A kritikus infrastruktúra biztonsági terv készítésére vonatkozó követelmény teljesíthető -e a rendszerbiztonsági terv elkészítésével?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/11

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.01.20	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A 7/2024. (VI. 24.) MK rendelet 1.9. pontja szerint a szervezetnek kritikus infrastruktúra biztonsági tervet kell készítenie, amely során kezelnie kell az információbiztonsági kérdéseket. A kérdés, hogy ez a követelmény teljesíthető-e a Nemzeti Kibervédelmi Intézet (NKI) által kiadott rendszerbiztonsági terv sablonnal.

Az NKI által kiadott rendszerbiztonsági terv sablon kitöltése önmagában nem meríti ki teljesen az 1.9. követelményt, de a megfelelés egyik legfontosabb eszköze. Az audit során az 1.9 pont teljesüléséhez a szervezetnek igazolnia kell, az üzleti hatáselemzés (BIA) elkészítését, amely azonosítja a kritikus folyamatokat és erőforrásokat.

Az auditor azt vizsgálja, hogy a szervezet rendszerszinten kezeli-e a kockázatokat, nem csupán technikai sablonokat töltött-e ki.

2. A VIZSGÁLANDÓ KÉRDÉS

A 7/2024. (VI. 24.) MK rendelet (a továbbiakban: MKr.) 1.9 pontja előírja a kritikus infrastruktúra biztonsági terv készítését

> *1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve*
> *1.9. A szervezet a szervezet működése szempontjából kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervének kidolgozása, dokumentálása és frissítése során kezeli az információbiztonsági kérdéseket*

Kérdés, hogy ez a követelmény teljesíthető a rendszerbiztonság terv elkészítésével (az NKI által kiadott sablonban)?

3. VÁLASZ

Az MKr. 2. mellékletének 1.9. pontja a „Programmenedzsment” követelménycsalád részét képezi. Ez a kontroll nem egy konkrét informatikai rendszer technikai beállítására vonatkozik, hanem egy magasabb szintű szervezeti folyamatra: arra kötelezi a szervezetet, hogy a működése szempontjából kritikus infrastruktúra tervezésekor az információbiztonsági szempontokat integráltan kezelje.

A jogszabály szövege szerint:

> *1.9. A szervezet a szervezet működése szempontjából kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervének kidolgozása, dokumentálása és frissítése során kezeli az információbiztonsági kérdéseket. [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.9.]*

Ez a követelmény az Alap (A), Jelentős (J) és Magas (M) biztonsági osztályba sorolt rendszerek esetében egyaránt kötelező. A kiberbiztonsági audit során ez egy „Biztosító" típusú követelményként vizsgálandó, ahol az auditor dokumentumvizsgálattal és interjúval ellenőrzi a megfelelőséget.

A rendszerbiztonsági tervvel való kapcsolat kérdésére a válasz összetett: az MKr. külön követelményként nevesíti a rendszerbiztonsági terv elkészítését a 13.2. pont alatt.

> *13.2. A szervezet:*
> *13.2.1. Az EIR-hez rendszerbiztonsági tervet készít, amely:*
> *13.2.1.1. Összhangban áll a szervezeti felépítéssel.*
> *13.2.1.2. Meghatározza az EIR-t alkotó rendszerelemeket.*
> *13.2.1.3. Meghatározza az EIR hatókörét, alapfeladatait és biztosítandó szolgáltatásait az ügymeneti és üzleti folyamatok szempontjából.*
> *13.2.1.4. Azonosítja azokat a személyeket, akik az EIR szerepeit és felelősségeit betöltik.*
> *13.2.1.5. Meghatározza az EIR által feldolgozott, tárolt és továbbított információtípusokat.*
> *13.2.1.6. Megfelelően alátámasztott módon meghatározza az EIR jogszabály szerinti biztonsági osztályát.*
> *13.2.1.7. Felsorolja az EIR-t érintő konkrét fenyegetéseket.*
> *13.2.1.8. Meghatározza az EIR működési környezetét és más EIR-ekkel vagy rendszerelemekkel való kapcsolatait vagy azoktól való függőségeit.*
> *13.2.1.9. Dokumentálja a rendszerre vonatkozó biztonsági követelményeket.*
> *13.2.1.10. Meghatározza a biztonsági alapkövetelményeket és szükség esetén az ezen felül alkalmazott kiegészítő védelmi intézkedéseket.*
> *13.2.1.11. Meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket, intézkedésbővítéseket és azok indoklását, végrehajtja a jogszabály szerinti biztonsági feladatokat.*
> *13.2.1.12. Tartalmazza az EIR-t érintő olyan biztonsággal kapcsolatos tevékenységeket, amelyek meghatározott személyek és csoportok között koordinációt vagy tervezést igényelnek. (…)*
> *[7/2024. (VI. 24.) MK rendelet 2. melléklet 13.2.]*

Ez a követelmény szintén kötelező az Alap (A), Jelentős (J) és Magas (M) biztonsági osztályok számára. Míg a 13.2. pont magára a dokumentum (az RBT) meglétére és tartalmára fókuszál, addig az 1.9. pont azt várja el, hogy a szervezet általános (nem feltétlenül csak informatikai) kritikus infrastruktúra-tervezési folyamataiban jelenjen meg az információbiztonság.

Szakmai szempontból a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete (NBSZ NKI) által kiadott rendszerbiztonsági terv sablon kitöltése önmagában nem meríti ki teljesen az 1.9. követelményt, de a megfelelés egyik legfontosabb eszköze. A teljesítéshez az alábbi összefüggéseket kell figyelembe venni:

- Az 1.9. követelmény, amely a kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervezése során az információbiztonsági szempontok érvényesítését írja elő;

- A 13.2. követelmény, amely a konkrét elektronikus információs rendszer (EIR) biztonsági paramétereit rögzítő tervdokumentum (RBT) elkészítését követeli meg;
- A szervezeti szintű egyéb tervek, amelyek a fizikai és üzemeltetési biztonságot kezelik (pl. fizikai védelmi terv vagy üzletmenet-folytonossági terv).

Amennyiben a szervezet működése szempontjából kritikus infrastruktúra elemeit (például egy gyártósor vezérlését vagy egy központi adatbázist) a szervezet elektronikus információs rendszerként (EIR) azonosította és biztonsági osztályba sorolta, úgy az ezekre elkészített rendszerbiztonsági terv (az NKI sablonja alapján) bizonyítékként szolgál arra, hogy a szervezet „kezeli az információbiztonsági kérdéseket.

Az audit során azonban a szervezetnek igazolnia kell, hogy:

- A kritikus erőforrások azonosítása megtörtént;
- Az információbiztonsági vezető (vagy a felelős személy) részt vett ezen erőforrások biztonsági tervezésében;
- A rendszerbiztonsági tervben rögzített intézkedések összhangban vannak a szervezet általános működési kockázataival.

A kiberbiztonsági audit során az auditor célja annak megállapítása, hogy a szervezet nem csupán egy-egy technikai sablont töltött-e ki, hanem rendszerszinten kezeli a kockázatokat. Az 1.9. és a 13.2. követelmények közötti különbségtétel kulcsfontosságú a sikeres audit szempontjából, mivel az egyik a stratégiai tervezésről, a másik a konkrét megvalósításról szól.

Az 1.9. pont a „Programmenedzsment” (PM) családba tartozik. Az auditor itt azt vizsgálja, hogy a szervezet hogyan azonosítja a számára létfontosságú erőforrásokat és hogyan építi be a biztonságot a stratégiai szintű tervezésbe.

Az audit során az alábbi dokumentumok szolgálhatnak bizonyítékként:

- Az üzleti hatáselemzés (BIA), amelyben a szervezet azonosította a kritikus üzleti folyamatokat és az azokhoz rendelt kulcsfontosságú erőforrásokat;
- A kritikus infrastruktúra védelmi terv (ha a szervezet a 2012. évi CLXVI. törvény hatálya alá is tartozik), amely tartalmazza az információbiztonsági aspektusokat is;
- Olyan felsővezetői döntések vagy jegyzőkönyvek, amelyek igazolják, hogy az infrastruktúra fejlesztése során az információbiztonsági vezető (IBV) véleményét kikérték;
- A szervezet éves információbiztonsági stratégiája, amely nevesíti a kulcsfontosságú erőforrások védelmi irányelveit.

A 13.2. pont a „Rendszer- és szolgáltatásbeszerzés” család része. Ez egy konkrét, technikai és adminisztratív fókuszú dokumentumot igényel minden egyes elektronikus információs rendszerre (EIR) vonatkozóan.

Az auditor által kért dokumentáció elemei:

- A Nemzeti Kibervédelmi Intézet (NKI) által közzétett módszertan szerinti rendszerbiztonsági terv (RBT), amely kitér a logikai, fizikai és adminisztratív védelmi intézkedésekre;

- A rendszer architektúra-terve és hálózati topológiája, amely alátámasztja az RBT-ben rögzített technikai határokat;
- A kockázatelemzési jegyzőkönyv, amely az adott EIR-re jellemző fenyegetéseket és sérülékenységeket veszi számba;
- Az üzemeltetési és biztonsági szabályzatok, amelyek az RBT-ben leírt intézkedések végrehajtását részletezik.

Az elkülönítés lényege az audit szempontjából

A két követelmény közötti különbséget és a dokumentációs átfedéseket az alábbi táblázat foglalja össze:

Szempont	**1.9. Kritikus infrastruktúra biztonsági terve**	**13.2. Rendszerbiztonsági terv (RBT)**
Szint	Stratégiai / Szervezeti szint	Operatív / Rendszer szint
Fókusz	Erőforrások és folyamatok prioritása	Konkrét védelmi kontrollok és beállítások
Fő bizonyíték	Üzleti hatáselemzés, Stratégia	NKI sablon szerinti RBT dokumentum
IBF szerepe	Tervezésben való részvétel és tanácsadás	A dokumentum elkészítése vagy jóváhagyása

Az auditor számára az 1.9. teljesítése azt jelenti, hogy a szervezet tudja, mi a legfontosabb neki, míg a 13.2. teljesítése azt bizonyítja, hogy a szervezet tudja, hogyan védi meg a konkrét informatikai rendszert. Csak az RBT bemutatása (13.2.) nem igazolja automatikusan, hogy a szervezet elvégezte a stratégiai szintű kritikus infrastruktúra-tervezést (1.9.).

4. FELHASZNÁLT FORRÁSOK:

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 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