőrend jóváhagyása	39 000
35	Komp- és révátkelőhely használatba vételi eljárásának díja	189 000
36	Kikötők üzemben tartásának engedélyezése a kikötők part élének hossza, a vendégmóló hossza, úszóműves kikötőhelynél az úszómű hossza, a ferde pályás hajókiemelő berendezés szélessége alapján méterenként	13 000
37	Kikötő megszüntetésének eljárása	68 000
38	Komp- és révátkelőhely üzemben tartásának engedélyezése	183 300
39	Komp- és révátkelés megszüntetése	180 700
40	Hajózási engedély kiadásának alapdíja	116 000
41	Hajózási engedély kiadásának további díja vízkiszorítási tonnánként	26
42	Hajózási engedély meghosszabbításának alapdíja	4000
43	Hajózási engedély meghosszabbításának további díja vízkiszorítási tonnánként	26
44	Hajózási engedély módosításának alapdíja	112 000
45	Hajózási engedély módosításának további díja vízkiszorítási tonnánként	26
46	Harmadik országos/lobogós és kabotázs engedélyezéssel kapcsolatos eljárás megkezdett eljárásonként	197 600
47	Elvi hajózási engedély kiállítása	13 000
48	Különleges szállítás, valamint radioaktív anyag belvízi szállításának engedélyezése	115 000
49	Üzemeltetési engedély kiadás korlátozás alá eső vízterületekre (hajózási engedélyköteles tevékenységhez)	55 000
50	Üzemeltetési engedély kiadás korlátozás alá eső vízterületekre (sportegyesületek)	48 000
51	Zsilipszabályzat jóváhagyása	51 000
52	Rajnai hajózásban való részvételi jogosultságot igazoló okmány kiállítása	113 000
53	Nyaralóhajó bérbeadására vonatkozó egyedi engedélyezés alapdíja, továbbá nyaralóhajónként	124 000
54	Nyaralóhajó bérbeadására vonatkozó egyedi engedélyezés további díja nyaralóhajónként	57 000
55	Nyaralóhajó bérbeadására vonatkozó egyedi engedély módosításának alapdíja	114 400
56	Nyaralóhajó bérbeadására vonatkozó egyedi engedély módosításának további díja a módosítással érintett nyaralóhajónként	58 000
57	A víziközlekedés irányítására szolgáló jelzések elhelyezése (létesítés), üzembe helyezése, fennmaradása, üzemeltetése, valamint megszüntetésének alapdíja	72 000
58	Az 57. soron túl jelenként/jelzésenként további (db)	2 600
59	Víziúton vagy annak közelében munkavégzés engedélyezése	67 000
60	Az 59. soron túl továbbá ideiglenes rakodási tevékenység esetében megkezdett 100 tonnánként	800
61	Hajózási tevékenység korlátozása nemzetközi vízi úton	75 400
62	Hajózási tevékenység korlátozása egyéb belvizeken	39 000
63	A hajóútban felakadt, elsüllyedt hajóval kapcsolatos szemle vagy felülvizsgálat díja alkalmanként (Ft/óra)	13 000

64	A hajóutat és a hajók forgalmát érintő jelzőállomás létesítésének használatba vételének és üzemben tartásának engedélyezése eljárásonként	156 000
65	A vízi sportpályák és vízi repülőterek létesítésének használatba vételének és üzemben tartásának engedélyezése eljárásonként	72 000
66	Hajóokmányok és egyéb engedélyek pótlása, cseréje	13 000
67	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – nemzetközi, hajó okmányok kiállítása és kiegészítése tengeri nagyhajók esetében	63 000
68	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – nemzetközi, hajó okmányok érvényesítése tengeri nagyhajók esetében	63 000
69	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – tengeri hajók különböző nemzeti okmányai kiállítása szemlejegyzőkönyv alapján	35 000
70	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – hajónapló kiadása esetén	9 400
71	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – személyzeti jegyzék kiadása esetén	9 400
72	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – okmányok pótlása, cseréje (a 69. pontban foglaltak kivételével)	9 400
73	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – kártya formátumú biztonsági okmány kiállítása esetén	10 400
74	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – fáradtolaj, motor, tengeri olaj és hulladékkezelési napló kiadása esetén	9 100
75	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – gépnapló kiadása esetén	9 100
76	Nemzetközi, hajó és hajós, illetve tengerész okmányok (okmány-nyomtatványok árának térítése nélkül) díjai – hajónapló, felszerelési füzet, személyzeti jegyzék kiadása kedvtelési célú kishajó esetében	9 100
77	Átmeneti hatósági rendelkezés közzététele kérelemre	22 900
78	A hatósági nyilvántartásban szereplő adatokban (kivéve lajstrom) bekövetkezett változások átvezetése (például tulajdonjog-változás, üzemeltetői jog, átalakulás, névváltozás)	13 000
79	Az úszólétesítmény építés közben kérelemre lefolytatott szemléje	44 000
80	Típus-jóváhagyási eljárás	35 000
81	A típus-jóváhagyási bizonyítvány érvényessége meghosszabbításának díja	27 300
82	Úszólétesítmények előírttól eltérő feltételekkel közlekedésének, illetve igénybevételének ideiglenes engedélyezése	78 000
83	Úszóműállás létesítési engedélyezése vagy időszakos szemléjének alapdíja	3 900
84	A 80. soron túl a fő fedélzet területe szerinti négyzetméterenként	260
85	Úszóműállás használatba vételének és üzemben tartásának engedélyezése eljárásonként	22 100
86	Tengeri hajók előírt biztonsági dokumentumainak jóváhagyása (például riadóterv, rakománykezelési, tűzvédelmi, hajóelhagyási, stabilitási, biztonsági kézikönyvek)	90 000
87	Megbízás kiadása hatósági szemle megtartására, kérelemre	24 000
88	Hajósoknak, illetve tengerészeknek szóló hatósági tájékoztató kiadása kérelemre A/4-es oldalanként	54 000
89	Adatszolgáltatás hatósági nyilvántartásban szereplő adatokról kérelemre A/4-es oldalanként	30 000
90	Szakvélemény kiadása kérelemre A/4-es oldalanként	54 000
91	Szakhatósági díj szakhatósági eljárás esetén	54 000

92	Nemzetközi azonosítók (nominatív) kijelölése	25 000
93	Szemlebizottság felkért tagjainak díjazása, óránként	13 000
94	Úszóműállás üzemeltetési szabályzat, kikötőrend, zsilipszabályzat jóváhagyása	60 000
95	Az engedélyezés során szükségessé váló szemle, továbbá a helyszíni felülvizsgálat díja alkalmanként	36 000
96	Úszólétesítmények üzemképességi vizsgálatához és tanúsításához, úszólétesítményeken alkalmazott felszerelések, berendezések alkalmasságának megállapításához szükséges külön vizsgálatok hatósági szemléje	62 000
97	Szállítótartályokat gyártó és javító üzemek, próbaállomások jóváhagyása elismerése	165 000
98	Konténer terv jóváhagyása	140 000
99	Konténer szemléi (üzembe helyezés, időszakos, javítás utáni, illetve az engedélyezés során előírt)	140 000
100	Szállítótartály okmánykiállítása CSC tábla érvényesítés	22 900
101	Gyártó és javító üzemek jóváhagyása elismerése, időszakonkénti vizsgálata	106 000
102	A tengerész munkaközvetítő és a tengerész kölcsönbeadó nyilvántartásba vétele és a nyilvántartásba vételt tanúsító bizonyítvány kiállítása	207 000
103	A hajózási egészségi alkalmasság vizsgálatára jogosult orvos nyilvántartásba vétele	100 000

2. melléklet a 3/2025. (I. 31.) ÉKM rendelethez

Úszólétesítmények lajstromozásával kapcsolatos hatósági eljárások (szolgáltatások) díjai

	A	B
1	Eljárás	Díj (Ft)
2	Új úszólétesítmény lajstromozásakor vagy a tulajdonjogban bekövetkezett változás bejegyzésekor – belvízi nagyhajók és úszómunkagépeknél	65 000
3	Új úszólétesítmény lajstromozásakor vagy a tulajdonjogban bekövetkezett változás bejegyzésekor – belvízi kompok, gazdasági célból üzemeltetett úszóművek és kishajónál	6 750
4	Új úszólétesítmény lajstromozásakor vagy a tulajdonjogban bekövetkezett változás bejegyzésekor – kedvtelési célból üzemeltetett kishajó, úszómű és motoros vízi sporteszközöknél	40 300
5	A lajstromba bejegyezhető jogok, és feljegyezhető tények; bejegyzésre kerülő jogonként és feljegyezhető tényenként, külön-külön be- vagy feljegyzési, módosítási és törlési eljárásonként, valamint bejegyzési ranghely előzetes biztosítási kérelemmel kapcsolatos eljárás díja belvízi nagyhajók és úszómunkagépeknél	41 000
6	A lajstromba bejegyezhető jogok, és feljegyezhető tények; bejegyzésre kerülő jogonként és feljegyezhető tényenként, külön-külön be- vagy feljegyzési, módosítási és törlési eljárásonként, valamint bejegyzési ranghely előzetes biztosítási kérelemmel kapcsolatos eljárás díja belvízi kompok, gazdasági célból üzemeltetett úszóműveknél és kishajónál	20 000
7	A lajstromba bejegyezhető jogok, és feljegyezhető tények; bejegyzésre kerülő jogonként és feljegyezhető tényenként, külön-külön be- vagy feljegyzési, módosítási és törlési eljárásonként, valamint bejegyzési ranghely előzetes biztosítási kérelemmel kapcsolatos eljárás díja kedvtelési célból üzemeltetett kishajó, úszómű és motoros vízi sporteszközöknél	40 300
8	Ideiglenes lajstromba vétel	42 900
9	Tulajdoni lap igazolás kiadása úszólétesítményenként	42 900
10	Lajstromozási okmány kiállítása	32 500
11	A lajstrom adataiban igazolt változás miatti módosítás, lajstromból és ideiglenes lajstromból történő törlés és a változás bejegyzésének tanúsítása	22 100

3. melléklet a 3/2025. (I. 31.) ÉKM rendelethez

A hajózási képesítések megszerzésére irányuló képzésekkel és hajózási hatósági személyi nyilvántartásokkal kapcsolatos eljárások díjai

	A	B
1	Eljárás	Díj (Ft)
2	Személyi nyilvántartásba vétel, a hajózási hatóság nyilvántartásában, névjegyzékeiben szereplő adatok módosítása, igazolása	9 100
3	Oktatási napló kiadása	3 900
4	Képzés engedélyezésének alapdíja	113 000
5	A 4. soron felül a képzés engedélyezésének díja további tárgyanként	5 300
6	Képzési engedély módosításának, megújításának, kiegészítésének alapdíja	54 000
7	Képzési engedély módosításának, megújításának, kiegészítésének díja továbbá tárgyanként a 6. soron túl	5 300
8	Számítógépes képzési program jóváhagyásának alapdíja	43 200
9	A 8. soron felül továbbá minden megkezdett megabájt	3 900
10	Képesítő okmány honosítása esetén	23 400
11	Hajózási gyakorlati idő mérséklésének engedélyezése esetén	23 400

Az építési és közlekedési miniszter 4/2025. (I. 31.) ÉKM rendelete a nem közúti mozgó gépek belső égésű motorjaival kapcsolatos típusjóváhagyási eljárással összefüggésben fizetendő igazgatási szolgáltatási díjakról

[1] A közúti közlekedésről szóló törvény alapján a hatósági eljárásokért fizetendő díjakat rendeletben kell megállapítani, amely törvényi felhatalmazás alapján a rendelet célja a nem közúti mozgó gépek belső égésű motorjaival kapcsolatos típusjóváhagyási eljárással összefüggésben fizetendő igazgatási szolgáltatási díjak mértékének, megfizetésével összefüggő szabályainak meghatározása.

[2] A közúti közlekedésről szóló 1988. évi I. törvény 48. § (3) bekezdés e) pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 95. § 8. pontjában meghatározott feladatkörömben eljárva – a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 103. § (1) bekezdés 21. pontjában meghatározott feladatkörében eljáró nemzetgazdasági miniszterrel egyetértésben – a következőket rendelem el:

1. § A nem közúti mozgó gépek belső égésű motorjainak a gáz- és szilárd halmazállapotú szennyezőanyag-kibocsátási határértékeire és típusjóváhagyására vonatkozó követelményekről, az 1024/2012/EU és a 167/2013/EU rendelet módosításáról, valamint a 97/68/EK irányelv módosításáról és hatályon kívül helyezéséről szóló, 2016. szeptember 14-i (EU) 2016/1628 európai parlamenti és tanácsi rendeletben (a továbbiakban: 2016/1628 európai parlamenti és tanácsi rendelet) szabályozott hatósági eljárásokért az eljáró közlekedési hatóság részére az 1. mellékletben meghatározott igazgatási szolgáltatási díjat (a továbbiakban: díj) kell fizetni.

2. § (1) A kérelemre indult hatósági eljárások esetén az eljárás kezdeményezőjének a díjat az Építési és Közlekedési Minisztériumnak (a továbbiakban: ÉKM) a Magyar Államkincstárnál vezetett, 10032000-00003582-06020015 számú számlájára kell az eljárás kezdeményezésével egyidejűleg megfizetnie.

(2) A díj az ÉKM bevétele.

(3) A díjak beszedésére, kezelésére, nyilvántartására, elszámolására és visszatérítésére az államháztartás számviteléről szóló kormányrendelet előírásait kell alkalmazni.

(4) Ha a kérelem és a befizetést igazoló okiratok alapján megállapítható, hogy az ügyfél
a) az e rendeletben meghatározott mértéket meghaladó összegű díjat fizetett, vagy
b) eljárás megindítása nélkül fizetett díjat,
akkor az a) pont szerinti esetben a különbözet összegét, a b) pont szerinti esetben a befizetett összeget vissza kell téríteni.

(5) A visszatérítést a többletbefizetés megállapítását követően haladéktalanul, de legfeljebb 8 napon belül hivatalból el kell rendelni.

(6) Ha a többletbefizetést a kérelmező jelzi az eljáró hatóságnak, a visszatérítésre vonatkozó kérelem beérkezését követően haladéktalanul, de legfeljebb 8 napon belül kell elrendelni a visszatérítést.

(7) A visszatérítés teljesítése iránt a visszatérítés elrendelését követő 30 napon belül intézkedni kell. A visszatérítést arra a bankszámlaszámra kell teljesíteni, amelyről a befizetés érkezett. Az ügyfél nyilatkozatával kérheti ettől eltérő bankszámlaszámra is a visszautalást.

(8) Amennyiben készpénzben történt a befizetés, és az ügyfél nem tett nyilatkozatot a bankszámlára történő visszautalásról, a visszatérítést készpénzátutalási megbízással kell teljesíteni.

3. § Az e rendeletben meghatározott díjak tekintetében
a) a díjfizetési kötelezettségre az illetékekről szóló 1990. évi XCIII. törvény (a továbbiakban: Itv.) 28. § (2) és (3) bekezdésében foglaltakat,
b) a díjfizetésre kötelezettek körének megállapítására az Itv. 31. § (1) és (2) bekezdésében foglaltakat
kell alkalmazni, azzal, hogy ahol az Itv. illetéket említ, azon e jogszabály tekintetében díjat kell érteni.

4. § Ez a rendelet a kihirdetését követő 31. napon lép hatályba.

5. § E rendelet rendelkezéseit a hatálybalépését követően kezdeményezett eljárásokra kell alkalmazni.

6. § Hatályát veszti a nem közúti mozgó gépek belső égésű motorjaival kapcsolatos típusjóváhagyási eljárással összefüggésben fizetendő igazgatási szolgáltatási díjakról szóló 35/2019. (IX. 18.) ITM rendelet.

Lázár János s. k.,
építési és közlekedési miniszter

1. melléklet a 4/2025. (I. 31.) ÉKM rendelethez

A 2016/1628 európai parlamenti és tanácsi rendeletben szabályozott hatósági eljárásokért fizetendő díjak

	A	B
1	Eljárás	Díj (Ft)
2	Típusjóváhagyási eljárás motorcsaládonként	120 800
3	Típusjóváhagyási eljárás alóli felmentés, a rugalmas végrehajtás engedélyezése iránti kérelemre végzett hatósági eljárás, valamint a típusjóváhagyási bizonyítvány módosítása, kiterjesztése	120 800
4	A 2016/1628 európai parlamenti és tanácsi rendelet 37. cikk (1) bekezdése szerinti regisztrációért fizetendő díj	motoronként 8 800

Az építési és közlekedési miniszter 5/2025. (I. 31.) ÉKM rendelete a veszélyes áru szállítási biztonsági tanácsadók névjegyzékbe vételének díjairól

[1] A közúti közlekedésről szóló törvény alapján a hatósági eljárásokért fizetendő díjakat rendeletben kell megállapítani, amely törvényi felhatalmazás alapján a rendelet célja a veszélyes áru szállítási biztonsági tanácsadók névjegyzékbe vételére irányuló hatósági eljárásokért fizetendő igazgatási szolgáltatási díjak mértékének, megfizetésével összefüggő szabályainak meghatározása.

[2] A közúti közlekedésről szóló 1988. évi I. törvény 48. § (3) bekezdés e) pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 95. § 8. pontjában meghatározott feladatkörömben eljárva – a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 103. § (1) bekezdés 21. pontjában meghatározott feladatkörében eljáró nemzetgazdasági miniszterrel egyetértésben – a következőket rendelem el:

1. § (1) A veszélyes áru szállítási biztonsági tanácsadók névjegyzékébe vételéért az 1. melléklet szerinti díjat az eljárás kezdeményezőjének az Építési és Közlekedési Minisztérium (a továbbiakban: ÉKM) Magyar Államkincstárnál vezetett, 10032000-00003582-06020015 számú számlájára kell az eljárás kezdeményezésével egyidejűleg megfizetnie.

(2) Az eljárásokért fizetett díj az ÉKM bevétele.

(3) A díjak beszedésére, kezelésére, nyilvántartására, elszámolására és visszatérítésére az államháztartás számviteléről szóló kormányrendelet előírásait kell alkalmazni.

(4) Ha a kérelem és a befizetést igazoló okiratok alapján megállapítható, hogy az ügyfél

a) az e rendeletben meghatározott mértéket meghaladó összegű díjat fizetett, vagy

b) eljárás megindítása nélkül fizetett díjat,

akkor az a) pont szerinti esetben a különbözet összegét, a b) pont szerinti esetben a befizetett összeget vissza kell téríteni.

(5) A visszatérítést a többletbefizetés megállapítását követően haladéktalanul, de legfeljebb 8 napon belül hivatalból el kell rendelni.

(6) Ha a többletbefizetést a kérelmező jelzi az eljáró hatóságnak, a visszatérítésre vonatkozó kérelem beérkezését követően haladéktalanul, de legfeljebb 8 napon belül kell elrendelni a visszatérítést.

(7) A visszatérítés teljesítése iránt a visszatérítés elrendelését követő 30 napon belül intézkedni kell. A visszatérítést arra a bankszámlaszámra kell teljesíteni, amelyről a befizetés érkezett. Az ügyfél nyilatkozatával a visszautalást kérheti attól eltérő bankszámlaszámra, amelyről a befizetés érkezett.

(8) Amennyiben készpénzben történt a befizetés és az ügyfél nem tett nyilatkozatot a bankszámlára történő visszautalásról, a visszatérítést készpénzátutalási megbízással kell teljesíteni.

2. § Az e rendeletben meghatározott díjak tekintetében

a) a díjfizetési kötelezettségre az illetékekről szóló 1990. évi XCIII. törvény (a továbbiakban: Itv.) 28. § (2)–(3) bekezdésében foglaltakat,

b) a díjfizetésre kötelezettek körének megállapítására az Itv. 31. § (1) és (2) bekezdésében foglaltakat

kell alkalmazni, azzal, hogy ahol az Itv. illetéket említ, azon e jogszabály tekintetében díjat kell érteni.

3. § Ez a rendelet a kihirdetését követő 31. napon lép hatályba.

4. § E rendelet rendelkezéseit a hatálybalépését követően kezdeményezett eljárásokra kell alkalmazni.

5. § Hatályát veszti a veszélyes áru szállítási biztonsági tanácsadó képzésének, vizsgáztatásának szabályairól és díjairól szóló 8/2002. (I. 30.) KöViM rendelet.

Lázár János s. k.,
építési és közlekedési miniszter

1. melléklet az 5/2025. (I. 31.) ÉKM rendelethez

A veszélyesáru-szállítási biztonsági tanácsadó névjegyzékbe vételének díjai

	A	B
1	Eljárás	Díj (Ft/db)
2	Névjegyzékbe vétel alágazatonként	8700
3	Az érvényesség öt évre szóló meghosszabbítása	3000

A honvédelmi miniszter 2/2025. (I. 31.) HM rendelete a katonával szemben elrendelt bűnügyi felügyelet betartásának ellenőrzéséről

A büntetőeljárásról szóló 2017. évi XC. törvény 866. § (4) bekezdés b) pontjában kapott felhatalmazás alapján, a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 112. § 1. pontjában meghatározott feladatkörömben eljárva – a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 119. § 1. pontjában meghatározott feladatkörében eljáró igazságügyi miniszterrel egyetértésben –,
a 10. § tekintetében a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 110. § (2) bekezdés 7. pontjában meghatározott feladatkörömben eljárva
a következőket rendelem el:

1. Általános rendelkezések

1. § E rendelet alkalmazásában

1. *bíróság:* a bűnügyi felügyeletet határozatban vagy végzésben elrendelő bíróság,
2. *bűnügyi felügyelet:* a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) 281. § (2) bekezdés a) pontjában meghatározott kényszerintézkedés,
3. *honvédelmi szervezet:* a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 3. § 14. pontja szerinti honvédelmi szervezet,
4. *katona:* a Magyar Honvédség hivatásos, szerződéses, a tényleges szolgálatát teljesítő önkéntes tartalékos állományú tagja és a honvéd tisztjelölt,
5. *katonai rendész:* a bűnügyi felügyelet helye szerinti katonai rendészeti alkalmazási körzetbe kirendelt katonai rendész járőr,
6. *szakképző intézmény:* a honvédelemért felelős miniszter fenntartói irányítása alá tartozó, honvédelmi szervezetnek nem minősülő, többcélú szakképző intézmény.

2. A bűnügyi felügyelet szabályai betartásának ellenőrzése

2. § (1) A bűnügyi felügyelet keretében előírt magatartási szabályok megtartásának ellenőrzését katona terhelt esetében a parancsnok végzi, szükség esetén a terhelt tényleges tartózkodási helye szerint illetékes, a magatartási szabállyal érintett rendőrkapitányság (a továbbiakban: illetékes rendőrkapitányság) közreműködésével.

(2) A bíróság vagy az ügyészség a bűnügyi felügyelet elrendeléséről, meghosszabbításáról, fenntartásáról, megszűnéséről, megszüntetéséről, részleges feloldásáról, módosításáról, a terhelt számára enyhébb vagy hátrányosabb magatartási szabályok megállapításáról hozott döntéséről a határozat vagy a határozat rendelkező részének megküldésével tájékoztatja az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnokot.

(3) A parancsnok a bűnügyi felügyelet szabályai betartásának ellenőrzését a nyomozótiszt útján, szükség esetén a katonai rendész bevonásával, közreműködésével hajtja végre. A katonai rendészt a parancsnok írásos felkérése alapján a katonai rendészeti szerv vezetője rendeli ki. A katonai rendész – a bűnügyi felügyeletet elrendelő bírósági határozatban foglaltaknak megfelelő módon és mértékben – kapcsolatot tart az illetékes rendőrkapitánysággal.

(4) Az ellenőrzési kötelezettség a bűnügyi felügyeletet elrendelő bírósági határozat vagy végzés (a továbbiakban együtt: bírósági határozat) parancsnok általi kézhezvételével kezdődik, és a bűnügyi felügyelet megszüntetéséig, megszűnéséig vagy a katona szolgálati viszonyának fennállásáig tart.

(5) Ha a bíróság vagy az ügyészség határozata több terheltről rendelkezik, a bíróság vagy az ügyészség a határozat vagy a határozat rendelkező része megküldésével egyidejűleg tájékoztatja az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnokot, hogy az ellenőrzést mely terhelt vagy terheltek tekintetében kell végrehajtania, illetve megszüntetnie.

(6) Ha a bíróság vagy az ügyészség a bűnügyi felügyelet megszűnéséről nem hoz határozatot, akkor a büntetőeljárást folytató bíróság, ügyészség vagy nyomozó hatóság az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnokot a bűnügyi felügyelet megszűnéséről tájékoztatja.

(7) Az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnokot a bűnügyi felügyelet elrendeléséről, meghosszabbításáról, fenntartásáról, megszűnéséről, megszüntetéséről, részleges feloldásáról, módosításáról, valamint a terhelt számára enyhébb vagy hátrányosabb magatartási szabályok megállapításáról haladéktalanul tájékoztatni kell.

3. § (1) Ha a bíróság a bűnügyi felügyelet magatartási szabályainak megtartását biztosító intézkedésként a katona mozgását nyomon követő technikai eszköz használatát rendelte el, a bíróság a technikai eszköz telepítéséről az illetékes rendőrkapitányság útján intézkedik.

(2) A terhelt mozgását nyomon követő technikai eszköz elrendelése esetén a bíróság tájékoztatja a terheltet arról, hogy a technikai eszköz telepítése során köteles a telepítést végző rendőri szervvel együttműködni, valamint arról is, hogy ha az együttműködési kötelezettségét megszegi, az a magatartási szabályok megszegésének minősül.

(3) A terhelt mozgását nyomon követő technikai eszköz elrendelését követően a technikai eszköz telepítését végző rendőri szerv a terheltet a bíróság által kijelölt tényleges tartózkodási helyére kíséri.

(4) Ha a bűnügyi felügyelet elrendelésére vagy megkezdésére fogvatartásban lévő terhelt szabadlábra helyezésével egyidejűleg került sor, a terhelt mozgását nyomon követő technikai eszköz telepítésével kapcsolatos feladatok ellátása érdekében a bíróság a terheltet fogva tartó intézettel, valamint az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnokkal egyeztethet.

(5) A terhelt mozgását nyomon követő technikai eszköz alkalmazása esetén a telepítést végző rendőri szerv felhívja a terheltet, hogy biztosítsa a technikai eszköz testére történő rögzítésének, valamint a technikai eszköz telepítésének lehetőségét.

(6) A technikai eszközt a terhelt testére oly módon kell rögzíteni, hogy az a külvilág számára lehetőleg ne legyen látható, és a terheltet a mindennapi teendőinek elvégzésében ne akadályozza.

(7) A technikai eszköz telepítése során a telepítést végző rendőri szerv tájékoztatja a terheltet a technikai eszköz működésével kapcsolatos tudnivalókról, valamint a technikai eszközben okozott kár polgári jogi és büntetőjogi következményeiről. A tájékoztatás írásbeli tájékoztató átadásával is teljesíthető, azonban ebben az esetben is meg kell győződni arról, hogy a terhelt a technikai eszközzel kapcsolatos tájékoztatóban foglaltakat megértette.

(8) Ha a telepítést végző rendőri szerv azt állapítja meg, hogy a terhelt mozgását nyomon követő technikai eszköz a kijelölt helyen nem telepíthető, erről a vádemelés előtt a nyomozó hatóságot vagy az ügyészséget, a vádemelés után a bíróságot tájékoztatja. A terhelt őrizetének a bíróság, az ügyészség vagy a nyomozó hatóság által a Be. 293. § (1) bekezdése alapján történt elrendelését követően a rendőri szerv a terheltet a Rendőrségről szóló 1994. évi XXXIV. törvény 33. § (1) bekezdés c) pontja alapján haladéktalanul elfogja és előállítja.

4. § (1) A parancsnok a katonával szemben elrendelt, a Be. 705. § (5) bekezdése szerinti bűnügyi felügyeletről való tudomásszerzést követően parancsban vagy határozatban (a továbbiakban együtt: parancs) rendelkezik

a) a bírósági határozatban foglaltakra figyelemmel a bűnügyi felügyelet ellenőrzése végrehajtásának módjáról, gyakoriságáról,

b) a katonának az a) pont szerint meghatározott ellenőrzéssel kapcsolatos együttműködési kötelezettségeiről,

c) az ellenőrzést végrehajtó személyek köréről, az ellenőrzés kijelölt vezetőjéről és

d) az ellenőrzés végrehajtásáról készítendő okmányokról.

(2) A bírósági határozatban foglaltakra figyelemmel a parancsban a parancsnok felhívja a katona figyelmét az ellenőrzés tűrésével és az abban való együttműködéssel kapcsolatos törvényi kötelezettségeire.

5. § (1) A bűnügyi felügyelet keretében előírt magatartási szabályok megtartásának ellenőrzése ellátható
a) a katonai rendész útján napi, többnapi, heti vagy többheti rendszerességgel,
b) eseti ellenőrzéssel, illetve
c) folyamatos ellenőrzéssel.

(2) A bíróság az (1) bekezdés c) pontja szerinti ellenőrzés elrendeléséről akkor rendelkezhet, ha a terhelt letartóztatása a Be. 298. § (1) bekezdésében meghatározott tartam letelte miatt szűnik meg.

(3) Az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnok a magatartási szabályok ellenőrzését elláthatja a bíróság rendelkezése hiányában – a magatartási szabályok jellegéhez, illetve a személyi szabadságot érintő kényszerintézkedés végrehajtásával összefüggésben rendelkezésére álló információkhoz igazodóan – az (1) bekezdés a) és b) pontja alapján.

(4) A Be. 281. § (2) bekezdés c) pontja szerinti jelentkezési kötelezettség előírása esetén az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnok rögzíti, hogy a terhelt eleget tesz-e a határozatban megjelölt jelentkezési módnak és időköznek.

6. § (1) Halasztást nem tűrő – különösen a terhelt egészségét veszélyeztető – esetben a terhelt mozgását nyomon követő technikai eszköz eltávolításáról az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnok is rendelkezhet. Az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnok a technikai eszköz eltávolítását követően az 5. § (1) bekezdés a), b) vagy c) pontja szerint biztosítja a terhelt megfelelő ellenőrzését, és a technikai eszköz eltávolításának okáról, körülményeiről haladéktalanul tájékoztatja a büntetőeljárást folytató bíróságot, ügyészséget vagy nyomozó hatóságot.

(2) A terhelt mozgását nyomon követő technikai eszköz üzemzavara vagy üzemszünete esetén, a bíróság eltérő rendelkezése hiányában, az előírt magatartási szabályok megtartásának ellenőrzését végző parancsnok az 5. § (1) bekezdés a), b) vagy c) pontja szerint biztosítja a terhelt megfelelő ellenőrzését, és az üzemzavar, üzemszünet okáról és körülményeiről haladéktalanul tájékoztatja a büntetőeljárást folytató bíróságot, ügyészséget vagy nyomozó hatóságot.

7. § (1) A bűnügyi felügyelet ellenőrzéséről jegyzőkönyv készül. A jegyzőkönyv elkészítéséért az ellenőrzés kijelölt vezetője felelős.

(2) A jegyzőkönyv tartalmazza a bűnügyi felügyelet elrendeléséről szóló bírósági határozatra való hivatkozást, a katona figyelmeztetését a bűnügyi felügyelettel és annak ellenőrzésével kapcsolatos kötelezettségeire, az ellenőrzés helyét, idejét, a jelen lévő személyeket és az ellenőrzés megállapításait a bűnügyi felügyelet szabályai betartására vonatkozóan.

(3) Ha az ellenőrzés a bűnügyi felügyelet szabályainak megsértését állapítja meg, a parancsnok a jegyzőkönyvet haladéktalanul megküldi a bíróság részére.

3. Záró rendelkezések

8. § (1) Ez a rendelet – a (2) bekezdésben foglalt kivétellel – a kihirdetését követő napon lép hatályba.

(2) Az 1–7. §, a 9. § és a 11. § az e rendelet kihirdetését követő 8. napon lép hatályba.

9. § E rendelet hatálybalépését követően a katona tekintetében nem alkalmazható a szoros felügyelet alá helyezés végrehajtásának, valamint a katonával szemben elrendelt lakhelyelhagyási tilalom ellenőrzésének szabályairól szóló 46/2002. (X. 10.) HM–BM–IM–MeHVM együttes rendelet.

10. § A kegyeleti gondoskodásról és az ehhez kapcsolódó egyes szociális feladatokról szóló 7/2013. (VII. 25.) HM rendelet 2. § (4) bekezdése helyébe a következő rendelkezés lép:
„(4) Azt az elhunytat, aki honvédelmi területen vagy a honvédelem érdekében tevékenykedett, a miniszter – át nem ruházható egyedi döntésével – a „Honvédelmi Minisztérium saját halottjává” nyilváníthatja.”

11. § Hatályát veszti a szoros felügyelet alá helyezés végrehajtásának, valamint a katonával szemben elrendelt lakhelyelhagyási tilalom ellenőrzésének szabályairól szóló 46/2002. (X. 10.) HM–BM–IM–MeHVM együttes rendelet

a) 1. § d) pontjában az „a Magyar Honvédség (a továbbiakban: MH) hivatásos (szerződéses) állományába tartozó katona tekintetében az MH hivatásos és szerződéses állományú katonáinak jogállásáról szóló 2001. évi XCV. törvény (a továbbiakban: Hjt.) 2. §-ának (3) bekezdésében, más katona tekintetében" szövegrész,

b) 1. § e) pontjában az „az MH tekintetében a Hjt. 2. §-ának (10) bekezdésében, más fegyveres szerv vonatkozásában" szövegrész,

c) 1. § h) pontjában az „az MH hivatásos és szerződéses állományú katonája vonatkozásában a Hjt. 2. §-ának (21) bekezdésében, más katona tekintetében" szövegrész,

d) 1. § i) pontjában az „az MH hivatásos és szerződéses állományú katonája esetén a Hjt. 2. §-ának (22) bekezdése, más katona tekintetében" szövegrész,

e) 1. § j) pontjában az „az MH hivatásos és szerződéses állományába tartozó katona tekintetében a Hjt. 2. §-ának (28) bekezdésében, más katona vonatkozásában" szövegrész,

f) 8. § (1) és (5) bekezdésében az „a Hjt., illetve" szövegrész.

Szalay-Bobrovniczky Kristóf s. k.,
honvédelmi miniszter

A közigazgatási és területfejlesztési miniszter 1/2025. (I. 31.) KTM rendelete a közigazgatási és területfejlesztési miniszter feladat- és hatáskörét érintően a nemzetbiztonsági ellenőrzés alá eső munkakörök meghatározásáról

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 78. § (1a) bekezdés a) pontjában kapott felhatalmazás alapján, az Alaptörvény 18. cikk (2) bekezdésében meghatározott feladatkörömben eljárva – a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 9. § (1) bekezdés 14. pontjában meghatározott feladatkörében eljáró Miniszterelnöki Kabinetirodát vezető miniszterrel egyetértésben – a következőket rendelem el:

1. § E rendelet alkalmazásában *foglalkoztató szervezet*

a) a Közigazgatási és Területfejlesztési Minisztérium (a továbbiakban: minisztérium),

b) a közigazgatási és területfejlesztési miniszter (a továbbiakban: miniszter) által irányított, illetve felügyelt központi államigazgatási szerv,

c) a fővárosi és vármegyei kormányhivatal,

d) a miniszter által irányított vagy felügyelt, központi államigazgatási szervnek nem minősülő költségvetési szerv.

2. § A foglalkoztató szervezettel a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) szerinti foglalkoztatási jogviszonyban (a továbbiakban: foglalkoztatási jogviszony) vagy a Polgári Törvénykönyv rendelkezésein alapuló szerződéses jogviszonyban álló vagy ilyen jogviszonyt létesíteni szándékozó személyek esetében a 3. §-ban és az 1. mellékletben meghatározott

a) munkakör betöltésére, feladat ellátására irányuló foglalkoztatási jogviszony, illetve

b) feladat ellátására irányuló, a Polgári Törvénykönyv rendelkezésein alapuló szerződéses jogviszony (a továbbiakban: szerződéses jogviszony)

az Nbtv. 74. § i) pont in) alpontja szerinti jogviszonynak minősül.

3. § A foglalkoztató szervezetnél

a) a gazdasági vezető,

b) a belső ellenőr,

c) a biztonsági vezető, a helyettes biztonsági vezető,

d) a nemzetbiztonsági ellenőrzéssel kapcsolatban kijelölt biztonsági megbízott,

e) a titkos ügykezelő, továbbá a minősített adat szállítására kijelölt személyes kézbesítő,

f) az elektronikus információs rendszer biztonságáért felelős személy,
g) a rendszerbiztonsági felügyelő,
h) a rendszer-adminisztrátor,
i) a rejtjelfelügyelő és a rejtjelző

munkakör betöltésére, feladat ellátására irányuló foglalkoztatási jogviszony vagy szerződéses jogviszony az Nbtv. 74. § i) pont in) alpontja szerinti jogviszonynak minősül.

4. § Az 1. § d) pontjában meghatározott foglalkoztató szervezet vezetője és a helyettesítésére jogosult személy munkakörének betöltésére, feladatának ellátására irányuló foglalkoztatási jogviszony vagy szerződéses jogviszony az Nbtv. 74. § i) pont in) alpontja szerinti jogviszonynak minősül.

5. § Ez a rendelet a kihirdetését követő napon lép hatályba.

6. § (1) Az e rendelet hatálybalépésének napján az e rendelet hatálya alá tartozó foglalkoztató szervezetnél munkakört betöltő, kockázatmentes biztonsági szakvéleménnyel nem rendelkező személy nemzetbiztonsági ellenőrzésének megindítása érdekében a munkáltatói jogkör gyakorlója a biztonsági kérdőív kitöltésének megkezdéséhez szükséges intézkedéseket legkésőbb az e rendelet hatálybalépését követő hatvan napon belül teszi meg.

(2) Az e rendelet hatálybalépését megelőzően nemzetbiztonsági ellenőrzés alá esőnek nem minősülő munkakört betöltő személy jogviszonya a nemzetbiztonsági ellenőrzés lefolytatásához szükséges időtartam alatt – a biztonsági szakvélemény elkészültének és a vele való közlésének időtartamáig – érvényes szakvélemény hiányában is fenntartható, a jogviszonyával, munkakörével kapcsolatos feladatait elláthatja.

7. § Hatályát veszti a közigazgatási és területfejlesztési miniszter feladat- és hatáskörét érintően a nemzetbiztonsági ellenőrzés alá eső munkakörök meghatározásáról szóló 2/2024. (III. 5.) KTM rendelet.

Dr. Navracsics Tibor s. k.,
közigazgatási és területfejlesztési miniszter

1. melléklet az 1/2025. (I. 31.) KTM rendelethez

Nemzetbiztonsági ellenőrzés alá eső munkakörök meghatározása

1. A minisztériumban
   1.1. a miniszteri kabinet valamennyi munkaköre,
   1.2. a minisztériumi protokollfeladatok ellátásával kapcsolatos döntés-előkészítésben részt vevő és döntéshozó munkakör,
   1.3. a főigazgató, igazgató,
   1.4. az államtitkárok kabinetjének, illetve titkárságának, a szakmai felsővezetők, főigazgatók, igazgatók, valamint a miniszteri, illetve kormánybiztosok titkárságának valamennyi munkaköre, ide nem értve az irányításuk alá tartozó osztályok munkaköreit,
   1.5. a főosztályvezető, a főosztályvezető helyettesítésére jogosult osztályvezető,
   1.6. a kabinetfőnök, a politikai főtanácsadó, a politikai tanácsadó,
   1.7. a parlamenti államtitkár irányítása alá tartozó szervezeti egységek döntés-előkészítésben részt vevő és döntéshozó munkaköre,
   1.8. a Belső Ellenőrzési és Integritási Igazgatóság szervezeti egységeinek valamennyi munkaköre,
   1.9. a közbeszerzési felügyeletért felelős helyettes államtitkár irányítása alá tartozó szervezeti egységek döntés-előkészítésben részt vevő és döntéshozó munkaköre,
   1.10. a védelmi és biztonsági igazgatási feladat ellátására kijelölt munkakör,
   1.11. a minisztérium jogi képviseletét ellátó szervezeti egységek döntés-előkészítésben részt vevő és döntéshozó munkaköre,
   1.12. a szervezetbiztonsági és információvédelmi feladatokat ellátó valamennyi munkakör,
   1.13. a minősített adat felhasználásával kapcsolatos feladatot ellátó valamennyi munkakör,

1.14. a támogatások kedvezményezettjeivel, a pályázati kérelmek benyújtóival, az ellenőrző szervek által végzett vizsgálatba bevont ügyfelekkel és a pályázati ágazat szereplőivel közvetlen kapcsolatba kerülő, a helyszíni ellenőrzési, illetve előzetes helyszíni szemlét lefolytató feladatokat ellátó szervezeti egységek valamennyi munkaköre.

2. A vármegyei kormányhivatalokban
   2.1. a járási hivatalvezető,
   2.2. az igazgató,
   2.3. a védelmi és biztonsági igazgatási feladatot ellátó, valamint ilyen feladat ellátására kijelölt munkakör.
3. Budapest Főváros Kormányhivatalánál
   3.1. a kerületi hivatalvezető,
   3.2. az igazgató,
   3.3. a védelmi és biztonsági igazgatási feladatot ellátó, valamint ilyen feladat ellátására kijelölt munkakör,
   3.4. az országos illetékességgel eljáró, kereskedelmi, haditechnikai, exportellenőrzési és nemesfémhitelesítési feladatokat ellátó önálló szervezeti egység főosztályvezetője és osztályvezetői,
   3.5. az országos illetékességgel eljáró, honosított és határon túli anyakönyvezéssel kapcsolatos feladatokat ellátó önálló szervezeti egység főosztályvezetője és osztályvezetői,
   3.6. az országos illetékességgel eljáró, közúti és hajózási hatósági feladatokat ellátó önálló szervezeti egység döntés-előkészítésben részt vevő és döntéshozó munkakörei,
   3.7. az országos illetékességgel eljáró, rehabilitációs igazgatási feladatokat ellátó önálló szervezeti egység főosztályvezetője.

VIII. A Kúria határozatai

A Kúria Önkormányzati Tanácsának Köf.5.041/2024/4. számú határozata

Az ügy száma:	Köf.5.041/2024/4.
A tanács tagjai:	Dr. Balogh Zsolt a tanács elnöke, Dr. Kiss Árpád Lajos előadó bíró, Dr. Demjén Péter bíró, Dr. Hajnal Péter bíró, Dr. Kalas Tibor bíró
Az indítványozó:	Kúria
Az érintett önkormányzat:	Muraszemenye Község Önkormányzata
Az érintett önkormányzat képviselője:	Dr. Belső Béla Krisztián egyéni ügyvéd (…)
Az ügy tárgya:	önkormányzati rendelet más jogszabályba ütközésének vizsgálata

Rendelkező rész

A Kúria Önkormányzati Tanácsa

– megállapítja, hogy Muraszemenye Község Önkormányzat képviselő-testületének a helyi építési szabályzatról szóló 10/2007. (XII.14.) önkormányzati rendeletének 4. § (3) bekezdésének b) pontja, 11. § (1) bekezdésének b) pontja és 11. § (4) bekezdésének c) pontja és a hozzájuk tartozó, a rendelet mellékletét képező szabályozási terv térképi része más jogszabályba ütközött;
– megállapítja, hogy e rendelkezés nem alkalmazható Kúria előtt folyó Kfv.VI.37.260/2024/5. számú perben;
– elrendeli határozatának közzétételét a Magyar Közlönyben;
– elrendeli, hogy a határozat közzétételére – a Magyar Közlönyben való közzétételt követő 8 napon belül – az önkormányzati rendelet kihirdetésével azonos módon kerüljön sor.

A határozat ellen jogorvoslatnak nincs helye.

Indokolás

Az indítvány alapjául szolgáló tényállás

[1] A Kúria mint felülvizsgálati bíróság (a továbbiakban: indítványozó bíróság) előtt Kfv.VI.37.260/2024/5. szám alatt folyamatban lévő közigazgatási per irányadó tényállása szerint az alperes 2022. december 5. napján előzetes értesítést követően helyszíni ellenőrzést tartott a felperes … 0175/5, 0176/6, 0176/7, 0176/8 és 0176/9 hrsz-ú ingatlanain az ott végzett építési tevékenységek szabályosságának vizsgálata tárgyában. Ennek eredményeként a 2023. március 14-én kelt ZA/ETDR/406-8/2023. iktatószámú határozatával (a továbbiakban: alperesi határozat) a felperest az építmények alapszerkezeteinek szabályossá tételére kötelezte. A határozatát az épített környezet alakításáról és védelméről szóló 1997. évi LXXVIII. törvény (a továbbiakban: Étv.) és az építésügyi és építésfelügyeleti hatósági eljárásokról és ellenőrzésekről, valamint az építésügyi hatósági szolgáltatásról szóló 312/2012. (XI. 8.) Korm.rendelet (a továbbiakban: R.) mellett a Muraszemenye Község Önkormányzata Képviselő-testületének 10/2007. (XII.14.) önkormányzati rendelettel elfogadott helyi építési szabályzatának (továbbiakban: HÉSZ) 8. § (1), (21) bekezdés, 11. § (1) bekezdés b) pont, 11. § (4) bekezdés c) pont, 11. § (6) bekezdés a) és b) pont előírásaira alapította.

[2] Az alperesi határozat indokolása szerint az ingatlanokon található épületek kialakításuk tekintetében emberi tartózkodásra szolgálnak, villany közműbekötéssel is rendelkeznek, ezért építési engedély birtokában lettek volna megépíthetők.

[3] Az alperesi határozattal szemben a felperes keresettel élt, melyben többek között arra is hivatkozott, hogy álláspontja szerint a HÉSZ 4. §-a és 11. §-ának rendelkezése ellentétes a jogszabályi hierarchiában magasabb szintű Étv. 2. § 13. pontjával és az országos településrendezési és építési követelményekről szóló 253/1997. (XII. 20.)

Korm. rendelet (a továbbiakban: OTÉK) 27. §-ával, arra a lényeges körülményre tekintettel, hogy a HÉSZ kifejezetten magántulajdonban álló területen kíván közterületi célokat megvalósítani, illetve magánterületet sorol a nyilvánvalóan közterületi célokat betöltő építési övezetbe.

[4] Az elsőfokú bíróság ítéletével a keresetet elutasította. Az ügy anyagi jogi tárgyát illetően rögzítette, hogy a felek között nem volt vitatott a HÉSZ egyes ingatlanokra vonatkozó övezeti besorolása, valamint a felperes maga sem vonta kétségbe, hogy szabálytalanul, építési engedély nélkül végzett építési tevékenységet. Alaptalannak értékelte ugyanakkor azt a felperesi álláspontot, miszerint a HÉSZ vonatkozó szabályozása ellentétes az OTÉK-kal, mint a jogszabályi hierarchiában magasabb szintű jogszabállyal, arra a körülményre tekintettel, hogy a HÉSZ kifejezetten magántulajdonban álló területen kíván közterületi célokat megvalósítani, illetve magánterületet sorol a nyilvánvalóan közterületi célokat betöltő építési övezetbe.

[5] Az elsőfokú bírósági döntéssel szemben a felperes felülvizsgálati kérelmet terjesztett elő, arra hivatkozással, hogy az alperesi hatóságnak az eljárás során hivatalból észlelnie kellett volna, hogy a határozatának alapját képező HÉSZ ütközik a határozat másik alapját képező, magasabb szintű jogszabállyal (az OTÉK-kal), és ezen lényeges körülmény észlelésére tekintettel az alperesi hatóságnak az önkormányzati rendelet más jogszabályba ütközésének vizsgálatára irányuló eljárást kellett volna kezdeményeznie a saját eljárásának egyidejű felfüggesztése mellett.

Az indítvány és az Önkormányzat védirata

[6] Az indítványozó bíróság a 2024. július 4. napján kelt Kfv.VI.37.260/2024/5. számú végzésében a közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.) 144. §-a alapján az Önkormányzati Tanács eljárását kezdeményezte és egyidejűleg a per tárgyalását felfüggesztette. A bírói indítvány szerint a HÉSZ 4. § (3) bekezdésének b) pontja, 11. § (1) bekezdésének b) pontja és 11. § (4) bekezdésének c) pontja és a hozzájuk tartozó, a rendelet mellékletét képező szabályozási terv térképi része magasabb szintű jogszabályba ütközik.

[7] Az indítványozó bíróság szerint közparkként való besorolás csak közterület esetében lehetséges, a közterület pedig nem állhat az ingatlan-nyilvántartás szerint magántulajdonban. A perbeli ingatlanok a „Zkp1 övezetben" nem vitatottan magántulajdonban állnak. A HÉSZ-nek az ezt figyelembe nem vevő szabályozása az Étv. 2. § 13. pontjával, az OTÉK 27. §-ával, 6. § (3) bekezdésével és 1. számú mellékletének 71. pontjával ellentétes. A Zöldterület – közpark (Zkp1) övezetnek az OTÉK 1. számú melléklet 71. pontja értelmében közparkként közterületnek kellene lennie. Az OTÉK 6. § (3) bekezdésének meghatározása szerint egy település igazgatási területének a beépítésre nem szánt területe annak általános használata szerinti zöldterület esetében lehet az e bekezdésben szereplő 5. pontnak megfelelő közpark, illetve 6. pontnak megfelelő közkert. Az OTÉK 27. § (1) bekezdés rendelkezése alapján a földterület állandóan növényzettel fedett közterület, amely a település klimatikus viszonyainak megőrzését, javítását, ökológiai rendszerének védelmét, a pihenést és testedzést szolgálja. A zöldterület általános használata szerint közpark vagy közkert.

[8] Álláspontja szerint a helyi építési szabályzatban az önkormányzatnak a telkekhez fűződő sajátos helyi követelményeket, jogokat és kötelezettségeket az Étv. 13. § (1) bekezdésében foglaltak szerint az országos szabályoknak megfelelően, illetve az azokban megengedett eltérésekkel kell megállapítania. A perbeli ingatlan az ingatlan-nyilvántartás szerint nem közterület, ezért annak közparkként való minősítése ellentétes a magasabb szintű jogszabályok, az Étv. és az OTÉK hivatkozott rendelkezéseivel, ezáltal sérti az Alaptörvény idézett 32. cikk (3) bekezdését is.

[9] Az indítványozó bíróság a helyi szabályozás önellentmondásosságára is hivatkozott. Érvelése szerint a zöldterületi szabályozása körében a 11. § (6) bekezdés a) és b) pont alapján a (4) bekezdés c) pontjában szereplő zöldterületeken az OTÉK vonatkozó előírásának szigorításával csak a pihenést szolgáló építmény (sétaút, pihenőhely stb.) és az e) pont szerint a terület fenntartásához szükséges épület helyezhető el. Az ügy idején hatályos HÉSZ-nek az OTÉK vonatkozó előírásainak szigorításával rögzített megállapítása szerint az épület a zöldterület teljes területének 0,5%-os beépítésével lehetséges, az építménymagasság legfeljebb 3,50 méter. Ezzel ellentétben a HÉSZ üdülőterületi szabályozása más építési szabályokat rögzít. A HÉSZ 8. § (21) bekezdése a hétvégi házas üdülőövezetben (Üh3) az üdülőépületek elhelyezésére vonatkozó építési előírások cím alatt rögzíti, hogy az üdülőépületek elhelyezésére szolgáló kialakult, vagy újonnan kialakított építési telken:

a) a telek beépítettségének mértéke 10%, de legfeljebb 55 m^2 lehet. Egy épület létesíthető.

f) az OTÉK alapján számított építménymagasság legfeljebb 5,00 méter lehet.

g) az épületet 2,00 méter magas pillérekre („lábakra") kell állítani.

[10] Ebből kifolyólag az indítványozó bíróság szerint a HÉSZ vitatott rendelkezései ellentétesek a jogalkotásról szóló 2010. évi CXXX. törvény (a továbbiakban: Jat.) 2. § (1) bekezdésében kimondott normavilágosság követelményével, miszerint a jogszabálynak a címzettek számára egyértelműen értelmezhető szabályozási tartalommal kell rendelkeznie.

[11] Mindezekre tekintettel az indítványozó bíróság szerint a HÉSZ vitatott rendelkezései az Alaptörvény 32. cikk (3) bekezdésébe, a Jat. 2. § (1) bekezdésébe, az Étv. 2. § 13. pontjába, valamint az OTÉK 6. § (3) bekezdésébe, 27. § (1) bekezdésébe, 111. § (1) és (2) bekezdésébe és az 1. számú Melléklete 71. pontjába ütközik és kérte azok „törvényellenessége megállapítását".

[12] Az Önkormányzati Tanács a Kp. 140. § (1) bekezdése szerint alkalmazandó 42. § (1) bekezdése alapján az érintett önkormányzatot felhívta az indítványra vonatkozó nyilatkozata megtételére.

[13] Az Önkormányzat védiratot nem terjesztett elő, ugyanakkor 2024. november 21. napján kelt nyilatkozatában kifejtette, hogy a képviselő-testület a 114/2024. (X.8.) számú határozatával új településterv készítésről döntött. Előadta, hogy a HÉSZ módosítása és azzal összefüggő előkészületek folyamatban vannak.

[14] Időközben – a Nemzeti Jogszabálytár adatai szerint – Muraszemenye Község Önkormányzata Képviselő-testülete elfogadta a helyi építési szabályzatról szóló 14/2024. (XII. 16.) önkormányzati rendeletét (a továbbiakban: új HÉSZ), mely 2025. január 1. napján lépett hatályba. Egyúttal a HÉSZ-t az új HÉSZ 41. §-a 2025. január 1. napjával hatályon kívül helyezte.

Az Önkormányzati Tanács döntésének indokai

[15] Az indítvány az alábbiak szerint megalapozott.

[16] A Kúria Önkormányzati Tanácsának a bírói indítványban foglaltak alapján abban a kérdésben kellett állást foglalnia, hogy a HÉSZ szabályozása magasabb jogszabályba ütközik-e.

[17] A Kúria Önkormányzati Tanácsa több korábbi határozatában rögzítette, hogy az Önkormányzati Tanács bírói kezdeményezés esetén azt a jogot vizsgálja, amelyet a bírónak alkalmaznia kell. Így kerülhet sor hatályon kívül helyezett, vagy a későbbiekben módosult önkormányzati rendeletek vizsgálatára (Köf.5012/2016/4., Köf.5083/2012/4., Köf.5024/2019/4. sz. határozatok).

[18] Jelen ügyben megállapítható, hogy az alperesi határozat 2023. március 14. napján kelt, így a Kp. 85. § (2) bekezdése alapján az Önkormányzati Tanácsnak ezt az időállapotot kellett vizsgálnia.

[19] A Kp. 144. §-a és a 146. § (1) bekezdés b) pontja bírói indítvány alapján lehetővé teszi a már nem hatályos önkormányzati rendelet egyes, az indítványozó bíróság által alkalmazandó rendelkezéseinek a felülvizsgálatát.

[20] A HÉSZ indítvánnyal érintett, alkalmazandó, 2024. december 31. napjáig hatályos szövegének releváns részei a következők:

„4. § Beépítésre szánt és beépítésre nem szánt területek, terület felhasználási egységek

(1) A Tervben Muraszemenye község közigazgatási területe beépítésre szánt és beépítésre nem szánt területekre oszlik.

(2) A beépítésre szánt területek az alábbi, az OTÉK-ban szereplő terület felhasználási módokra, területegységekre oszlanak:

a) falusias lakóterület;

b) településközpont vegyes terület;

c) kereskedelmi, szolgáltató gazdasági terület;

d) 3 üdülőházas üdülőterület, hétvégi házas üdülőterület;

e) különleges terület.

(3) A beépítésre nem szánt területek, a Tervben ábrázolt módon az alábbi, az OTÉK szerinti, terület felhasználási egységekre oszlanak:

b) zöldterület;

11. § Zöldterület (Z…)

(1) A községben a zöldterület területfelhasználási módú terület a Tervben jelölt határok szerint négy övezetre oszlik:

b) zöldterület – közpark (Zkp1);

(4) A Zöldterület – közpark (Zkp1) övezetbe sorolódnak a község Tervben lehatárolt részei:

a) a községháza melletti terület;

b) a temető melletti terület;

c) az üdülőterületen, a tópartok menti zöldsávok."

[21] Az Alaptörvény 32. cikk (1)–(2) bekezdése „a helyi közügyek intézése körében törvény keretei között" hatalmazza fel a helyi önkormányzatokat rendeletalkotásra. E rendelkezés szerint „[f]eladatkörében eljárva a helyi önkormányzat törvény által nem szabályozott helyi társadalmi viszonyok rendezésére, illetve a törvényben kapott felhatalmazás alapján önkormányzati rendeletet alkot". A 32. cikk (3) bekezdése kimondja, hogy „az önkormányzati rendelet más jogszabállyal nem lehet ellentétes."

[22] Az Étv. 2. § 13. pontja értelmében a közterület a közhasználatra szolgáló minden olyan állami vagy önkormányzati tulajdonban álló földterület, amelyet az ingatlan-nyilvántartás ekként tart nyilván.

[23] Az Étv. 2. §-ának 2. és 3. pontja megkülönbözteti a beépítésre szánt és a beépítésre nem szánt területeket. Eszerint „Beépítésre nem szánt terület: a település közigazgatási területének a zöldterületi, a közlekedési, a mezőgazdasági, az erdőművelési, illetve az egyéb célra szolgáló része."„Beépítésre szánt terület: a település közigazgatási területének a beépített, illetve a további beépítés céljára szolgáló területrésze." A település zöldterületi része így beépítésre nem szánt területnek minősül.

[24] A Kúria Önkormányzati Tanácsa a korábbi közzétett gyakorlata alapján rámutat arra, hogy az OTÉK rendszerével ellentétes az olyan helyi alövezeti besorolás, mely alövezeti kategória egy beépítésre szánt építési övezetet egyesít egy beépítésre nem szánt övezettel. A Köf.5.017/2020/4. számú határozat szerint „az igazgatási terület területfelhasználási egysége csakis »beépítésre szánt« vagy »beépítésre nem szánt« kategóriába tartozhat, azaz nem létezik e két átfogó területi kategóriának közös metszete". Az Étv. és az OTÉK rendszerében az övezetek alapvetően elkülönülnek aszerint, hogy azokat a helyi építési szabályzat beépítésre szánja-e. Ezen övezetek között az átjárás, az egyes kategóriák keresztezése nem lehetséges. Az, hogy egy terület beépítésre nem szánt területnek minősül nem jelenti egyben azt is, hogy az adott területen építési tilalom is fennállna. Az OTÉK 6. § (1) bekezdés b) pontja ugyanis a beépítésre nem szánt területen a beépítést általánosságban lehetővé teszi, az Étv. 20. §-a pedig az építési tilalmat „az érintett területre" teszi elrendelhetővé. {Köf.5.017/2020/4. határozat [23] és [24] bekezdései}

[25] Az OTÉK. 27. § (1) bekezdése szerint a zöldterület állandóan növényzettel fedett közterület, amely a település klimatikus viszonyainak megőrzését, javítását, ökológiai rendszerének védelmét, a pihenést és testedzést szolgálja. A zöldterület általános használata szerint közpark vagy közkert.

[26] Az indítvány helytállóan mutatott rá, hogy a zöldterület fogalmi eleme a közterületi jelleg, miközben az alapperben nem volt vitatott, hogy az érintett, zöldterületnek minősített ingatlanok nem minősültek közterületnek. Az ilyen ingatlanok zöldterületté minősítése ellentétes az OTÉK 27. § (1) bekezdésével, valamint az Étv. 2. § 13. pontjában foglaltakkal {Köf.5.017/2020/4. határozat [19] és [20] bekezdései}.

[27] A Jat. 2. § (1) bekezdésének értelmében a jogszabálynak a címzettek számára egyértelműen értelmezhető szabályozási tartalommal kell rendelkeznie.

[28] A Kúria Önkormányzati Tanácsa megállapította, hogy az indítvánnyal támadott rendelkezések „üdülőterület" fogalma nem meghatározható. A HÉSZ 8. § „hétvégiházas üdülőterület"-ről rendelkezik, de az beépítésre szánt övezetnek minősül, így a kifejtettek szerint nem lehet beépítésre nem szánt terület is egyben. Más meghatározást a HÉSZ egyáltalán nem tartalmaz. Ehhez hasonlóan a „zöldsáv" fogalmát sem a HÉSZ, sem az Étv., sem az OTÉK nem rendezi. Mindezen rendelkezésekben tetten érhető a normavilágosság sérelme, nem állapítható meg ugyanis egyértelműen, hogy az adott rendelkezés beépítésre szánt, vagy nem szánt területre, azon belül milyen jellegű területre vonatkozik.

[29] A fentiekre tekintettel a Kúria Önkormányzati Tanácsa a Kp. 146. § (1) bekezdés b) pontja alapján megállapította, hogy a HÉSZ. 2024. december 31-ig hatályban volt 4. § (3) bekezdésének b) pontja, 11. § (1) bekezdésének b) pontja és 11. § (4) bekezdésének c) pontja és a hozzájuk tartozó, a rendelet mellékletét képező szabályozási terv térképi része más jogszabályba ütközött, azok egyrészt magántulajdonban álló területre állapítottak meg közterületi jellegű szabályozást, továbbá az egyes hivatkozott fogalmak tekintetében a címzettek számára egyértelműen értelmezhető tartalommal nem rendelkeztek.

[30] A HÉSZ hatályon kívül helyezése folytán annak általános időbeli hatálya megszűnt, így a Kúria Önkormányzati Tanácsa általi megsemmisítésre már nincs lehetőség, de az adott jogvitában való alkalmazási tilalma kimondható. (Köf.5.017/2018/3.) A Kúria Önkormányzati Tanácsa a fentiek alapján a rendelkező részben foglaltak szerint megállapította a támadott rendelkezések más jogszabályba ütközését ezért annak rendelkezései – a Kp. 147. § (1) és (2) bekezdés alkalmazásával – az indítvány alapjául szolgáló perben nem alkalmazhatók. A Kúria az általános alkalmazási tilalom elrendelését – figyelemmel az indítványozó bíróság előtt fekvő ügy egyedi sajátosságaira – a közérdek védelme érdekében mellőzte.

[31] A Kúria Önkormányzati Tanácsa megjegyzi, hogy jelen döntése nem érinthette azt az alapperben vitatott körülményt, hogy az érintett építmények építési engedély nélkül létesíthetők voltak-e, figyelemmel arra, hogy az alperesi határozat az engedély beszerzésének kötelezettségét nem a normakontroll eljárással érintett rendelkezésekre alapította, így erről a körülményről az indítványozó bíróság jogosult állást foglalni.

A döntés elvi tartalma

[32] I. A zöldterület fogalmi eleme a közterületi jelleg. A közterület magántulajdonban álló területen nem állhat fenn, ezért a magántulajdonban álló ingatlan nem minősíthető zöldterületnek.

II. A címzettek számára nem egyértelműen meghatározható tartalmú norma sérti a normavilágosság követelményét.

Záró rész

[33] A Kúria Önkormányzati Tanácsa az indítványt a Kp. 141. § (2) bekezdése szerint tárgyaláson kívül bírálta el.

[34] A Kúria a törvényellenesség jogkövetkezményeit a Kp. 146. § (1) bekezdés b) pontja alapján állapította meg.

[35] A Magyar Közlönyben történő közzététel a Kp. 146. § (2) bekezdésén, a helyben történő közzététel a Kp. 142. § (3) bekezdésén alapul.

[36] A megsemmisített rendelkezésnek a folyamatban lévő ügyben és általános alkalmazási tilalmát a Kp. 147. § (1) bekezdése mondja ki.

[37] Jelen eljárásban a Kp. 141. § (4) bekezdése alapján a feleket teljes költségmentesség illeti meg és saját költségeiket maguk viselik.

[38] A határozat elleni jogorvoslatot a Kp. 116. § d) pontja és a 146. § (5) bekezdése zárja ki.

Budapest, 2025. január 21.

Dr. Balogh Zsolt s. k.,
a tanács elnöke

Dr. Kiss Árpád Lajos s. k.,
előadó bíró

Dr. Demjén Péter s. k.,
bíró

Dr. Hajnal Péter s. k.,
bíró

Dr. Kalas Tibor s. k.,
bíró

IX. Határozatok Tára

A köztársasági elnök 3/2025. (I. 31.) KE határozata állami kitüntetés adományozásáról

Az Alaptörvény 9. cikk (4) bekezdés f) pontja, illetve a Magyarország címerének és zászlajának használatáról, valamint állami kitüntetéseiről szóló 2011. évi CCII. törvény 17. §-a és 18. § (1) bekezdése alapján – a miniszterelnök előterjesztésére –

Oleg Ţulea, a Moldovai Köztársaság magyarországi rendkívüli és meghatalmazott nagykövete részére a magyar–moldáv kapcsolatok előmozdítása érdekében végzett tevékenysége elismeréseként

a MAGYAR ÉRDEMREND
parancsnoki keresztje
polgári tagozat

kitüntetést adományozom.

Budapest, 2025. január 23.

Dr. Sulyok Tamás s. k.,
köztársasági elnök

Ellenjegyzem:

Budapest, 2025. január 24.

Orbán Viktor s. k.,
miniszterelnök

SP ügyszám: SP/465-3/2025

A köztársasági elnök 4/2025. (I. 31.) KE határozata közigazgatási államtitkár felmentéséről és közigazgatási államtitkár kinevezéséről

1. Az Alaptörvény 9. cikk (4) bekezdés j) pontja, valamint a kormányzati igazgatásról szóló 2018. évi CXXV. törvény 233. § (1) bekezdése alapján – a miniszterelnök javaslatára – *dr. Bíró Attilát,* az Igazságügyi Minisztérium közigazgatási államtitkárát e tisztségéből 2025. január 31-ei hatállyal felmentem.

2. Az Alaptörvény 9. cikk (4) bekezdés j) pontja, valamint a kormányzati igazgatásról szóló 2018. évi CXXV. törvény 229. § (1) bekezdése alapján – a miniszterelnök javaslatára – *dr. Pilz Tamást* 2025. február 1-jei hatállyal az Igazságügyi Minisztérium közigazgatási államtitkárává kinevezem.

Budapest, 2025. január 30.

Dr. Sulyok Tamás s. k.,
köztársasági elnök

Ellenjegyzem:

Budapest, 2025. január 31.

Orbán Viktor s. k.,
miniszterelnök

SP ügyszám: SP/544-2/2025

A köztársasági elnök 5/2025. (I. 31.) KE határozata bírák kinevezéséről

Az Alaptörvény 9. cikk (3) bekezdés k) pontja és 26. cikk (2) bekezdése, valamint a bírák jogállásáról és javadalmazásáról szóló 2011. évi CLXII. törvény 3. § (2) bekezdése és 23. § (1) bekezdése alapján – az Országos Bírósági Hivatal elnökének javaslatára –

Balláné dr. Illés Ivettet,
dr. Kámán Petrát,
dr. Kollárné dr. Varga Beátát,
dr. Németh-Egry Emőkét és
dr. Wayda Gertrúdot

a 2025. február 1. napjától 2028. január 31. napjáig terjedő időtartamra bíróvá kinevezem.

Budapest, 2025. január 28.

Dr. Sulyok Tamás s. k.,
köztársasági elnök

SP ügyszám: SP/406-2/2025

A köztársasági elnök 6/2025. (I. 31.) KE határozata egyetemi tanárok kinevezéséről

Az Alaptörvény 9. cikk (4) bekezdés c) pontja alapján – a kultúráért és innovációért felelős miniszternek a fenntartóval egyetértésben tett javaslatára –

Dr. Bachmann Erzsébetet,
Balogh Zoltánt,
Dr. Bányainé Dr. Tóth Ágota Anikót,
Dr. Bessenyei Mihályt,
Dr. Bodnár Istvánt,
Dr. Choi In Sut,
Dr. Csiky Botond Szabolcsot,
Dr. Csiszárik-Kocsir Ágnes Terézt,
Dr. Egedy Tamást,
Dr. Faludi Rékát,
Dr. Ferenci Tamást,
Gálné Dr. Remenyik Judit Juliannát,
Dr. Garai-Fodor Mónikát,
Dr. Gáspár Marcell Gyulát,
Győriványi György Sándort,
Hegyi Csabát,
Dr. Jancsó Tamást,
Dr. Juhász Lajos Ferencet,
Dr. Kálmán Anikót,
Dr. Kovács Tünde Annát,
Dr. Kvell Krisztiánt,
Dr. Laufer Editet,
Dr. Lábadi Beatrixet,
Láng Andrást,
Lengyel Péter Jánost,
Dr. Lengyel Szabolcs Lászlót,
Dr. Lukács András Szilárdot,
Dr. Máté Domiciánt,
Dr. Meskó Norbertet,
Dr. Nagy Andrást,
Dr. Nagy Szabolcsot,
Dr. Oross Veronikát,
Dr. Pál Ágnes Máriát,
Dr. Pirkhoffer Ervin Balázst,
Dr. Prokisch Józsefet,
Dr. Rácz Ervint,
Dr. Rétfalvi Donátot,
Simon John Thompsont,
Dr. Szabados Esztert,
Szabó Tündét,
Szente-Varga Mónikát,
Dr. Szepes Zoltán Gábort,
Dr. Szereday Lászlót,
Szitka Rudolfot,
Dr. Varga Zoltán Bélát,
Dr. Vámossy Zoltán Imrét és
Dr. Zajzon Norbertet

2025. február 1. napjával egyetemi tanárrá kinevezem.

Budapest, 2025. január 13.

Dr. Sulyok Tamás s. k.,
köztársasági elnök

Ellenjegyzem:

Budapest, 2025. január 22.

Dr. Hankó Balázs Zoltán s. k.,
kultúráért és innovációért felelős miniszter

SP ügyszám: SP/127-2/2025

A Kormány 1008/2025. (I. 31.) Korm. határozata
a Nemzet Sportolóinak javaslata alapján a Nemzet Sportolója cím adományozásáról

A Kormány a sportról szóló 2004. évi I. törvény 62. § (1) bekezdése alapján – megismerve és tudomásul véve a Nemzet Sportolóinak javaslatát – *Sákovicsné Dömölky Lídia* tőrvívó részére a Nemzet Sportolója címet és az azzal járó életjáradékot adományozza.

Orbán Viktor s. k.,
miniszterelnök

A Kormány 1009/2025. (I. 31.) Korm. határozata
az Emberi Jogok Európai Bírósága magyar bírójelöltjeinek kiválasztási rendjéről

A Kormány egyetért azzal, hogy az Emberi Jogok Európai Bírósága magyar bírójelölti listáján szereplő jelöltek nyilvános pályázat kiírását követően kerüljenek kiválasztásra. A Kormány felhívja az igazságügyi minisztert a pályázati eljárás előkészítéséhez szükséges intézkedések megtételére és a pályázat lefolytatására.

Felelős: igazságügyi miniszter
Határidő: 2025. április 15.

Orbán Viktor s. k.,
miniszterelnök

A Kormány 1010/2025. (I. 31.) Korm. határozata az ENSZ Gyermekalapja budapesti Globális Szolgáltató Központjának negyedik ütemű bővítéséről

A Kormány

1. egyetért az ENSZ Gyermekalapja Budapesten működő Globális Szolgáltató Központjának (a továbbiakban: UNICEF Központ) negyedik ütemű bővítésének a 2027. évtől való megvalósításával;
2. felhívja a nemzetgazdasági minisztert, hogy az UNICEF Központ negyedik ütemű bővítéséig az UNICEF Központ egyes szervezeti egységeinek átmeneti elhelyezéséről a Közbeszerzési és Ellátási Főigazgatóság (a továbbiakban: KEF) útján gondoskodjon;

   Felelős: nemzetgazdasági miniszter
   Határidő: folyamatos
3. felhívja a nemzetgazdasági minisztert, hogy az UNICEF Központ negyedik ütemű bővítésére vonatkozó megállapodásnak megfelelően a KEF útján gondoskodjon az UNICEF Központjának negyedik ütemű bővítésével összefüggésben kiválasztott ingatlan rendeltetésszerű használatának biztosítása érdekében szükséges építészeti, átalakítási, bútorozási tevékenység elvégzéséről;

   Felelős: nemzetgazdasági miniszter
   Határidő: folyamatos
4. felhívja a nemzetgazdasági minisztert, hogy a 2027. évtől kezdődően gondoskodjon az UNICEF Központjának negyedik ütemű bővítésével összefüggésben a KEF útján – a megkötésre kerülő megállapodás tartalma és időbeli hatálya szerint – a kiválasztott ingatlan bérletéről és folyamatos üzemeltetéséről.

   Felelős: nemzetgazdasági miniszter
   Határidő: a 2027. évtől kezdődően folyamatos

Orbán Viktor s. k.,
miniszterelnök

A Kormány 1011/2025. (I. 31.) Korm. határozata a Magyarország egyes területei közötti gazdasági egyenlőtlenség csökkentése érdekében szükséges fejlesztési programot koordináló szervezet működtetéséről

A Kormány

1. egyetért a Kedvezményezett Települések Gazdaságélénkítő Programja további, helyi szintű működtetésével és az ehhez szükséges projektkoordinátori személyi állománynak a 2025. évben a – Magyar Nemzeti Társadalmi Felzárkózási Stratégiával összhangban a társadalmi felzárkózás képzési, szervezési, területi módszertani és kutatási feladatait ellátó, fejlesztési programot koordináló – Társadalmi Esélyteremtési Főigazgatóságon történő foglalkoztatásával;
2. az államháztartásról szóló 2011. évi CXCV. törvény (a továbbiakban: Áht.) 33. § (2) bekezdésében biztosított jogkörében eljárva, az államháztartásról szóló törvény végrehajtásáról szóló 368/2011. (XII. 31.) Korm. rendelet 34. § (2) bekezdés b) pontja alapján – az 1. pontban meghatározott cél megvalósítása érdekében – felhívja a nemzetgazdasági minisztert, hogy a Magyarország 2025. évi központi költségvetéséről szóló 2024. évi XC. törvény (a továbbiakban: Kvtv.) 1. melléklet LXIII. Nemzeti Foglalkoztatási Alap fejezet, 6. Start-munkaprogram cím előirányzatról utaljon át 219 000 000 forintot a Kvtv. 1. melléklet XIV. Belügyminisztérium fejezet, 16. Társadalmi Esélyteremtési Főigazgatóság cím javára;

   Felelős: nemzetgazdasági miniszter
   Határidő: 2025. január 31.
3. az Áht. 36. § (4c) bekezdés a) pontjában biztosított jogkörében eljárva a 2025. évben a Kvtv. 1. melléklet XIV. Belügyminisztérium fejezet, 16. Társadalmi Esélyteremtési Főigazgatóság cím terhére vállalható kötelezettségek mértékét 219 000 000 forint összegben állapítja meg;

4. tudomásul veszi, hogy a 2. pontban biztosított támogatásból 173 100 000 forint a Kvtv. 1. melléklet XIV. Belügyminisztérium fejezet, 16. Társadalmi Esélyteremtési Főigazgatóság cím 2025. évi személyi juttatása eredeti költségvetési kiadási előirányzatának növelésére irányul.

Orbán Viktor s. k.,
miniszterelnök

A Kormány 1012/2025. (I. 31.) Korm. határozata
a rendkívüli kormányzati intézkedésekre szolgáló tartalékból történő és fejezetek közötti előirányzat-átcsoportosításról

A Kormány

1. az államháztartásról szóló 2011. évi CXCV. törvény (a továbbiakban: Áht.) 21. § (1) bekezdésében és 33. § (2) bekezdésében biztosított jogkörében eljárva 4 002 400 000 forint egyszeri átcsoportosítását rendeli el elszámolási, a fel nem használt rész tekintetében visszatérítési kötelezettséggel a Magyarország 2025. évi központi költségvetéséről szóló 2024. évi XC. törvény 1. melléklet XLII. A költségvetés közvetlen bevételei és kiadásai fejezet, 46. Központi tartalékok cím, 3. Rendkívüli kormányzati intézkedések alcím terhére, az 1. melléklet szerint;
   Az átcsoportosítás tekintetében
   Felelős: nemzetgazdasági miniszter
   Határidő: azonnal
   Az elszámolás és a visszatérítési kötelezettség tekintetében
   Felelős: a miniszterelnök általános helyettese
   Határidő: 2025. december 31.
2. az Áht. 33. § (2) bekezdésében biztosított jogkörében eljárva 30 000 000 forint egyszeri átcsoportosítását rendeli el, a 2. melléklet szerint.
   Felelős: nemzetgazdasági miniszter
   Határidő: azonnal

Orbán Viktor s. k.,
miniszterelnök

1. melléklet az 1012/2025. (I. 31.) Korm. határozathoz

XLII. A költségvetés közvetlen bevételei és kiadásai
LXV. Bethlen Gábor Alap

ADATLAP A KÖLTSÉGVETÉSI ELŐIRÁNYZATOK MÓDOSÍTÁSÁRA
Költségvetési év: 2025.

forintban

Államház-tartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	KIADÁSOK Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/határozat száma
	XLII.						A költségvetés közvetlen bevételei és kiadásai									
		42						Alapok támogatása								
263478			2						Bethlen Gábor Alap támogatása							
						K5						Egyéb működési célú kiadások		2 400 000		
						K8						Egyéb felhalmozási célú kiadások		4 000 000 000		
		46						Központi tartalékok								
297102			3						Rendkívüli kormányzati intézkedések							
						K5						Egyéb működési célú kiadások		-4 002 400 000		
	LXV.						Bethlen Gábor Alap									
263145		4						Nemzetpolitikai célú támogatások								
						K8						Egyéb felhalmozási célú kiadások		4 000 000 000		
379839		5						Működtetési célú kifizetések								
						K3						Dologi kiadások		2 400 000		
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																

forintban

Államház-tartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	BEVÉTEL Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/határozat száma
	LXV.						Bethlen Gábor Alap									
		2						Költségvetési támogatás								
284901			3						Eseti támogatás							
						B1						Működési célú támogatások államháztartáson belülről		2 400 000		
						B2						Felhalmozási célú támogatások államháztartáson belülről		4 000 000 000		
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																

forintban

Államház-tartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	TÁMOGATÁS Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/határozat száma
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																
												Foglalkoztatottak létszáma (fő) - időszakra				

Az adatlap 1 eredeti példányban töltendő ki	A támogatás folyósítása/zárolása (módosítása +/-)	Összesen		I. n.év	II. n.év	III. n.év	IV. n.év
Magyar Államkincstár 1 példány	időarányos teljesítésarányos egyéb: azonnal	4 002 400 000		4 002 400 000			

* Az összetartozó előirányzat-változásokat (+/-) egymást követően kell szerepeltetni.

2. melléklet az 1012/2025. (I. 31.) Korm. határozathoz

III. Alkotmánybíróság
XI. Miniszterelnökség

ADATLAP A KÖLTSÉGVETÉSI ELŐIRÁNYZATOK MÓDOSÍTÁSÁRA
Költségvetési év: 2025.

forintban

Államház-tartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	KIADÁSOK Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/határozat száma
	III.						Alkotmánybíróság									
000385		1						Alkotmánybíróság								
						K3						Dologi kiadások		30 000 000		
	XI.						Miniszterelnökség									
		30						Fejezeti kezelésű előirányzatok								
296668			2						Fejezeti általános tartalék							
						K5						Egyéb működési célú kiadások		-30 000 000		
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																

forintban

Államház-tartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	BEVÉTEL Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/határozat száma
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																

forintban

Államház-tartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	TÁMOGATÁS Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/határozat száma
	III.						Alkotmánybíróság									
000385		1						Alkotmánybíróság						30 000 000		
	XI.						Miniszterelnökség									
		30						Fejezeti kezelésű előirányzatok								
296668			2						Fejezeti általános tartalék					-30 000 000		
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																
												Foglalkoztatottak létszáma (fő) - időszakra				

Az adatlap 1 eredeti példányban töltendő ki	A támogatás folyósítása/zárolása (módosítása +/-)	Összesen		I. n.év	II. n.év	III. n.év	IV. n.év
Magyar Államkincstár 1 példány	időarányos teljesítésarányos egyéb: azonnal	30 000 000		30 000 000			

* Az összetartozó előirányzat-változásokat (+/-) egymást követően kell szerepeltetni.

A Kormány 1013/2025. (I. 31.) Korm. határozata egyes helyi önkormányzatok támogatásáról

A Kormány

1. az államháztartásról szóló 2011. évi CXCV. törvény (a továbbiakban: Áht.) 33. § (1) bekezdésében biztosított jogkörében eljárva elrendeli a Magyarország 2025. évi központi költségvetéséről szóló 2024. évi CX. törvény (a továbbiakban: Kvtv.) IX. Helyi önkormányzatok támogatásai fejezet címrendjének a 7. Egyes helyi önkormányzatok működési feladatainak kiegészítő támogatása címmel és az 1. melléklet szerinti alcímekkel történő kiegészítését;

   Felelős: nemzetgazdasági miniszter
   közigazgatási és területfejlesztési miniszter
   Határidő: azonnal

2. az Áht. 33. § (2) bekezdésében biztosított jogkörében eljárva 182 170 000 forint egyszeri átcsoportosítását rendeli el a Kvtv. 1. melléklet IX. Helyi önkormányzatok támogatásai fejezet, 2. A helyi önkormányzatok működési célú kiegészítő támogatásai cím, 1. A helyi önkormányzatok általános feladatainak működési célú támogatása alcím terhére, a Kvtv. 1. melléklet IX. Helyi önkormányzatok támogatásai fejezet, 7. Egyes helyi önkormányzatok működési feladatainak kiegészítő támogatása cím 1. melléklet szerinti alcímei javára, a 2. melléklet szerint;

   Felelős: nemzetgazdasági miniszter
   Határidő: azonnal

3. egyetért azzal, hogy a közigazgatási és területfejlesztési miniszter a 2. pont szerint átcsoportosított forrás terhére külön pályázat és kérelem benyújtása nélkül vissza nem térítendő egyedi támogatást nyújtson az érintett önkormányzatok részére támogatási előlegként, a támogatás felhasználásának és elszámolásának részletes feltételeit meghatározó támogatói okirat alapján úgy, hogy a támogatás felhasználási határideje 2025. december 31. legyen;
4. egyetért azzal, hogy a közigazgatási és területfejlesztési miniszter a 3. pont szerinti egyedi költségvetési támogatást a támogatói okirat kiadását követően folyósítsa az 1. melléklet szerinti önkormányzatok számára.

Orbán Viktor s. k.,
miniszterelnök

1. melléklet az 1013/2025. (I. 31.) Korm. határozathoz

Alcímszám	Alcímnév	Támogatás összege (forint)	Támogatás célja
1.	Tardona Község Önkormányzata kötelező feladatainak támogatása	170 000 000	kötelező feladatok ellátása
2.	Szakácsi Község Önkormányzata működési feladatainak támogatása	12 170 000	fennálló tartozás rendezése

2. melléklet az 1013/2025. (I. 31.) Korm. határozathoz

IX. Helyi önkormányzatok támogatásai

ADATLAP A KÖLTSÉGVETÉSI ELŐIRÁNYZATOK MÓDOSÍTÁSÁRA
Költségvetési év: 2025.

forintban

Államháztartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	K I A D Á S O K / Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/ határozat száma
	IX.						Helyi önkormányzatok támogatásai									
405495		7						Egyes helyi önkormányzatok működési feladatainak kiegészítő támogatása								
405506			1						Tardona Község Önkormányzata kötelező feladatainak támogatása							
						K5						Egyéb működési célú kiadások		170 000 000		
405517			2						Szakácsi Község Önkormányzata működési feladatainak támogatása							
						K5						Egyéb működési célú kiadások		12 170 000		
		2						A helyi önkormányzatok működési célú kiegészítő támogatásai								
380073			1						A helyi önkormányzatok általános feladatainak működési célú támogatása							
						K5						Egyéb működési célú kiadások		-182 170 000		
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																

forintban

Államháztartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	B E V É T E L / Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/ határozat száma
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																

forintban

Államháztartási egyedi azonosító	Fejezet szám	Cím szám	Alcím szám	Jog-cím csop. szám	Jog-cím szám	Kiemelt előir. szám	Fejezet név	Cím név	Alcím név	Jog-cím csop. név	Jog-cím név	T Á M O G A T Á S / Kiemelt előirányzat neve	A módosítás jogcíme	Módosítás (+/-)	A módosítás következő évre áthúzódó hatása	A módosítást elrendelő jogszabály/ határozat száma
Az előirányzat-módosítás érvényessége: a) a költségvetési évben egyszeri jellegű																
												Foglalkoztatottak létszáma (fő) - időszakra				

Az adatlap 1 eredeti példányban töltendő ki	A támogatás folyósítása/zárolása (módosítása +/-)	Összesen		I. n.év	II. n.év	III. n.év	IV. n.év
Magyar Államkincstár 1 példány	időarányos teljesítésarányos egyéb: azonnal	182 170 000		182 170 000			

* Az összetartozó előirányzat-változásokat (+/-) egymást követően kell szerepeltetni.

A Kormány 1014/2025. (I. 31.) Korm. határozata a Magyarország Kormánya és a Laoszi Népi Demokratikus Köztársaság Kormánya közötti pénzügyi együttműködési keretprogram kialakításáról szóló megállapodás szövegének végleges megállapítására adott felhatalmazásról

A Kormány

1. egyetért a Magyarország Kormánya és a Laoszi Népi Demokratikus Köztársaság Kormánya közötti pénzügyi együttműködési keretprogram kialakításáról szóló megállapodás (a továbbiakban: Megállapodás) bemutatott szövegével;
2. felhatalmazza a külgazdasági és külügyminisztert vagy az általa kijelölt személyt a Megállapodás bemutatott szövegének – a jóváhagyás fenntartásával történő – végleges megállapítására;
3. felhívja a külgazdasági és külügyminisztert, hogy a Megállapodás szövegének végleges megállapításához szükséges meghatalmazási okiratot adja ki;
4. jóváhagyja a Megállapodás kihirdetéséről szóló kormányrendelet tervezetét, és elrendeli a Megállapodás szövegének végleges megállapítását követően annak a Magyar Közlönyben történő kihirdetését.

Orbán Viktor s. k.,
miniszterelnök

A miniszterelnök 9/2025. (I. 31.) ME határozata helyettes államtitkár felmentéséről

A kormányzati igazgatásról szóló 2018. évi CXXV. törvény 228. § (2) bekezdés b) pontja alapján – az igazságügyi miniszter javaslatára –

dr. Pilz Tamást, az Igazságügyi Minisztérium helyettes államtitkárát e tisztségéből

– közigazgatási államtitkárrá történő kinevezésére tekintettel –

2025. január 31-ei hatállyal

felmentem.

Orbán Viktor s. k.,
miniszterelnök

A Magyar Közlönyt az Igazságügyi Minisztérium szerkeszti.
A szerkesztésért felelős: dr. Bíró Attila.
A szerkesztőség címe: 1051 Budapest, Nádor utca 22.
A Magyar Közlöny hiteles tartalma elektronikus dokumentumként a https://www.magyarkozlony.hu honlapon érhető el.