IBF szolgáltatás igénybevétele esetén javasolt szervezeti elvárások és az IBF megbízásának részletei

VFP2 KiberVéd - NIS2 Audit felkészítés szakmai iránymutatás 2026/11

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.08.08	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

A Szabályozott Tevékenységek Felügyeleti Hatósága által véleményezett dokumentum

1. VEZETŐI ÖSSZEFOGLALÓ

Az információbiztonsági felelős elsődleges feladata a szervezet információbiztonsági irányítási rendszerének szakmai felügyelete és koordinálása. Ennek keretében gondoskodik az információbiztonsági követelmények kialakításáról, érvényesülésének nyomon követéséről, a kockázatok és biztonsági intézkedések felügyeletéről, az auditok és fejlesztések szakmai támogatásáról, valamint a vezetés rendszeres tájékoztatásáról. Az információbiztonsági felelős tevékenysége elsősorban irányító, koordináló és ellenőrző jellegű, nem helyettesíti az informatikai üzemeltetés vagy más szervezeti egységek operatív feladatait.

2. A VIZSGÁLANDÓ KÉRDÉS

Mi az IBF feladata? Információbiztonsági felelős szolgáltatás igénybevétele során - milyen szervezeti elvárásokat javasolt megfogalmazni, IBF felkészítő megbízásának részletei?

3. VÁLASZ

3.1 Az IBF szerepe a szervezetben

Az IBF többféleképpen vehet részt a szervezet életében. Teheti ezt úgy, mint Columbo felesége, mindenki tudja, hogy van, de senki sem látta, vagy ellenkezőleg minden informatikával kapcsolatos dologban részt - vesz. A IBF nem vezető, nem architect, nem rendszermérnök, nem az informatikai területen vagy informatikáért felelős vezető irányítása alatt végzi munkáját. Az azonban elképzelhető, hogy, hogy rendelkezik valamilyen informatikai végzettséggel. Az információbiztonsági felelős feladata nem az, hogy minden informatikai biztonsági feladatot maga végezzen el, hanem hogy **ha még nincs elkészítse, irányítsa, felügyelje és ellenőrizze** a szervezet információbiztonsági rendszerét, valamint biztosítsa a jogszabályi és belső követelményeknek való megfelelést.

Alapvető jogi és garanciális elv, hogy bár az információbiztonsági felelős (IBF) kulcsszerepet játszik a szervezet kiberbiztonsági folyamatainak kialakításában, felügyeletében és szakmai irányításában, az információbiztonságért és a vonatkozó jogszabályi (pl. Kiberbiztonsági tv., NIS2 irányelv) előírásoknak való megfelelésért a végső jogi és anyagi felelősséget minden esetben a szervezet mindenkori vezetője viseli. Az IBF tevékenysége a vezetői döntések szakmai és operatív támogatására irányul, feladata a kockázatok transzparens bemutatása, azonban a szervezet vezetője a felelősséget a megbízással nem ruházhatja át az IBF-re.

3.2 Az IBF fő feladatai (a szervezet jogos elvárásai)

Feladat	Azon belül végzett tevékenység
Információbiztonsági irányítás	• kialakítja és működteti az információbiztonsági irányítási rendszert (IBIR),

Feladat	Azon belül végzett tevékenység
	• elkészíti vagy koordinálja a szükséges szabályzatokat, • gondoskodik azok folyamatos felülvizsgálatáról, • biztosítja a vezetői jóváhagyást.
Kockázatkezelés	Koordinálja: • az informatikai kockázatok felmérését, • a kockázatelemzéseket, • a kockázatkezelési intézkedéseket, • a vezetői döntések előkészítését.
Biztonsági intézkedések felügyelete	Ellenőrzi többek között: • hozzáférés-kezelést • jogosultságkezelést • naplózást • mentéseket • visszatöltéseket, rendszer helyreállításokat • sérülékenységkezelést • patch menedzsmentet • konfigurációkezelést • titkosítás alkalmazását • végpontvédelmet • hálózatbiztonságot • beszállítói biztonságot • felhasználói tevékenységet
Incidenskezelés	Részt vesz: • az információbiztonsági incidensek kezelésében, • azok kivizsgálásában, • a kiváltó okok elemzésében, • a javító intézkedések meghatározásában, • szükség esetén kapcsolatot tart a hatóságokkal, elvégzi a hatósági bejelentéseket.
Biztonságtudatosság	Szervezi: • éves oktatásokat, • szerepkör alapú képzéseket, • új belépők oktatását,

Feladat	Azon belül végzett tevékenység
	• biztonságtudatosság szintjének folyamatos fenntartását
Beszállítók felügyelete	Ellenőrzi: • biztonsági szerződéses követelményeket, • külső szolgáltatók biztonsági intézkedéseit, • beszállítói kockázatokat.
Jogszabályi megfelelőség biztosítása	Figyelemmel kíséri: • a hazai jogszabályokat, • az uniós előírásokat (NIS2 stb.), • az SZTFH/NKI ajánlásait, • a vonatkozó információbiztonsági szabványokat, • gyártói, iparági ajánlásokat • javaslatot készít a szükséges intézkedésekre.
Vezetői tájékoztatás, tanácsadás	Jelentéseket készít, rendszeresen tájékoztatja a vezetést: • a biztonsági helyzetről, • a kockázatokról, • a fejlesztési igényekről, • az auditok eredményeiről, • a megfelelőségi állapotról.

3.3 IBF megbízásával kapcsolatos főbb szempontok

Jogosan merül fel a kérdés, ezt a nagy mennyiségű feladatot hogyan lehet számonkérni az IBF-en, milyen feltételek mellett bízzunk meg akár céget, akár magánszemélyt a feladatok elvégzésére. Fontos hangsúlyozni, hogy az IBF pozíció belső munkaviszonyban és külső megbízási jogviszonyban (cég vagy magánszemély bevonásával) egyaránt betölthető. Az alábbi szempontok a jogviszony jellegétől függetlenül, munkaszerződésben, munkaköri leírásban vagy megbízási szerződésben egyaránt érvényesítendők a feladatok elvégzésére.

3.3.1 Jól definiált megbízási szerződés

Nem elegendő a szerződésben annyit írni a szerződésbe, hogy „ellátja az információbiztonsági feladatokat”, hanem részletesen meg kell határozni a feladatköröket, felelősségeket, jogosultságokat, együttműködési kötelezettségeket, illetve jelentési kötelezettségeket. A szerződés mellékleteként célszerű csatolni egy **feladatjegyzéket** a szabályozásokból készített kivonatként, például az alábbi meghatározásokkal:

- elkészíti és a szervezet vezetőjének jóváhagyását (aláírását) követően megküldi a nemzeti kiberbiztonsági hatóság részére a szervezet információbiztonsági szabályzatát;

- elkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását, melyet a szervezet vezetője hagy jóvá;
- megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket,
- folyamatot tart fent az információbiztonsági tudatosításra és adatgazdai oktatásra megtartja vagy koordinálja az oktatásokat és az oktatóanyagok éves frissítését,
- véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet elektronikus információbiztonságot érintő szerződéseit és az informatikai beszerzéseket és fejlesztéseket;
- gondoskodik az elektronikus információbiztonságot érintő szabályzatok elkészítéséről és naprakészen tartásáról, éves felülvizsgálatáról;
- nyomon követi a jogszabályi változásokat és érvényesíti a szervezet szabályozási környezetében;
- GAP elemzést és intézkedési tervet készít és nyomon követi annak teljesülését;
- kapcsolatot tart az SZTFH-val, valamint szükség esetén a Nemzeti Kiberbiztonsági Intézettel;
- opcionálisan felkészíti a kiberbiztonsági auditra a Megbízót, illetve kontrollálja az audit tevékenységeket;
- elvégzi az EIR (Elektronikus Információs Rendszer) besorolások és kockázatelemzés felülvizsgálatát;
- meghatározott időnként elvégzi a jogosultság-nyilvántartás ellenőrzését, (AD adatainak exportálása alapján a felhasználói jogosultságok rendszeres kontrollját elvégzi és egyezteti a jogosultságokat az elvárt szerepkörökkel.)
- elvégzi a karbantartási terv ellenőrzését, IT eszközökre és rendszerekre vonatkozó karbantartási ütemterv meglétének és végrehajtásának vizsgálatát;
- részt vesz az üzletmenet-folytonossági és katasztrófahelyreállítási teszteléseken, elvégzi a BCP/DRP teszt jegyzőkönyv ellenőrzését az EIR működőképességének biztosítása érdekében;
- elvégzi az adatmentések vizsgálatát, a mentési rendszer rendszeres ellenőrzését, beleértve a mentések meglétét, integritását és visszaállíthatóságát;
- felülvizsgálja az incidenskezelési eljárásokat, az incidensek bejelentésének, dokumentálásának és kezelésének szabályozását;
- meghatározott időnként biztonságértékeléseket végez a meghatározott Biztonságértékelési terven szereplő mérőszámok alapján és jelentést készít a vezetőség számára.

Természetesen amennyiben az IBF készíti el a szabályozásokat akkor erre nincsen szükség.

3.3.2 Éves munkaterv

Érdemes számon kérhető éves munkatervet készíteni, amelyben negyedéves, akár havi lebontásban szerepelnek a felsorolt feladatok, így egy évre előre tervezhetőek a szükséges erőforrások, valamint mely területek mikor kerülnek ellenőrzésre, felülvizsgálatra.

3.3.3 Kötelező jelenlét

Nem feltétlenül óraszámot kell meghatározni, hanem **eseményekhez kötött részvételi kötelezettséget**. Egy fix havi minimum rendelkezésre állási idő (például 16-32 óra) ugyanakkor segíthet biztosítani, hogy legyen elegendő kapacitás a rendszeres feladatokra. Ebből az is kiderül, hogy az olyan IBF, **aki 10-15 vagy akár több szervezetnél lát el IBF feladatokat jó eséllyel nem tud teljeskörűen megfelelni** a jogszabályok által támasztott követelményeknek!

Fontosnak tartjuk megjegyezni, hogy jogilag az IBF jelenlétére nincs elvárás. Több iparágat is átölelő tapasztalatok alapján egy IBF feladatai havi szinten 2-3 napot minimum igényelnek, havi egy napos munkával, évi 12 napnyi munkával egy irányítási rendszer összes ellenőrzési és felügyeleti tevékenysége általában nem végezhető el. A feladatok időigénye természetesen függ attól is, hogy mekkora a szervezet és végez-e a szervezet saját maga ellenőrzéseket dokumentáltan, jegyzőkönyvezve, vagy sem.

3.3.4 Eredménytermékek, jelentések listája

Érdemes előre meghatározni milyen dokumentumokat kell elkészíteni az IBF-nek. A jelenlegi szabályozási környezet nagymértékű adminisztrációt ró a szervezetekre, meg kell határozni, ebből melyik az IBF felelőssége. Az alábbiakban tipikusan ilyen dokumentumok találhatóak.

Fő dokumentumok:

- IBSZ
- szabályzatok és eljárásrendek (külön a 19 követelménycsaládhoz vagy egyben az IBSZ-szel)

Stratégiák, tervek:

- Kockázatmenedzsment stratégia (Kockázatkezelési módszertan, Kockázatelemzés, GAP elemzés)
- Biztonságértékelési terv
- Üzletmenetfolytonossági terv (BCP)
- Katasztrófa utáni helyreállítási terv (DRP)
- Folyamatos felügyeleti stratégia

Biztonságtudatossággal kapcsolatos anyagok:

- általános információbiztonsági képzés tematika
- szerepkörszerinti képzések tematikája

Jegyzőkönyvek, jelentések

- felülvizsgálatok jegyzőkönyvei
- tesztelések jegyzőkönyvei
- időszakos biztonságértékelési jelentések
- vezetői tájékoztatók

3.4 IBF (felkészítő) kiválasztása

A NIS2 irányelv (2022/2555 EU Parlament és Tanács 2022. december 14-i irányelve) hatálybalépése óta nagyon sokan kezdtek el **információbiztonsági felelősi szolgáltatást** kínálni, miközben a szervezetnek gyakran nincs eszköze annak megítélésére, hogy a szolgáltató valóban rendelkezik-e a szükséges szakmai tapasztalattal. Az audit tapasztalatok sajnos azt is megmutatták, hogy **nagy múltú cégek sem jelentenek garanciát, nem minden esetben sikerült az új szabályozásnak megfelelő tudást és módszertant** integrálniuk szolgáltatásaikba.

A szervezetnek ezért kiválasztási eljárás során érdemes bekérni a pályázóktól az alábbiakat:

- a szakmai önéletrajzot, különös tekintettel az információbiztonsági tapasztalatra;
- a releváns szakmai végzettségeket, képesítéseket alátámasztó tanúsítványokat, igazolásokat;
- az elmúlt években ellátott információbiztonsági felelősi megbízások ismertetését (hány szervezetnél lát el IBF feladatokat, mekkora szervezeteket támogat, milyen biztonsági osztályú szervezetekkel dolgozott);
- a korábban végzett hasonló projektek rövid bemutatását (hány NIS2 auditot készített elő, kísért végig, **milyen sikerességgel**);
- az érintett ágazatban (pl. önkormányzat, egészségügy, pénzügyi szektor, energetika) szerzett tapasztalat igazolását, referenciát;
- a tervezett munkamódszer, együttműködési rend és jelentési rendszer bemutatását;
- szakmai felelősségbiztosítás meglétének igazolását (ha rendelkezésre áll);
- a helyettesítés biztosításának módját akadályoztatás esetén

A kiválasztás folyamata során a gyakorlati tapasztalatot, a korábbi referenciákat, a bemutatott munkamódszert és a dokumentált szakmai teljesítményt legalább olyan súllyal célszerű értékelni, mint a végzettségeket és tanúsítványokat.

3.5 Szakmai ajánlás

A fentiekből látható, hogy az IBF munkája sokrétű és felelősségteljes feladat, ugyanakkor rendkívüli mértékben függ a szervezet többi területével való (informatikai üzemeltetés, munkaügy, felsővezetés) együttműködéstől és azok támogatásától. Ha ezek nincsenek meg, az IBF munkája sem lesz teljes értékű, ami hosszú távon az információbiztonságot veszélyeztetheti. A megfelelő személy kiválasztása ugyanakkor hosszú távon befolyásolja a szervezet ellenállóképességet és üzletmenet folytonosságát.

A piaci szereplők (a törvény 1. § (1) d) és e) pontja szerinti szervezetek) jogilag mentesülnek a szigorú összeférhetetlenségi szabályok alól, így kinevezhetnek informatikai vezetőt is IBF-nek. Ezt a megoldást azonban szakmai szempontból érdemes kerülni. Az IBF feladata többek között az IT üzemeltetési tevékenységek (például a jogosultságkezelés, a javításmenedzsment és az adatmentések) biztonsági felügyelete és ellenőrzése. Az **érdekkonfliktus elkerülése, valamint a biztonsági intézkedések objektív, független kontrollja érdekében kiemelten javasolt az üzemeltetői és az információbiztonsági ellenőrző szerepkörök szervezeti vagy személyi**

szintű szétválasztása, még akkor is, ha azt a jogszabály az adott szervezettípusnál nem teszi kötelezővé.

4. JOGI HÁTTÉR

4.1 Általános követelmények

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban, mint „Kiberbiztonsági tv.") részletesen meghatározza az IBF kijelölésének, feladatainak és felelősségének kereteit.

A legfontosabb előírások az alábbiak.

- A Magyarország kiberbiztonságáról szóló törvény alapján minden érintett szervezet köteles kijelölni vagy megbízni egy felelős személyt.

> *A szervezet vezetője az elektronikus információs rendszer védelméhez kapcsolódó feladatok ellátása, a kockázatmenedzsment keretrendszer működtetése, a kiberbiztonsági incidensek bejelentése és a kiberbiztonsági incidenskezelő központtal való kapcsolattartás érdekében a szervezeten belül kijelöli az elektronikus információs rendszer biztonságáért felelős személyt vagy a szervezeten kívüli személlyel megállapodást köt. [2024. évi LXIX. törvény 11. § (1) bekezdés]*

- Az IBF feladatait kizárólag olyan természetes személy láthatja el, aki megfelel az alapvető törvényi kritériumoknak:

> *Az elektronikus információs rendszer biztonságáért felelős személy feladatait csak olyan személy végezheti, aki a) 18. életévét betöltötte, b) cselekvőképes, büntetlen előéletű [2024. évi LXIX. törvény 11. § (3) bekezdés]*

- A hatékony munkavégzés érdekében a jogszabály garantálja az IBF függetlenségét és megfelelő erőforrás-ellátottságát.

> *A szervezet vezetője biztosítja, hogy az elektronikus információs rendszer biztonságáért felelős személy a) az elektronikus információs rendszerek védelmét érintő döntés előkészítésében részt vegyen; b) részére rendelkezésre álljanak az elektronikus információs rendszer védelmének biztosításához szükséges feltételek, jogosultságok, információk, és pénzügyi erőforrások; [2024. évi LXIX. törvény 11. § (6) bekezdés]*

A biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelet (a továbbiakban „7/2024 MK rendelet") a védelmi intézkedések katalógusában a feladatkört az alábbiak szerint konkretizálja az összes biztonsági osztályra (Alap, Jelentős, Magas) vonatkozóan:

> *A szervezet vezetője a jogszabályi követelményeknek megfelelő, az elektronikus információs rendszerek biztonságáért felelős személyt nevez*

ki a szervezeti szintű információbiztonsági szabályzatnak való megfelelés koordinálására, fejlesztésére, bevezetésére és fenntartására és biztosítja számára a célok eléréséhez szükséges erőforrásokat. [7/2024. (VI. 24.) MK rendelet 2. melléklet 1.2 (A), (J), (M)]

- Az IBF kiemelt jogosultságokkal rendelkezik, ugyanakkor szigorú titoktartás is köti.

Az elektronikus információs rendszer biztonságáért felelős személyt feladata ellátásával kapcsolatosan tudomására jutott adatok és információk tekintetében titoktartási kötelezettség terheli. [2024. évi LXIX. törvény 11. § (7) bekezdés]
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]

4.2 Különbségek az egyes szervezettípusokra vonatkozó szabályok között

A Kiberbiztonsági törvény szövege alapján eltérő rendelkezések vonatkoznak a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozó, azaz a középvállalkozás méretet elérő és kockázatos vagy kiemeleten kockázatos ágazatba tartozó szervezetek valamint az e) pont alá tartozó hírközlési és bizalmi szolgáltatókra és az a) -c) és f) pontokba tartozó szervezetekre (közigazgatás, többségi állami befolyás alatt álló szervezetek, honvédelem, a továbbiakban „közszférába tartozó szervezetek”).

Követelmény	**a), b), c) és f) pont szerinti szervezetek (Közigazgatás, állami cégek, honvédelem)**	**d) és e) pont szerinti szervezetek (Közép- és nagyvállalatok, spec. szolgáltatók)**
Szakirányú végzettség / tapasztalat kötelező?	Igen (törvényi előírás)	Nem (kivéve, ha kritikus szervezetnek minősülnek)
Összeférhetetlenségi szabály alkalmazandó?	Igen (kivéve az a)-c) "fontos" minősítésűeket)	Nem
Részletes IBF feladatkör (Korm. rendelet szerint)?	Igen	Nem (kivéve, ha kritikus szervezetnek minősülnek)
Külső IBF esetén szerződés kötelező tartalmi elemei?	A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet határozza meg.	Szabad megállapodás tárgya

A szigorú képesítési előírások főszabály szerint csak a közigazgatási, állami és honvédelmi (a-c, f), valamint a kritikus szervezetekre vonatkoznak.

> *Az 1. § (1) bekezdés a)-c) és f) pontja szerinti szervezet, a Kszetv. alapján kritikus szervezetként kijelölt szervezet, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet esetében rendelkezik a feladatellátáshoz szükséges, az informatikáért felelős miniszter rendeletében előírt végzettséggel, valamint rendelkezik [...] szakképzettséggel, vagy [...] szakmai tapasztalattal. [2024. évi LXIX. törvény 11. § (4) bekezdés]*

Az elektronikus információs rendszer biztonságáért felelős személy (IBF) végzettségére, szakképzettségére, valamint képzésére és továbbképzésére vonatkozó részletes követelményeket a 17/2025. (VII. 24.) EM rendelet határozza meg.

Lényegesek az összeférhetetlenségi szabályok. Az alapvető állami szerveknél az IBF nem lehet azonos az IT vezetővel, de a d) és e) pont szerinti piaci szereplők mentesülnek ez alól.

> *Az elektronikus információs rendszer biztonságáért felelős személyként [...] nem jelölhető ki vagy bízható meg a szervezet informatikai üzemeltetési vagy informatikai fejlesztési vezetői feladatait ellátó személy vagy az a személy, aki a szervezeten belül informatikai üzemeltetéssel, informatikai fejlesztéssel kapcsolatos munkakört lát el, illetve ilyen személy közvetlen alárendeltségébe tartozik. [2024. évi LXIX. törvény 11. § (4) bekezdés]*
> *Az (5) bekezdést nem kell alkalmazni a következő szervezetek vonatkozásában: a) az 1. § (1) bekezdés a)-c) pontja szerinti fontos szervezetek, b) az 1. § (1) bekezdés d) és e) pontja szerinti szervezetek. [2024. évi LXIX. törvény 11. § (6) bekezdés]*

A Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelet részletes feladatlistát határoz meg (pl. szabályzatok előkészítése, helyzetértékelés készítése, hatósággal való kapcsolattartás), de ennek hatálya alól a d) és e) pont szerinti normál szervezetek kikerülnek.

> *E rendeletnek az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó rendelkezéseit az alábbi szervezetekre kell alkalmazni: a) a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) és f) pontja, valamint 1. § (2a) bekezdése szerinti szervezetekre, b) a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti azon szervezetekre, amelyek a [...] Kszetv. alapján kritikus szervezetként vannak kijelölve [...], valamint c) a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti azon szervezetekre, amelyek a [...] Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kerültek kijelölésre [...] [418/2024. (XII. 23.) Korm. rendelet 1. § (2) bekezdés]*

5. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény a Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)

- 1/2025 (I.31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- 418/2024. (XII. 23.) Korm. rendelet a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- **AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2022. december 14-i (EU) 2022/2555 IRÁNYELVE 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)** *