Anyavállalat, mint EIR beszállító kezelése az auditon

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/12

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.08.13	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

1 VEZETŐI ÖSSZEFOGLALÓ

Jelen dokumentum azt vizsgálja, hogyan kell kezelnie a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kiberbiztonsági tv.) hatálya alá tartozó szervezetnek azt a helyzetet, amikor valamely elektronikus információs rendszerét (EIR), rendszerelemét vagy rendszerszolgáltatását az anyavállalata, más csoporttag vagy központi csoportszolgáltató biztosítja, üzemelteti, fejleszti, felügyeli vagy támogatja.

A külön jogi személyiséggel rendelkező anyavállalat tényleges tevékenysége alapján a Kiberbiztonsági tv. szerinti közreműködőként, kihelyezett szolgáltatóként az 7/2024 (VI.24.) MK rendelet (a továbbiakban: MK rendelet) külső EIR-szolgáltatásokra vonatkozó követelményei szerint, valamint az ellátási lánc résztvevőjeként kezelendő lehet. Egy anya- vagy leány vállalat, ha NIS2 kötelezett akkor jellemzően kihelyezett szolgáltatónak, ha nem akkor közreműködőknek minősül. A fogalmak elhatárolását segíti a „A közreműködő és kihelyezett szolgáltató fogalma és elhatárolása” c. MKIK szakértői állásfoglalás is: **https://nis2.mkik.hu/jogi-allasfoglalasok/30**

A tulajdonosi kapcsolat, a konszernszintű irányítás önmagában nem mentesít a beszállítói kontrollok alól.

A legfontosabb következtetések:

- A magyar leányvállalat vezetőjének kiberbiztonsági felelőssége főszabály szerint akkor is fennmarad, ha az EIR-t vagy a kapcsolódó szolgáltatást az anyavállalat biztosítja, de a leányvállalat rendelkezésében van.
- Az informális csoportgyakorlat, globális szabályzat, költségfelosztási kimutatás vagy tulajdonosi utasítás nem helyettesíti az EIR-re szabott, kikényszeríthető szolgáltatási megállapodást és kiberbiztonsági mellékletet.
- A leányvállalatnak saját EIR-nyilvántartással, kockázatelemzéssel, felelősségi renddel, kontrolltérképpel és auditbizonyítékokkal kell rendelkeznie akkor is, ha a technikai kontrollokat központilag működtetik.
- A szerződésnek a főszolgáltató anyavállalat alvállalkozóira és további csoporttagjaira is tovább kell hárítania az EIR-rel összefüggő információbiztonsági követelményeket.

2 A VIZSGÁLANDÓ KÉRDÉS

Vállalatcsoportokban gyakori, hogy a magyar leányvállalat nem saját informatikai szervezetet és infrastruktúrát működtet, hanem az anyavállalat vagy egy regionális shared service center szolgáltatásait veszi igénybe. Tipikus példa a központi Microsoft Entra ID vagy ERP, vállalati e-mail, felhő-előfizetés, hálózati kapcsolat, SOC/SIEM, végpontmenedzsment, mentés, fejlesztés, licenckezelés vagy helpdesk.

A megfelelőséghez az alábbi kérdéseket kell egyértelműen megválaszolni:

- Mely szolgáltatások, rendszerelemek, adminisztrátori tevékenységek és adatkezelési műveletek tartoznak az anyavállalathoz?

- Mely EIR-ek felett rendelkezik a magyar szervezet, és ezek biztonsági osztálya milyen követelményeket támaszt a csoportszolgáltatással szemben?
- Van-e olyan írásbeli, érvényesíthető megállapodás, amely a kiberbiztonsági követelményeket, felelősségeket, ellenőrzési jogokat és teljesítési kritériumokat rögzíti?
- A leányvállalat hozzáfér-e a szükséges dokumentációhoz, naplókhoz, kockázati és kontrollbizonyítékokhoz, valamint képes-e a saját incidens- és auditkötelezettségeit határidőben teljesíteni?

3 MIKOR KEZELENDŐ AZ ANYAVÁLLALAT EIR BESZÁLLÍTÓKÉNT?

Az IT beszállítók a Kiberbiztonsági tv. fogalommeghatározásai szerint az alábbi kategóriába sorolhatók:

- **Kihelyezett szolgáltató**

A kiberbiztonsági törvény értelmező rendelkezései a kihelyezett (irányított) szolgáltatók két specifikus kategóriáját határozzák meg az általuk nyújtott szolgáltatás jellege és biztonsági funkciója alapján:

  - Kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, a hétköznapi üzleti nyelvben gyakran MSP-nek (Managed Service Provider)-nek nevezik.

    kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató: olyan szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról; [2024. évi LXIX. tv. 4. § 53.]

  - Kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató, Ezek a szolgáltatók az MSP-k egy speciális kategóriáját alkotják, amelyeket az iparági gyakorlatban MSSP (Managed Security Service Provider) rövidítéssel jelölnek. Tevékenységük során nem csak általános üzemeltetést végeznek, hanem dedikáltan a kiberbiztonságra fókuszálnak (például biztonsági incidensek megfigyelése, kockázatok felmérése és kezelése).

    kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató: olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt; [2024. évi LXIX. tv. 4. § 52.]

- **Közreműködő**

A „közreműködő” fogalmát a jogalkotó a kifejezést a szervezet által feladatellátásra bevont harmadik felekre (alvállalkozókra, külső szakértőkre) alkalmazza. A törvény az alapvető és fontos szervezetek általános kötelezettségei között adja meg a közreműködők funkcionális meghatározását, rögzítve az igénybevételük esetén alkalmazandó garanciális és szerződéses kereteket:

> *ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, biztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási feladatok ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek; [2024. évi LXIX. tv. 6. § (5) bekezdés d) pont]*

A fogalmak magyarázatát, elhatárolását és egymáshoz való viszonyát részletesen bemutatja az alábbi szakértői iránymutatás: **https://nis2.mkik.hu/jogi-allasfoglalasok/30**

Az anyavállalatot vagy más csoporttagot beszállítói kontroll alá kell vonni, ha a magyar szervezet EIR-évél kapcsolatban ténylegesen az alábbiak közül bármely tevékenységet végzi:

Tényleges szerep	Példa
EIR vagy rendszerszolgáltatás biztosítása	A rendszer, tenant, előfizetés, adatközponti vagy felhős szolgáltatás az anyavállalat tulajdonában vagy szerződésében áll, a leányvállalat azt használja.
Üzemeltetés és adminisztráció	Az anyavállalati IT jogosultsággal konfigurál, javít, frissít, ment, helyreállít, monitoroz vagy felhasználót kezel.
Fejlesztés, adaptálás vagy rendszerkövetés	Csoportközpont fejleszti, testre szabja vagy kiadja a leányvállalat által használt alkalmazást.
Adatkezelés vagy adatfeldolgozás	Az anyavállalat rendszereiben szervezeti adatot tárolnak, továbbítanak, elemeznek vagy hozzáférhetővé tesznek.
Kiberbiztonsági szolgáltatás	Csoport-SOC, SIEM, EDR, sérülékenységkezelés, incidenskezelés vagy IAM/PAM szolgáltatás működik.
Fővállalkozói közvetítés	Az anyavállalat szerződik felhő-, hálózati vagy szoftverszolgáltatóval, majd a szolgáltatást a leányvállalat rendelkezésére bocsátja.

Nem beszállítói szerep önmagában az, ha az anyavállalat kizárólag tulajdonosi irányítást gyakorol, csoportszintű minimumszabályt határoz meg vagy jóváhagyást ad, de nem nyújt EIR-t, rendszerszolgáltatást, technikai hozzáférést, üzemeltetést vagy adatfeldolgozást.

A szerepeket rendszerenként és szolgáltatásonként kell értékelni; ugyanaz az anyavállalat az egyik EIR-nél beszállító, a másiknál kizárólag tulajdonosi irányító lehet.

A Kiberbiztonsági tv. kivételt csak a kötelezően igénybe veendő központi szolgáltató vagy központi rendszer körében nevesít. A központi szolgáltató" vagy „központi rendszer" fogalma tipikusan az állami, kormányzati célú hálózatokra és a kijelölt állami szolgáltatókra (pl. NISZ Zrt.) vonatkozik, ezért a piaci szereplők esetében ritkán fordul elő. Ilyen lehet pl a DÁP azonosítás használata egy piaci szolgáltatásba való bejelentkezésnél.

4 MAGYAR JOGSZABÁLYI ALAP

> *„6. § (5) A szervezet vezetője az elektronikus információs rendszer védelmének biztosítása érdekében*
> *d) ha a szervezet közreműködőt vesz igénybe az elektronikus információs rendszer létrehozása, üzemeltetése, auditálása, karbantartása, javítása, illetve a kiberbiztonsági incidensek kezelése során, vagy a szervezet elektronikus információs rendszerével kapcsolatos adatkezelési, adatfeldolgozási tevékenység ellátásához, gondoskodik arról, hogy a közreműködő által az elektronikus információs rendszerrel kapcsolatosan ellátott tevékenységgel összefüggésben szükséges kiberbiztonsági követelmények az e törvényben foglaltaknak megfelelően szerződéses kötelemként teljesüljenek;"*
> *[2024. évi LXIX. törvény 6. § (5) bekezdés d) pont]*
>
> *„6. § (6) A (3)–(5) bekezdésben meghatározott feladatokért a szervezet vezetője az (5) bekezdés d) pontjában meghatározott esetben is felelős, kivéve – az igénybe vett szolgáltatások mértékéig – azokat az esetköröket, amikor központi szolgáltatót vagy központi rendszert kell a szervezetnek igénybe vennie."*
> *[2024. évi LXIX. törvény 6. § (6) bekezdés]*
>
> *„11. § (9) Az elektronikus információs rendszer biztonságáért felelős személy jogosult a szervezet elektronikus információbiztonsági kötelezettségeinek, feladatainak teljesítésében közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni."*
> *[2024. évi LXIX. törvény 11. § (9) bekezdés]*

A jogszabályi logika alapján az anyavállalat bevonása nem felelősség-átruházás, hanem kontrollált közreműködői modell. A magyar szervezetnek (leányvállalatnak) a követelményeket szerződésbe kell foglalnia, a teljesülést ellenőriznie kell, és az EIR biztonságáért felelős személy információkérését ténylegesen lehetővé kell tennie.

5 ALKALMAZANDÓ KÖVETELMÉNYEK

5.1 Kiemelt prioritású követelmények

A jelen fejezetben bemutatott kontrollok nem tekinthetők az anyavállalati szolgáltatás kapcsán kizárólagosan kezelendő követelmények teljes körű felsorolásának. Az alkalmazandó kontrollokat minden esetben az érintett Magyarországon használt EIR biztonsági osztálya, kockázatai és tényleges szolgáltatási hatóköre alapján kell meghatározni.

Az anyavállalat által bevezetett technológiai megoldásokat e kontrollok megvalósításának részeként szükséges értékelni. Egy kontroll csak akkor tekinthető a magyar EIR-ben teljesítettnek, ha a magyar szervezet annak teljes hatókörét, megfelelő kialakítását, tényleges működését és eredményességét aktuális, az adott EIR-hez egyértelműen hozzárendelhető bizonyítékokkal igazolni tudja.

> *„14.11. A szervezet:*
> *14.11.1. Személyi biztonsági követelményeket állít fel a külső szolgáltatókkal szemben, amelyek magukba foglalják a szükséges biztonsági szerepköröket és felelősségeket.*
> *14.11.2. Megköveteli a külső szolgáltatóktól, hogy tartsák be a szervezet által meghatározott személyi biztonsági szabályokat.*
> *14.11.3. Dokumentálja a személyi biztonsági követelményeket.*
> *14.11.4. Megköveteli a külső szolgáltatóktól, hogy a meghatározott időn belül értesítsék a meghatározott személyeket vagy szerepköröket minden olyan külső személy áthelyezéséről vagy kilépéséről, akik szervezeti hitelesítő eszközzel, belépőkártyával vagy rendszerjogosultsággal rendelkeztek.*
> *14.11.5. Ellenőrzi, hogy a szolgáltató megfelel-e a személyi biztonsági követelményeknek.”*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 14.11. pont] (A, J, M)*

A magyar szervezetnek az anyavállalati szolgáltató személyi állományára is meghatározott személyi biztonsági követelményeket kell előírnia. Ezeknek ki kell térniük a biztonsági szerepkörökre, a titoktartásra, a képzettségre, a jogszerűen alkalmazható háttérellenőrzésre, továbbá az áthelyezés és kilépés bejelentési, illetve hozzáférés-megszüntetési határidejére. A követelmény a további csoporttagokra és alvállalkozókra is kiterjed.

Az anyavállalatnak igazolnia kell, hogy a magyar EIR-hez hozzáférő személyek azonosítottak, megfelelő szerepkörrel rendelkeznek, elfogadták a szükséges szabályokat, és kilépés vagy szerepváltozás esetén a jogosultságuk határidőben megszűnik. Elfogadható bizonyíték lehet a szerepkörlista, a képzési és titoktartási nyilvántartás, az áthelyezési vagy kilépési értesítés, a hozzáférés-visszavonási jegy és a szolgáltatói megfelelőségi ellenőrzés.

> *„15.5. A szervezet:*
> *15.5.1. Felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.*

15.5.2. Meghatározott időközönként frissíti az ellátási lánc kockázatelemzését, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor a rendszer, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatására."
[7/2024. (VI. 24.) MK rendelet 2. melléklet 15.5. pont] (A, J, M)

Az ellátási lánc kockázatelemzését nem lehet kizárólag az anyavállalat általános vállalatcsoport-szintű kockázatértékelésére alapozni. A magyar szervezetnek EIR-enként fel kell mérnie az anyavállalati szolgáltatás, a további csoporttagok és az alvállalkozók kockázatait, ideértve a hozzáférési, koncentrációs, technológiai, földrajzi, joghatósági, folytonossági és kilépési függőségeket is.

A teljesítéshez aktuális szolgáltatói és alvállalkozói jegyzék, EIR-specifikus kockázatelemzés, kockázatkezelési intézkedések, felelősök és határidők szükségesek. Az anyavállalatnak adatot kell szolgáltatnia a tényleges szolgáltatási láncról és annak jelentős változásairól; a magyar szervezetnek pedig dokumentáltan újra kell értékelnie a kockázatot szolgáltató-, technológia-, helyszín- vagy alvállalkozó változás esetén.

„16.7. A szervezet a beszerzési folyamat során – beleértve a fejlesztést, az adaptálást, a rendszerkövetést és a karbantartást is – a szerződéseiben egységes nyelvezetet alkalmaz, továbbá követelményként rögzíti az alábbiakat:
16.7.1. A funkcionális biztonsági követelményeket.
16.7.2. A mechanizmusok erősségére vonatkozó követelményeket.
16.7.3. A biztonság garanciális követelményeit.
16.7.4. Az érintett EIR biztonsági osztályát és az ahhoz tartozó, illetve a szervezet által meghatározott további biztonsági követelmények teljesítéséhez szükséges védelmi intézkedéseket.
16.7.5. A biztonsággal kapcsolatos dokumentációs követelményeket.
16.7.6. A biztonsággal kapcsolatos dokumentumok védelmére vonatkozó követelményeket.
16.7.7. Az EIR fejlesztési környezetére és tervezett üzemeltetési környezetére vonatkozó előírásokat.
16.7.8. A felelősség megosztását vagy az információbiztonságért és az ellátási lánc kockázatkezeléséért felelős felek azonosítását.
16.7.9. A teljesítési kritériumokat."
[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.7. pont] (A, J, M)

A vállalatcsoporton belüli szolgáltatásnál a szervezetek közötti megállapodást tartalma alapján beszerzési és szolgáltatási szerződésként kell kezelni. A szerződésnek nem csupán általános biztonsági együttműködést kell rögzítenie, hanem a *16.7. pont* valamennyi elemét: a funkcionális követelményeket, a mechanizmusok elvárt erősségét, a garanciális és dokumentációs

követelményeket, az EIR biztonsági osztályát, a fejlesztési és üzemeltetési környezetet, a felelősségmegosztást és a mérhető teljesítési kritériumokat.

A magyar szervezetnek igazolnia kell, hogy minden alkalmazandó MK rendeletkövetelményéhez/csoportjához kijelölt végrehajtó, kontrollgazda, teljesítési kritérium és bizonyíték tartozik. Ennek alapja az aláírt szerződés, amelynek minimálisan kötelező tartalmát meghatározza a 7/2024 (VI.24.) MK rendelet. A közreműködővel kötött szerződés kötelező tartalmáról bővebben az alábbi, a „A közreműködővel kötött szerződés tartalma” című iránymutatásban írunk: **https://nis2.mkik.hu/iranymutatasok/10**. A szerződésből egyértelműen ki kell derülnie annak is, hogyan bizonyítja az anyavállalat a kontrollok teljes körű megvalósítását.

> *„16.15. A szervezet:*
> *16.15.1. Kidolgozza vagy beszerzi az EIR, rendszerelem vagy rendszerszolgáltatás adminisztrátori és üzemeltetői dokumentációját, amely tartalmazza:*
> *16.15.1.1. az EIR, rendszerelem vagy rendszerszolgáltatás biztonságos konfigurációját, telepítését és üzemeltetését;*
> *16.15.1.2. a biztonsági funkciók hatékony használatát és karbantartását; valamint*
> *16.15.1.3. az ismert sérülékenységeket a konfigurációval és a rendszergazdai vagy privilegizált funkciók használatával kapcsolatban.*
> *16.15.2. Kidolgozza vagy beszerzi a rendszer, rendszerelem vagy rendszerszolgáltatás felhasználói dokumentációját, amely tartalmazza:*
> *16.15.2.1. a felhasználók számára elérhető biztonsági funkciókat és mechanizmusokat és ezek hatékony használatának módját;*
> *16.15.2.2. a felhasználói interakció biztonságos módját;*
> *16.15.2.3. a felhasználók felelősségét az EIR, rendszerelem, rendszerszolgáltatás biztonságának fenntartásában.*
> *16.15.3. Amennyiben nem áll rendelkezésre vagy nem létezik adminisztrátori, üzemeltetői és felhasználói dokumentáció, úgy a szervezet dokumentálja az EIR, rendszerelem vagy rendszerszolgáltatás dokumentációjának beszerzésére tett kísérleteket, valamint végrehajtja a szervezet által meghatározott intézkedéseket; és*
> *16.15.4. a dokumentációkat eljuttatja a szervezet által meghatározott személyeknek vagy szerepköröknek.”*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.15. pont] (A, J, M)*

A magyar szervezetnek akkor is rendelkeznie kell az EIR biztonságos üzemeltetéséhez szükséges dokumentációval, ha azt az anyavállalat készíti és tartja karban. A dokumentációnak ténylegesen használhatónak, aktuálisnak és a kijelölt magyar szerepkörök számára hozzáférhetőnek kell lennie; egy általános, nem EIR-specifikus csoportwiki (pl Confluence) vagy intranet (pl Sharepoint) oldal vagy termékleírás nem feltétlenül teljesíti a követelményt.

Az anyavállalatnak át kell adnia vagy ellenőrzött hozzáféréssel elérhetővé kell tennie a biztonságos konfigurációs és üzemeltetési leírásokat, a biztonsági funkciók használatát, az ismert sérülékenységeket, a felhasználói felelősségeket, valamint a verzió- és változáskövetést.

> *„16.49. A szervezet:*
> *16.49.1. Szerződéses kötelezettségként követeli meg, hogy a szolgáltatási szerződés alapján általa igénybe vett EIR-ek szolgáltatásai megfeleljenek a szervezet elektronikus információbiztonsági követelményeinek, és a szervezet által meghatározott védelmi intézkedéseket alkalmazzák.*
> *16.49.2. Meghatározza és dokumentálja a szervezeti felügyelet és a szervezet felhasználóinak feladatait és kötelezettségeit a külső EIR-ek szolgáltatásával kapcsolatban.*
> *16.49.3. külső és belső ellenőrzési eszközökkel ellenőrzi, hogy a külső EIR szolgáltatója megfelel-e az elvárt védelmi intézkedéseknek.”*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 16.49. pont] (A, J, M)*

Ez a követelmény az anyavállalati EIR-szolgáltatás egyik központi kontrollja. A magyar szervezetnek szerződésben kell megkövetelnie a saját információbiztonsági követelményeit, dokumentálnia kell a helyi és anyavállalati feladatmegosztást, majd belső és külső ellenőrzési eszközökkel meg kell győződnie a követelmények tényleges teljesüléséről.

Az anyavállalat által működtetett kontroll csak akkor számítható teljesítettként, ha az alkalmazandó MK rendelet követelménycsoportjának valamennyi alpontjára, a teljes magyar EIR-hatókörre és az auditált időszakra vonatkozó bizonyíték rendelkezésre áll.

> *„19.13. A szervezet meghatározott beszerzési stratégiákat, szerződéses eszközöket és beszerzési módszereket alkalmaz annak érdekében, hogy kivédje, azonosítsa és csökkentse az ellátási láncból eredő kockázatokat.”*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 19.13. pont] (A, J, M)*

A szervezetnek kockázatalapú beszerzési és szerződéses eszközökkel kell csökkentenie az anyavállalati szolgáltatásból és annak beszállítói láncából eredő kockázatokat. Ide tartozhat a szolgáltatók kockázati kategorizálása, az előzetes átvilágítás, az auditjog, a hordozhatóság és exit támogatás, a függőségcsökkentés, a forráskód- vagy konfigurációátadás és a kritikus szolgáltatások alternatív megoldása.

Igazolni kell, hogy a kiválasztott beszerzési vagy szerződéses módszer az adott EIR kockázataihoz igazodik, és nem pusztán általános vállalatcsoport-szintű gyakorlat.

> *„19.19. A szervezet megállapodásokat köt és eljárásokat hoz létre a rendszer, rendszerelem vagy rendszerszolgáltatás beszállítói láncában részt vevő szervezetekkel.”*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 19.19. pont] (A, J, M)*

A szerződés önmagában nem elegendő, a beszállítói lánc résztvevőivel működő operatív eljárásokat is létre kell hozni. Ezeknek legalább az incidensértesítést, a változás- és

sérülékenységkezelést, a hozzáférések kezelését, a folytonosságot és helyreállítást, a bizonyítékátadást, az eszkalációt, valamint a szolgáltatás megszűnését és az adatok visszaadását vagy törlését kell rendezniük.

Az anyavállalatnak és a további szolgáltatóknak bizonyítaniuk kell, hogy a megállapodások nemcsak aláírt dokumentumként léteznek, hanem az operatív folyamatok ténylegesen működnek.

5.2 Az anyavállalat által végrehajtott kontrollok teljes körű igazolása

A *Kiberbiztonsági tv. 6. § (5) bekezdés d) pontja*, a vezetői felelősséget fenntartó *6. § (6) bekezdés*, valamint az MK rendelet valamennyi követelménye együttesen azt jelentik, hogy az anyavállalat technikai vagy szervezeti közreműködése nem váltható ki általános csoportszintű megfelelőségi nyilatkozattal. A magyar szervezetnek EIR-enként meg kell határoznia az alkalmazandó MK rendelet szerintikövetelményeket/követelménycsoportokat, és kontrollonként igazolnia kell, hogy az anyavállalat a rá kiosztott követelményt a teljes releváns hatókörben ténylegesen megvalósítja.

Az anyavállalat által végrehajtott kontroll csak akkor tekinthető a magyar EIR-ben teljesítettnek, ha a magyar szervezet bizonyítani tudja, hogy:

- a kontroll a követelmény teljes releváns tartalmát lefedi;
- kiterjed a magyar EIR valamennyi érintett elemére és szolgáltatási összetevőjére;
- a kontroll kialakítása megfelelő és dokumentált;
- a kontroll az értékelt időszakban ténylegesen működött;
- az eltéréseket, kivételeket és hiányosságokat megfelelően kezelték;
- a bizonyíték aktuális, megbízható és egyértelműen az érintett EIR-hez rendelhető.

A kontroll teljesítéséért és igazolhatóságáért fennálló felelősség az anyavállalati közreműködés ellenére is a magyar szervezetnél marad. Bizonyíték hiányában a kontroll nem tekinthető igazoltan teljesítettnek.

5.3 A teljes körű megvalósítás értékelési szempontjai

Az anyavállalat által működtetett kontrollok értékelését az alábbi szempontok szerint kell elvégezni.

Értékelési szempont	Elvárt tartalom
Követelményi teljesség	Az alkalmazandó MK rendelet szerinti követelmény/csoport valamennyi releváns alpontját le kell képezni. Nem elegendő egy hasonló célú csoportkontroll vagy általános szabályzat megnevezése.
Hatóköri teljesség	A kontrollnak ki kell terjednie az érintett EIR valamennyi releváns rendszerelemére, környezetére, telephelyére, felhasználójára,

Értékelési szempont	Elvárt tartalom
	privilegizált szerepkörére, adatáramlására és közreműködő szolgáltatójára.
Megfelelő kialakítás	Meghatározott kontrollcél, eljárás, műszaki konfiguráció, felelős, végrehajtási gyakoriság, hatókör és elfogadási kritérium szükséges.
Tényleges működés	Igazolni kell, hogy a kontroll az értékelt időszakban a meghatározott módon és gyakorisággal ténylegesen működött.
Aktualitás	A bizonyítéknak az auditált időszakra, az aktuális technológiai állapotra és a tényleges szolgáltatási környezetre kell vonatkoznia.
Nyomon követhetőség	Egyértelmű kapcsolatot kell teremteni az MK rendelet szerintikövetelmény/csoportok, az anyavállalati kontroll, az érintett EIR, a kontrollgazda és a bizonyíték között.
Helyi értékelés	Az átadott bizonyítékot a magyar szervezet kijelölt szerepkörének tartalmilag értékelnie és dokumentáltan elfogadnia kell.

5.4 Kontrollfelelősségi modell

Minden alkalmazandó MK rendelet szerinti követelménynél/követelménycsoportnál egyértelműen meg kell határozni a végrehajtási modellt:

- helyi kontroll, a kontrollt teljes egészében a magyar szervezet hajtja végre;
- anyavállalati kontroll, a kontroll végrehajtását az anyavállalat biztosítja;
- megosztott kontroll, a kontroll egyes részeit a magyar szervezet, más részeit az anyavállalat vagy további szolgáltató működteti.

Megosztott kontroll esetén különösen fontos a felelősségi határok és az átadási pontok meghatározása. Dokumentálni kell, hogy ki:

- alakítja ki és működteti a kontrollt;
- állítja elő a bizonyítékot;
- értékeli annak megfelelőségét;
- kezeli az eltéréseket;
- hagyja jóvá a maradványkockázatot;
- támogatja az auditot;
- gondoskodik a helyettesítésről és az eszkalációról.

Az anyavállalati végrehajtás nem érintheti a magyar szervezet végső felelősségét a kontroll megfelelőségének megállapításáért.

6 SZERZŐDÉSES ÉS DOKUMENTÁCIÓS ALAPMODELL

Az anyavállalati szolgáltatás megfelelőségének alapja nem egyetlen dokumentum, hanem egymásra épülő, egymásra hivatkozó és jogilag kötelező dokumentumcsomag. A dokumentumoknak együttesen kell meghatározniuk, hogy az anyavállalat pontosan milyen szolgáltatást és kontrollt biztosít, milyen hatókörben, milyen teljesítési kritériumokkal, milyen bizonyítékokkal és milyen felelősség mellett.

A csoportszintű szabályzat, biztonsági kézikönyv vagy technológiai leírás önmagában nem helyettesíti a szerződéses kötelmet. Az EIR-specifikus melléklet, az SLA, a kontrollmátrix és az operatív eljárások csak akkor használhatók szerződéses bizonyítékként, ha az alapszerződés azokat kötelező mellékletként vagy hivatkozott dokumentumként beemeli, és verziójuk, hatálybalépésük, jóváhagyóik és módosítási rendjük visszakövethető.

6.1 Az anyavállalattal kötött megállapodás ajánlott tartalma

A megállapodásban nem elegendő azt rögzíteni, hogy az anyavállalat *„kezeli az informatikát”, „biztosítja a kiberbiztonságot”* vagy *„megfelel a NIS2-nek”*. A vállalásokat EIR-hez, szolgáltatáshoz, kontrollhoz, felelőshöz, határidőhöz, elfogadási kritériumhoz kell kötni.

Szerződéses tárgy	Rögzítendő minimum
Felek, szolgáltatás és hatókör	A szerződő jogi személyek, az érintett szolgáltatások és EIR-ek, rendszerelemek, környezetek, helyszínek, interfészek, felhasználói körök, valamint a kizárt elemek.
Biztonsági követelmények	Az EIR biztonsági osztálya és kritikussága, az alkalmazandó MK rendelet szerinti követelménycsoportok, a belső követelmények.
Felelősségi megosztás	A helyi, anyavállalati és megosztott feladatok, kontrollgazdák, döntési jogok, kapcsolattartók, helyettesítési és eszkalációs rend.
Személyi és hozzáférési biztonság	A hozzáférés és privilegizált jogosultságok feltételei, a hitelesítés, a titoktartás és képzés, valamint a szerepváltozás és kilépés kezelésének határideje.
Változás- és sérülékenységkezelés	A jelentős és sürgősségi változások bejelentése, biztonsági értékelése és dokumentálása, továbbá a sérülékenységek és javítások kezelési határideje.
Incidenskezelés	Az értesítés belső határideje, a kötelezően átadandó információk, a rendszeres helyzetfrissítés, a bizonyítékmegőrzés és az együttműködési rend.
Üzemeltetési és biztonsági dokumentáció	A biztonságos konfigurációs, adminisztrátori, üzemeltetői és felhasználói dokumentáció rendelkezésre bocsátása, aktualizálása, verziókezelése és a kijelölt magyar szerepkörök hozzáférése.

Audit- és információhozzáférési jog	A magyar szervezet, az EIR biztonságáért felelős személy, az auditor és az arra jogosult hatóság dokumentum-, riport- és bizonyítékhozzáférése, továbbá a mintavételes, távoli vagy indokolt esetben helyszíni ellenőrzés és a megállapítások nyomon követése.
Megszűnés, exit és adattörlés	Az adatok, naplók, konfigurációk, kulcsok és dokumentáció átadása, az átmeneti támogatás, a hozzáférések megszüntetése, valamint a fennmaradó adatpéldányok biztonságos törlése és annak igazolása.
Folytonosság és helyreállítás	A rendelkezésre állási követelmények, RTO/RPO értékek, mentési és visszaállítási feladatok, tesztelési gyakoriság és válságkommunikáció.
Bizonyítékok és riportok	A kontrollonként átadandó bizonyítékok, azok formátuma, gyakorisága, határideje, felelőse, megőrzése és rendkívüli adatszolgáltatási rendje.
Alvállalkozói lánc	A további csoporttagok és alvállalkozók nyilvántartása, a lényeges változások bejelentése, a követelmények továbbhárítása és az anyavállalat felelősségének fenntartása.

6.2 Az EIR-specifikus kiberbiztonsági melléklet

Az intercompany keretszerződéshez célszerű EIR- vagy szolgáltatáscsoport-szintű kiberbiztonsági mellékletet kapcsolni. Ha külön melléklet nem készül, ugyanezeket az információkat a szerződésben vagy az abba kötelező hivatkozással beemelt, verziókezelt dokumentumban kell rögzíteni. A dokumentációnak az általános vállalatcsoport-szintű vállalásokat az érintett magyar EIR konkrét technológiai, szervezeti és jogszabályi hatókörére kell lefordítania.

A mellékletben legalább az alábbiakat kell rögzíteni:

- az érintett EIR vagy szolgáltatás azonosítását, rendeltetését, biztonsági osztályát, rendszerelemeit, környezeteit, helyszíneit és adatáramlásait;
- a kezelt adatok kategóriáit, biztonsági és megőrzési követelményeit;
- az alkalmazandó 7/2024 MK rendelet szerinti követelménycsoportokat, azok anyavállalati megvalósítását, valamint a helyi, anyavállalati és megosztott felelősségeket;
- a kontrollok teljesítési és elfogadási kritériumait, továbbá az előállítandó bizonyítékok típusát, gyakoriságát és átadási rendjét;
- az alvállalkozók és további csoporttagok szerepét, hozzáféréseit, valamint a jóváhagyott kivételeket és kompenzáló intézkedéseket;
- a melléklet verzióját, hatályát, jóváhagyóit és módosítási rendjét.

A mellékletnek konkrét, ellenőrizhető vállalásokat kell tartalmaznia. Az olyan általános állítások helyett, mint például a *„naplózás megfelelően működik”*, meg kell határozni a lefedett rendszereket, a felelős szerepköröket, a működési és riasztáskezelési követelményeket.

7 FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról